PCI Scan Vulnerability Report

PCI Status

The following table highlights the overall compliance status and each individual system's compliance status. Following the table is a detailed report specifying each system and its specific vulnerabilities.

Overall PCI Status	FAIL

Live IP Address Scanned	Security Risk Rating	PCI Status
162.144.102.68		FAIL

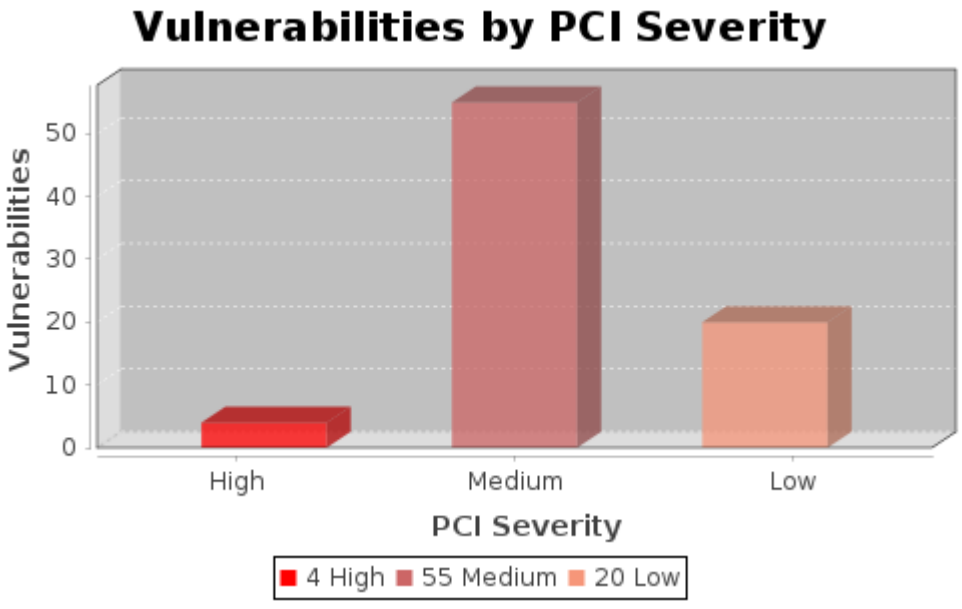
Report Summary	
Company:	MINNESOTA NURSERY AND LANDSCAPE
Hosts in account	3
Hosts scanned	3
Hosts active	1
Scan date	January 26, 2022
Report date	January 28, 2022

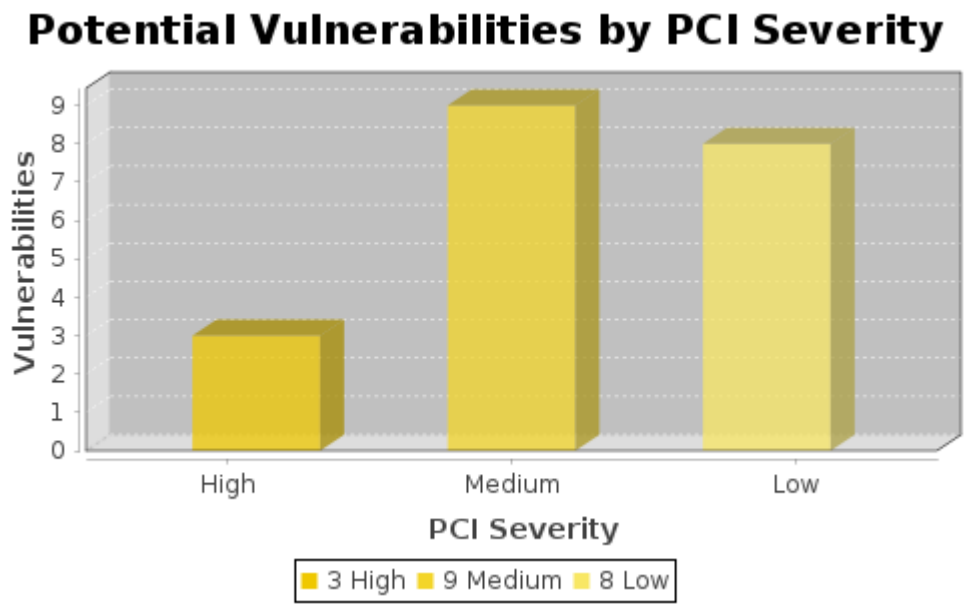
Summary of Vulnerabilities

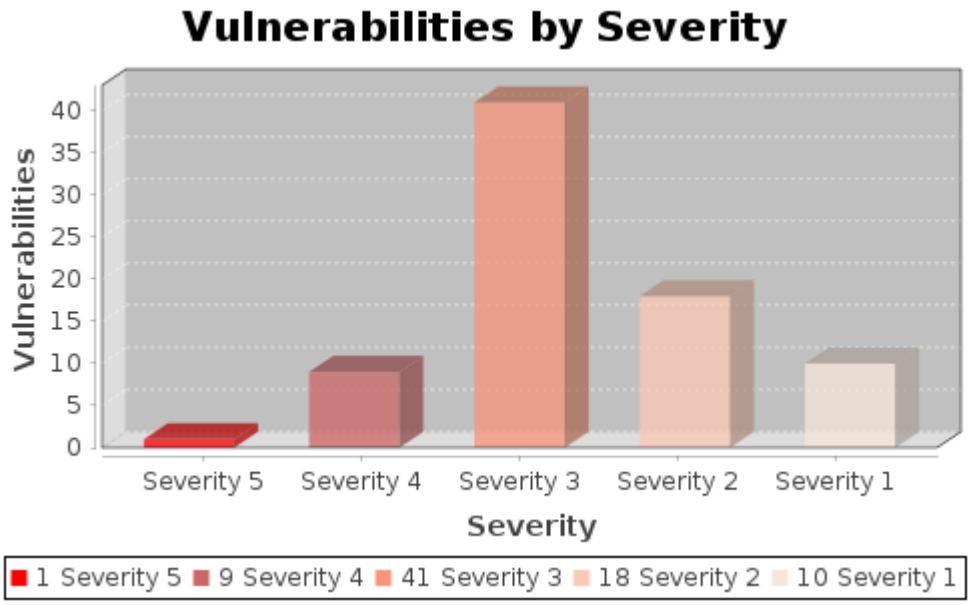
Vulnerabilities total:	391	Security risk:	5

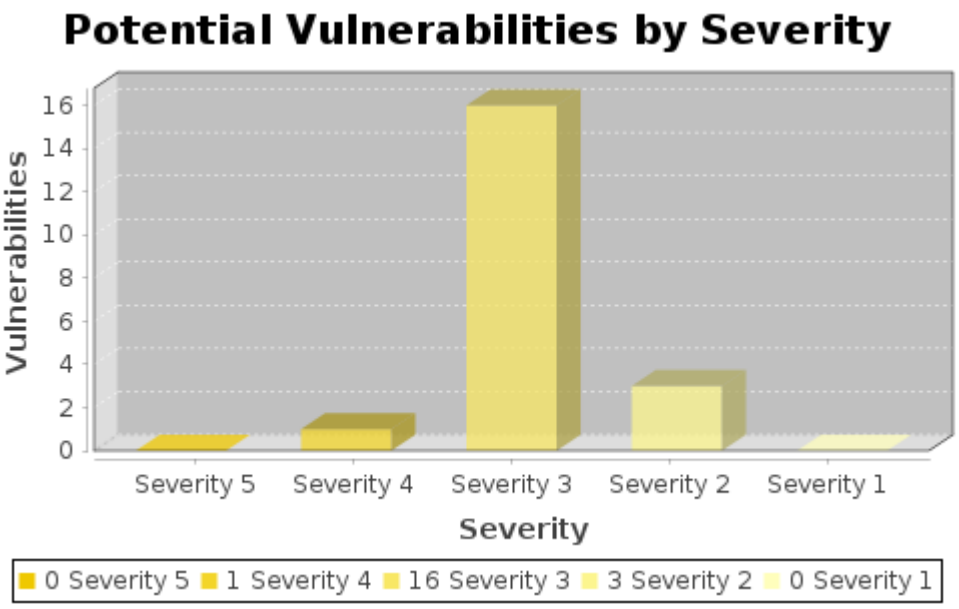
by Severity				
Severity	**Confirmed**	**Potential**	**Information gathered**	**Total**
5	1	0	0	1
4	9	1	0	10
3	41	16	9	66
2	18	3	28	49
1	10	0	255	265
Total	79	20	292	391

by PCI Severity			
PCI Severity	**Confirmed**	**Potential**	**Total**
High	4	3	7
Medium	55	9	64
Low	20	8	28
Total	79	20	99




Potential Vulnerabilities by PCI Severity
Vulnerabilities
0
1
2
3
4
5
6
7
8
9
High
Medium
Low
PCI Severity
3 High
9 Medium
8 Low


Vulnerabilities by Severity
Vulnerabilities
0
5
10
15
20
25
30
35
40
Severity 5
Severity 4
Severity 3
Severity 2
Severity 1
Severity
1 Severity 5
9 Severity 4
41 Severity 3
18 Severity 2
10 Severity 1


Potential Vulnerabilities by Severity
Vulnerabilities
16
14
12
10
8
6
4
2
0
Severity 5
Severity 4
Severity 3
Severity 2
Severity 1
Severity
0 Severity 5
1 Severity 4
16 Severity 3
3 Severity 2
0 Severity 1

Detailed Results

162.144.102.68 (server.northerngreenexpo.org,)

Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP

Vulnerabilities total:	391	Security risk:	5

Vulnerabilities (79)

Blind SQL Injection — port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

Automatic Failure: SQL Injection

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**9.3** AV:N/AC:M/Au:N/C:C/I:C/A:C
CVSS Temporal Score:	**6.8** E:U/RL:W/RC:UC
Severity:	**5**
QID:	150012
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-06-04 16:07:51.0

THREAT:

Blind SQL injection is a specialized type of SQL injection that enables an attacker to modify the syntax of a SQL query in order to retrieve, corrupt, or delete data. A successful exploit manipulates the query's logic. Queries created by concatenating strings with SQL syntax and user-supplied data are prone to this vulnerability. When any part of the string concatenation can be modified, an attacker has the ability to change the meaning of the query.

Typical detection techniques for SQL injection vulnerabilities use a payload that attempts to produce an SQL error from the web application. Detection based on blind SQL injection uses inference based on the differences among the application's responses to various payloads. Blind SQL does not rely on error messages, which is beneficial when testing web applications that trap errors.

The WAS scanning engine uses a well-known technique called True / False inference to determine if there is a blind SQL injection vulnerability. Basically, it uses two payloads: one with a True condition and another with a False condition. If there is a blind SQL injection vulnerability, the query with the True condition payload will cause the web application to return a different response than the False condition payload.

A good example of a True condition payload is ' AND 1=1 (since 1 always equals 1, the condition is true). An example of a False condition payload is ' AND 1=2 (since 1 does not equal 2, the condition is false).

Say there is a web application with an input that searches customer first names and displays the results inside a table. Assume that if someone searches for John there is one result only. When scanning for blind SQL injection, the scanning engine sends two payloads:
- True condition payload: John' AND 1=1
This condition is true, so one record is returned and the output is John, which is the same as if the payload was the name John by itself.
- False condition payload: John' AND 1=2
The condition is false, so no records are returned and the output is nothing or a message such as No Results Found.

Seeing the difference in results, the scanning engine draws the conclusion that there is a blind SQL injection vulnerability.

IMPACT:
The scope of a SQL injection exploit varies greatly. If any SQL statement can be injected into the query, then the attacker has the equivalent access of a database administrator. This access could lead to theft of data, malicious corruption of data, or deletion of data.

SOLUTION:
SQL injection vulnerabilities can be addressed in three areas: input validation, query creation, and database security.

All input received from the client side should be validated for correct content. If a value's type or content range is known beforehand, then stricter filters should be applied. For example, an email address should be in a specific format and only contain characters that make it a valid address; or numeric fields like a USA zip code should be limited to five digit values.

Prepared statements (also referred to as parameterized queries) provide strong protection from SQL injection. Prepared statements are precompiled SQL queries whose parameters can be modified when the query is executed. Prepared statements enforce the logic of the query and will fail if the query cannot be compiled correctly. Programming languages that support prepared statements provide specific functions for creating queries. These functions are more secure than string concatenation for assigning user-supplied data to a query.

Stored procedures are precompiled queries that reside in the database. Like prepared statements, they also enforce separation of query data and logic. SQL statements that call stored procedures should not be created via string concatenation, otherwise their security benefits are negated.

SQL injection exploits can be mitigated by the use of Access Control Lists or role-based access within the database. For example, a read-only account would prevent an attacker from modifying data, but would not prevent the user from viewing unauthorized data. Table and row-based access controls potentially minimize the scope of a compromise, but they do not prevent exploits.

For more information, see the OWASP SQL Injection Prevention Cheat Sheet.

RESULT:
url: http://northerngreen.org/?sid=1&bsa_pro_id=12%20%2B%20(SELECT%200%20FROM%20(SELECT%20SLEEP(29))qsqli_1111)%20&bsa_pro_url=1
Tested parameter: bsa_pro_id
Payload: %20%2B%20(SELECT%200%20FROM%20(SELECT%20SLEEP(29))qsqli_1111)%20
comment: (Times are expressed in milliseconds.)
Expected response delay: 28000
Observed response delay: 120000
Mean response time: 55
Standard deviation: 19
Number of stddev from mean: 6294.201096

matched: This vulnerability was identified using time-based inference that compared the average response time of a page to its response time with an injected payload. This vulnerability is confirmed based on timing rather than the content of the response.

Login Form Is Not Submitted Via HTTPS — port 2082 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**8.5** AV:N/AC:L/Au:N/C:N/I:P/A:C
CVSS Temporal Score:	**7.2** E:U/RL:U/RC:C
Severity:	**4**
QID:	150053
Category:	Web Application
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Last Update:	2017-10-06 20:39:30.0

THREAT:
The login form's default action contains a link that is not submitted via HTTPS (HTTP over SSL).

IMPACT:
Sensitive data such as authentication credentials should be encrypted when transmitted over the network. Otherwise they are exposed to sniffing attacks.

SOLUTION:
Change the login form's action to submit via HTTPS.

RESULT:
url: http://server.northerngreenexpo.org:2082/login/
Payload: N/A
comment: Parent URL of Login Form is : http://server.northerngreenexpo.org:2082/
matched: Login Form Is Not Submitted Via HTTPS

Login Form Is Not Submitted Via HTTPS — port 2086 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**8.5** AV:N/AC:L/Au:N/C:N/I:P/A:C
CVSS Temporal Score:	**7.2** E:U/RL:U/RC:C
Severity:	**4**
QID:	150053
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-10-06 20:39:30.0

THREAT:
The login form's default action contains a link that is not submitted via HTTPS (HTTP over SSL).

IMPACT:
Sensitive data such as authentication credentials should be encrypted when transmitted over the network. Otherwise they are exposed to sniffing attacks.

SOLUTION:
Change the login form's action to submit via HTTPS.

RESULT:
url: http://server.northerngreenexpo.org:2086/login/
Payload: N/A
comment: Parent URL of Login Form is : http://server.northerngreenexpo.org:2086/
matched: Login Form Is Not Submitted Via HTTPS

Login Form Is Not Submitted Via HTTPS — port 2095 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**8.5** AV:N/AC:L/Au:N/C:N/I:P/A:C
CVSS Temporal Score:	**7.2** E:U/RL:U/RC:C
Severity:	**4**
QID:	150053
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-10-06 20:39:30.0

THREAT:
The login form's default action contains a link that is not submitted via HTTPS (HTTP over SSL).

IMPACT:
Sensitive data such as authentication credentials should be encrypted when transmitted over the network. Otherwise they are exposed to sniffing attacks.

SOLUTION:
Change the login form's action to submit via HTTPS.

RESULT:
url: http://server.northerngreenexpo.org:2095/login/
Payload: N/A
comment: Parent URL of Login Form is : http://server.northerngreenexpo.org:2095/
matched: Login Form Is Not Submitted Via HTTPS

SSL Server Allows Anonymous Authentication Vulnerability — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.1** AV:N/AC:H/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	**4.1** E:U/RL:W/RC:C
Severity:	**4**
QID:	38142

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-25 17:36:07.0

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.

A vulnerability exists in SSL communications when clients are allowed to connect using no authentication algorithm. SSL client-server communication may use several different types of authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the communications are vulnerable to a man-in-the-middle attack."

IMPACT:

An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:

Disable support for anonymous authentication to mitigate this vulnerability.

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

SSL Server Allows Anonymous Authentication Vulnerability — port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.1** AV:N/AC:H/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	**4.1** E:U/RL:W/RC:C
Severity:	**4**
QID:	38142
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-25 17:36:07.0

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.

A vulnerability exists in SSL communications when clients are allowed to connect using no authentication algorithm. SSL client-server communication may use several different types of authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the communications are vulnerable to a man-in-the-middle attack."

IMPACT:

An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:

Disable support for anonymous authentication to mitigate this vulnerability.

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

SSL Server Allows Anonymous Authentication Vulnerability — port 21 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.1** AV:N/AC:H/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	**4.1** E:U/RL:W/RC:C
Severity:	**4**
QID:	38142
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-25 17:36:07.0

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.

A vulnerability exists in SSL communications when clients are allowed to connect using no authentication algorithm. SSL client-server communication may use several different types of authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the communications are vulnerable to a man-in-the-middle attack."

IMPACT:

An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:

Disable support for anonymous authentication to mitigate this vulnerability.

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
ADH-RC4-MD5	DH	None	MD5	RC4(128)	MEDIUM
ADH-DES-CBC3-SHA	DH	None	SHA1	3DES(168)	MEDIUM
ADH-AES128-SHA	DH	None	SHA1	AES(128)	MEDIUM
ADH-AES256-SHA	DH	None	SHA1	AES(256)	HIGH
ADH-CAMELLIA128-SHA	DH	None	SHA1	Camellia(128)	MEDIUM
ADH-AES128-SHA256	DH	None	SHA256	AES(128)	MEDIUM
ADH-AES256-SHA256	DH	None	SHA256	AES(256)	HIGH
ADH-CAMELLIA256-SHA	DH	None	SHA1	Camellia(256)	HIGH
ADH-SEED-SHA	DH	None	SHA1	SEED(128)	MEDIUM
ADH-AES128-GCM-SHA256	DH	None	AEAD	AESGCM(128)	MEDIUM
ADH-AES256-GCM-SHA384	DH	None	AEAD	AESGCM(256)	HIGH
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

SSL Server Allows Anonymous Authentication Vulnerability — port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.1** AV:N/AC:H/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	**4.1** E:U/RL:W/RC:C
Severity:	**4**
QID:	38142
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-25 17:36:07.0

THREAT:

The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.

A vulnerability exists in SSL communications when clients are allowed to connect using no authentication algorithm. SSL client-server communication may use several different types of authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the communications are vulnerable to a man-in-the-middle attack."

IMPACT:

An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:

Disable support for anonymous authentication to mitigate this vulnerability.

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION					
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.9** E:F/RL:W/RC:C
Severity:	**3**
QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:18:19.0

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:

PCI: ASV Program Guide v3.1 (page 27)

PCI: Use of SSL Early TLS and ASV Scans

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

RESULT:

TLSv1.0 is supported

Same Site Scripting

port 2086 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.9** AV:L/AC:M/Au:N/C:C/I:P/A:P
CVSS Temporal Score:	**5.6** E:H/RL:W/RC:C
Severity:	**3**
QID:	150353
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-14 12:31:05.0

THREAT:

Most of the DNS servers include records of the form localhost. IN A 127.0.0.1 But if by mistake, the administrator misses the trailing dot, the record is not fully qualified. So if the domain is example.com, the queries for localhost.example.com would resolve to 127.0.0.1. Reference: https://seclists.org/bugtraq/2008/Jan/270

IMPACT:

The websites in affected domain cannot be securely accessed on multi-user system. The attacker can trick another user on the same system to access websites on affected domain in such a manner as to result in cross site scripting leaking cookies.

SOLUTION:

Non fully qualified localhost entries should not be present in the nameserver for domains that host websites with HTTP state management (cookies).

RESULT:

url: http://server.northerngreenexpo.org:2086/
matched: Same site scripting detected
Host: localhost.northerngreenexpo.org IP: 127.0.0.1

Deprecated SSH Cryptographic Settings — port 22 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**6.4** AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	**4.7** E:U/RL:W/RC:UC
Severity:	**3**
QID:	38739
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-05-26 11:40:40.0

THREAT:

The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another.

The target is using deprecated SSH cryptographic settings to communicate.

IMPACT:

A man-in-the-middle attacker may be able to exploit this vulnerability to record the communication to decrypt the session key and even the messages.

SOLUTION:

Avoid using deprecated cryptographic settings.

Use best practices when configuring SSH.

Refer to Security of Interactive and Automated Access Management Using Secure Shell (SSH) .

Settings currently considered deprecated:

Ciphers using CFB of OFB

Very uncommon, and deprecated because of weaknesses compared to newer cipher chaining modes such as CTR or GCM

RC4 cipher (arcfour, arcfour128, arcfour256)

The RC4 cipher has a cryptographic bias and is no longer considered secure

Ciphers with a 64-bit block size (DES, 3DES, Blowfish, IDEA, CAST)

Ciphers with a 64-bit block size may be vulnerable to birthday attacks (Sweet32)

Key exchange algorithms using DH group 1 (diffie-hellman-group1-sha1, gss-group1-sha1-*)

DH group 1 uses a 1024-bit key which is considered too short and vulnerable to Logjam-style attacks

Key exchange algorithm "rsa1024sha1"

Very uncommon, and deprecated because of the short RSA key size

MAC algorithm "umac-32"

Very uncommon, and deprecated because of the very short MAC length

Cipher "none"

This is available only in SSHv1

RESULT:

Type	Name
key exchange	diffie-hellman-group1-sha1
cipher	arcfour256
cipher	arcfour128
cipher	3des-cbc
cipher	blowfish-cbc
cipher	cast128-cbc
cipher	arcfour

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

port 26 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0
The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.9** E:F/RL:W/RC:C
Severity:	**3**
QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:18:19.0

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27)
PCI: Use of SSL Early TLS and ASV Scans

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:
Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

RESULT:
TLSv1.0 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)
port 21 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38601
Category:	General remote services
CVE ID:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Last Update:	2021-09-27 12:30:52.0

THREAT:

Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.

SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4(Arcfour) to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that there is a stronger bias in RC4(Arcfour) , which makes statistical analysis of ciphertext more practical.

The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples that can be used for statistical analysis.

NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.

This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4(Arcfour) was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and TLS. However, TLSv 1.2 or later address these issues.

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ADH-RC4-MD5	DH	None	MD5	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

Discovery of Unix Account Names Vulnerability — port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	5001
Category:	Brute Force Attack
CVE ID:	CVE-2001-1013
Vendor Reference:	-
Bugtraq ID:	3335
Last Update:	2009-06-16 00:24:08.0

THREAT:

When a request for a user is made (http://your.host/~user), certain servers (such as Apache Versions 1.3.12 and 1.3.9) return a different reply depending on whether the account user exists on the host or not.

If a request is made for an account that exists on the host, a 403 error is returned. If a request is made for a non-existent account, then a 404 error is returned.

IMPACT:

Unauthorized remote users can implement brute force attacks on the Web server to guess a valid account name on the server. Even though they may be successful in obtaining a valid account, they will still have to guess the password. However, if user passwords are weak, some services may also be brute forced.

SOLUTION:

Disable the default-enabled "UserDir" directive. To do so, add the following line to the httpd.conf file:

UserDir Disabled

Apache Versions 1.3.9 and 1.3.12 are vulnerable. Other Web servers may also be vulnerable. There are currently no patches available. We strongly advise you to upgrade to a later version of Apache.

RESULT:

N.	**Server**	**Account**
	root	
	operator	

Same Site Scripting — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.9** AV:L/AC:M/Au:N/C:C/I:P/A:P

CVSS Temporal Score:	**5.6** E:H/RL:W/RC:C
Severity:	**3**
QID:	150353
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-14 12:31:05.0

THREAT:

Most of the DNS servers include records of the form localhost. IN A 127.0.0.1 But if by mistake, the administrator misses the trailing dot, the record is not fully qualified. So if the domain is example.com, the queries for localhost.example.com would resolve to 127.0.0.1. Reference: https://seclists.org/bugtraq/2008/Jan/270

IMPACT:

The websites in affected domain cannot be securely accessed on multi-user system. The attacker can trick another user on the same system to access websites on affected domain in such a manner as to result in cross site scripting leaking cookies.

SOLUTION:

Non fully qualified localhost entries should not be present in the nameserver for domains that host websites with HTTP state management (cookies).

RESULT:

url: https://server.northerngreenexpo.org/
matched: Same site scripting detected
Host: localhost.northerngreenexpo.org IP: 127.0.0.1

Web Server Uses Plain Text Basic Authentication — port 2077 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	MED
FAIL	The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.3** E:U/RL:U/RC:UC
Severity:	**3**
QID:	86763
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-11-22 13:35:55.0

THREAT:

During Web server authentication, communication can take place with the user by Clear Text User Credentials.
This Qid detects the HTTP basic authentication by sending a request and looks for the value of "WWW-Authenticate: Basic realm=" header field in response.

IMPACT:

Using Readable Clear Text can help eavesdropping and thereby compromise confidentiality. An attacker can successfully exploit this issue when the 401 error is returned when authentication is required. Also, an attacker can find out that the Basic Authentication scheme is used using the WWW-authenticate header.

SOLUTION:
Please contact the vendor of the hardware/software for a possible fix for the issue. It is advisable to work with vendor to disable communication over HTTP and make sure that every sensitive information transmits over HTTPS.

RESULT:
GET /localstart.asp HTTP/1.0
Host: server.northerngreenexpo.org:2077
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)

<html>Authorization Required</html>Service Name: HTTP on TCP port 2077.
HTTP Service Accepting Basic Auth Credentials Detected

Remote Management Service Accepting Unencrypted Credentials Detected(HTTP)

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.3** E:U/RL:W/RC:UR
Severity:	**3**
QID:	45242
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-02-18 04:31:23.0

THREAT:
A remote management service that accepts unencrypted credentials was detected on the target host.

Services like HTTP with basic auth are checked.

IMPACT:
A malicious individual can easily intercept unencrypted passwords during transmission using a "network sniffer" and use this data to gain unauthorized access.

SOLUTION:
If possible, use alternate services that provide encryption.
Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission.

RESULT:
Service Name: HTTP on TCP port 2079.
HTTP Service Accepting Basic Auth Credentials DetectedService Name: HTTP on TCP port 2077.
HTTP Service Accepting Basic Auth Credentials Detected

Mail Server Accepts Plaintext Credentials — port 587 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.6** E:U/RL:W/RC:UC
Severity:	**3**
QID:	74147
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-05-12 01:12:19.0

THREAT:

Your Mail Server responds to the EHLO command which implies that it uses the ESMTP protocol. ESMTP uses the AUTH command which indicates an authentication mechanism to the server. If the server supports the requested authentication mechanism, it performs an authentication protocol exchange to authenticate and identify the user. Optionally, it also negotiates a security layer for subsequent protocol interactions.

Your server accepts PLAIN or LOGIN as one of the AUTH parameters. The authentication credentials are transmitted in plaintext over the network and no encryption is performed.

IMPACT:

Malicious users could obtain mail server credentials by sniffing the traffic. This can allow unauthorized users to use the mail server as an open mail relay. It may also lead to compromise of account credentials that can be used to access other mail services like POP3 and IMAP.

SOLUTION:

Disable the plaintext authentication methods on your SMTP server for unencrypted (non-SSL/TLS) sessions. You may consider using more advanced challenge-based authentication methods like CRAM-MD5 or DIGEST-MD5.

Please contact your vendor for configuration information. Also check RFC 2554 and RFC 2487 for more details.

RESULT:

EHLO qualysguard.com

250-server.northerngreenexpo.org Hello qualysguard.com [64.39.98.8]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP

AUTH PLAIN

334

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.9** E:F/RL:W/RC:C
Severity:	**3**
QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:18:19.0

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:

PCI: ASV Program Guide v3.1 (page 27)

PCI: Use of SSL Early TLS and ASV Scans

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

RESULT:

TLSv1.0 is supported

Same Site Scripting

port 2080 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.9** AV:L/AC:M/Au:N/C:C/I:P/A:P
CVSS Temporal Score:	**5.6** E:H/RL:W/RC:C
Severity:	**3**
QID:	150353
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-14 12:31:05.0

THREAT:

Most of the DNS servers include records of the form localhost. IN A 127.0.0.1 But if by mistake, the administrator misses the trailing dot, the record is not fully qualified. So if the domain is example.com, the queries for localhost.example.com would resolve to 127.0.0.1. Reference: https://seclists.org/bugtraq/2008/Jan/270

IMPACT:

The websites in affected domain cannot be securely accessed on multi-user system. The attacker can trick another user on the same system to access websites on affected domain in such a manner as to result in cross site scripting leaking cookies.

SOLUTION:

Non fully qualified localhost entries should not be present in the nameserver for domains that host websites with HTTP state management (cookies).

RESULT:

url: https://server.northerngreenexpo.org:2080/
matched: Same site scripting detected
Host: localhost.northerngreenexpo.org IP: 127.0.0.1

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)

port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38601

Category:	General remote services
CVE ID:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Last Update:	2021-09-27 12:30:52.0

THREAT:

Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.

SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4(Arcfour) to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that there is a stronger bias in RC4(Arcfour) , which makes statistical analysis of ciphertext more practical.

The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples that can be used for statistical analysis.

NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.

This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4(Arcfour) was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and TLS. However, TLSv 1.2 or later address these issues.

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

Web Server Uses Plain-Text Form Based Authentication — port 2095 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.8** E:POC/RL:W/RC:UC
Severity:	**3**
QID:	86728
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-08-25 06:21:49.0

THREAT:

The Web server uses plain-text form based authentication. A web page exists on the target host which uses an HTML login form. This data is sent from the client to the server in plain-text.

IMPACT:

An attacker with access to the network traffic to and from the target host may be able to obtain login credentials for other users by sniffing the network traffic.

SOLUTION:

Please contact the vendor of the hardware/software for a possible fix for the issue. For custom applications, ensure that data sent via HTML login forms is encrypted before being sent from the client to the host.

RESULT:

GET /admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2095

<form novalidate id="login_form" action="/login/" method="post" target="_self" style="visibility:">
<label for="user">Email Address</label>

<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your email address." class="std_textbox" type="text" tabindex="1" required>

<label for="pass">Password</label>

<input name="pass" id="pass" placeholder="Enter your email password." class="std_textbox" type="password" tabindex="2" required>

<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>

</form>

GET /w3-msql/index.html HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /session/adminlogin HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /default.asp\ HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /loadpage.cgi?user_id=id&file=/ HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /commerce.cgi?page=../../../../../etc/passwd%00index.html HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /commerce.cgi?page=../../../../../../windows/system32/drivers/etc/hosts%00index.html HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /index.php3 HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/.htaccess HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/nph-publish HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/nph-publish.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/pagelog.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /nph-maillist.pl HTTP/1.0
Host: server.northerngreenexpo.org:2095

POST /login/newsup.pl HTTP/1.0
Host: server.northerngreenexpo.org:2095
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++POST /login/newsup.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2095
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++GET /login/subscribe.pl HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/whois.cgi?action=load&whois=%3Bcat+%2Fetc%2Fpasswd HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /stats.php HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/gbook.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2095

Web Server Uses Plain-Text Form Based Authentication — port 2082 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.8** E:POC/RL:W/RC:UC
Severity:	**3**
QID:	86728
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-08-25 06:21:49.0

THREAT:
The Web server uses plain-text form based authentication. A web page exists on the target host which uses an HTML login form. This data is sent from the client to the server in plain-text.

IMPACT:
An attacker with access to the network traffic to and from the target host may be able to obtain login credentials for other users by sniffing the network traffic.

SOLUTION:
Please contact the vendor of the hardware/software for a possible fix for the issue. For custom applications, ensure that data sent via HTML login forms is encrypted before being sent from the client to the host.

RESULT:
GET /admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2082

<form novalidate id="login_form" action="/login/" method="post" target="_self" style="visibility:">
<label for="user">Username</label>

<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your username." class="std_textbox" type="text" tabindex="1" required>

<label for="pass">Password</label>

<input name="pass" id="pass" placeholder="Enter your account password." class="std_textbox" type="password" tabindex="2" required>

<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>

</form>

GET /login/admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/.htaccess HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/nph-publish HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/nph-publish.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/pagelog.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082

POST /login/newsup.pl HTTP/1.0
Host: server.northerngreenexpo.org:2082
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++POST /login/newsup.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++GET /login/subscribe.pl HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/whois.cgi?action=load&whois=%3Bcat+%2Fetc%2Fpasswd HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/gbook.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/cgiforum.pl?thesection=../../../../../../../etc/passwd%00 HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/cgiforum.cgi?thesection=../../../../../../../etc/passwd%00 HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/bigconf.cgi?command=view_textfile&file=/etc/passwd&filters=; HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/QUALYS10197RSBD.pl HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/cachemgr.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/bb-hist.sh?HISTFILE=/home/* HTTP/1.0

Host: server.northerngreenexpo.org:2082

GET /login/unlg1.1 HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/unlg1.2 HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/AT-generate.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082

Mail Server Accepts Plaintext Credentials — port 26 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.6** E:U/RL:W/RC:UC
Severity:	**3**
QID:	74147
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-05-12 01:12:19.0

THREAT:
Your Mail Server responds to the EHLO command which implies that it uses the ESMTP protocol. ESMTP uses the AUTH command which indicates an authentication mechanism to the server. If the server supports the requested authentication mechanism, it performs an authentication protocol exchange to authenticate and identify the user. Optionally, it also negotiates a security layer for subsequent protocol interactions.

Your server accepts PLAIN or LOGIN as one of the AUTH parameters. The authentication credentials are transmitted in plaintext over the network and no encryption is performed.

IMPACT:
Malicious users could obtain mail server credentials by sniffing the traffic. This can allow unauthorized users to use the mail server as an open mail relay. It may also lead to compromise of account credentials that can be used to access other mail services like POP3 and IMAP.

SOLUTION:
Disable the plaintext authentication methods on your SMTP server for unencrypted (non-SSL/TLS) sessions. You may consider using more advanced challenge-based authentication methods like CRAM-MD5 or DIGEST-MD5.

Please contact your vendor for configuration information. Also check RFC 2554 and RFC 2487 for more details.

RESULT:
EHLO qualysguard.com

250-server.northerngreenexpo.org Hello qualysguard.com [64.39.98.8]

250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP

AUTH LOGIN

334 VXNlcm5hbWU6

EHLO qualysguard.com

250-server.northerngreenexpo.org Hello qualysguard.com [64.39.98.8]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP

AUTH PLAIN

334

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.9** E:F/RL:W/RC:C
Severity:	**3**
QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1

Bugtraq ID:	-
Last Update:	2021-07-12 22:18:19.0

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27)
PCI: Use of SSL Early TLS and ASV Scans

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:
Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

RESULT:
TLSv1.0 is supported

POP3 Server Allows Plain Text Authentication Vulnerability — port 110 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**6.4** AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	**5.5** E:POC/RL:W/RC:C
Severity:	**3**
QID:	74224
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2008-10-06 17:54:44.0

THREAT:
Post Office Protocol version 3 (POP3) is an application layer internet standard protocol to retrieve e-mail from a remote server.

Use of the PASS command sends passwords in the clear over the network. Also, servers that answer -ERR to the User command are giving potential attackers clues about which names are valid.

IMPACT:
Malicious users could obtain mail server credentials by sniffing the traffic. This can allow unauthorized users to use the mail server as an open mail relay.

SOLUTION:
POP3 supports several authentication methods to provide varying levels of protection. Contact your vendor for further configuration information.

RESULT:
N/A

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)

port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level:	MED
FAIL	Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38601
Category:	General remote services
CVE ID:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Last Update:	2021-09-27 12:30:52.0

THREAT:
Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.

SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4(Arcfour) to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that there is a stronger bias in RC4(Arcfour) , which makes statistical analysis of ciphertext more practical.

The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples that can be used for statistical analysis.

NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:
If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.

This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4(Arcfour) was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and TLS. However, TLSv 1.2 or later address these issues.

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM

Same Site Scripting — port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.9** AV:L/AC:M/Au:N/C:C/I:P/A:P
CVSS Temporal Score:	**5.6** E:H/RL:W/RC:C
Severity:	**3**
QID:	150353
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-14 12:31:05.0

THREAT:
Most of the DNS servers include records of the form localhost. IN A 127.0.0.1 But if by mistake, the administrator misses the trailing dot, the record is not fully qualified. So if the domain is example.com, the queries for localhost.example.com would resolve to 127.0.0.1. Reference: https://seclists.org/bugtraq/2008/Jan/270

IMPACT:
The websites in affected domain cannot be securely accessed on multi-user system. The attacker can trick another user on the same system to access websites on affected domain in such a manner as to result in cross site scripting leaking cookies.

SOLUTION:
Non fully qualified localhost entries should not be present in the nameserver for domains that host websites with HTTP state management (cookies).

RESULT:
url: http://server.northerngreenexpo.org/
matched: Same site scripting detected
Host: localhost.northerngreenexpo.org IP: 127.0.0.1

Same Site Scripting — port 2077 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.9** AV:L/AC:M/Au:N/C:C/I:P/A:P
CVSS Temporal Score:	**5.6** E:H/RL:W/RC:C
Severity:	**3**
QID:	150353
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-14 12:31:05.0

THREAT:
Most of the DNS servers include records of the form localhost. IN A 127.0.0.1 But if by mistake, the administrator misses the trailing dot, the record is not fully qualified. So if the domain is example.com, the queries for localhost.example.com would resolve to 127.0.0.1. Reference: https://seclists.org/bugtraq/2008/Jan/270

IMPACT:
The websites in affected domain cannot be securely accessed on multi-user system. The attacker can trick another user on the same system to access websites on affected domain in such a manner as to result in cross site scripting leaking cookies.

SOLUTION:
Non fully qualified localhost entries should not be present in the nameserver for domains that host websites with HTTP state management (cookies).

RESULT:
url: http://server.northerngreenexpo.org:2077/
matched: Same site scripting detected
Host: localhost.northerngreenexpo.org IP: 127.0.0.1

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

port 587 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.9** E:F/RL:W/RC:C
Severity:	**3**
QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:18:19.0

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:

PCI: ASV Program Guide v3.1 (page 27)

PCI: Use of SSL Early TLS and ASV Scans

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

RESULT:

TLSv1.0 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)

port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38601
Category:	General remote services
CVE ID:	CVE-2013-2566, CVE-2015-2808
Vendor Reference:	-
Bugtraq ID:	91787, 58796, 73684
Last Update:	2021-09-27 12:30:52.0

THREAT:

Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.

SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4(Arcfour) to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that there is a stronger bias in RC4(Arcfour) , which makes statistical analysis of ciphertext more practical.

The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples that can be used for statistical analysis.

NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.

This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4(Arcfour) was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and TLS. However, TLSv 1.2 or later address these issues.

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM

AECDH-RC4-SHA	ECDH	None	SHA1 RC4(128)	MEDIUM
TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED				
RC4-MD5	RSA	RSA	MD5 RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1 RC4(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1 RC4(128)	MEDIUM
AECDH-RC4-SHA	ECDH	None	SHA1 RC4(128)	MEDIUM

Same Site Scripting — port 2095 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.9** AV:L/AC:M/Au:N/C:C/I:P/A:P
CVSS Temporal Score:	**5.6** E:H/RL:W/RC:C
Severity:	**3**
QID:	150353
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-14 12:31:05.0

THREAT:

Most of the DNS servers include records of the form localhost. IN A 127.0.0.1 But if by mistake, the administrator misses the trailing dot, the record is not fully qualified. So if the domain is example.com, the queries for localhost.example.com would resolve to 127.0.0.1. Reference: https://seclists.org/bugtraq/2008/Jan/270

IMPACT:

The websites in affected domain cannot be securely accessed on multi-user system. The attacker can trick another user on the same system to access websites on affected domain in such a manner as to result in cross site scripting leaking cookies.

SOLUTION:

Non fully qualified localhost entries should not be present in the nameserver for domains that host websites with HTTP state management (cookies).

RESULT:

url: http://server.northerngreenexpo.org:2095/
matched: Same site scripting detected
Host: localhost.northerngreenexpo.org IP: 127.0.0.1

Same Site Scripting — port 2082 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.9** AV:L/AC:M/Au:N/C:C/I:P/A:P
CVSS Temporal Score:	**5.6** E:H/RL:W/RC:C
Severity:	**3**
QID:	150353
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-14 12:31:05.0

THREAT:

Most of the DNS servers include records of the form localhost. IN A 127.0.0.1 But if by mistake, the administrator misses the trailing dot, the record is not fully qualified. So if the domain is example.com, the queries for localhost.example.com would resolve to 127.0.0.1. Reference: https://seclists.org/bugtraq/2008/Jan/270

IMPACT:

The websites in affected domain cannot be securely accessed on multi-user system. The attacker can trick another user on the same system to access websites on affected domain in such a manner as to result in cross site scripting leaking cookies.

SOLUTION:

Non fully qualified localhost entries should not be present in the nameserver for domains that host websites with HTTP state management (cookies).

RESULT:

url: http://server.northerngreenexpo.org:2082/
matched: Same site scripting detected
Host: localhost.northerngreenexpo.org IP: 127.0.0.1

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.9** E:F/RL:W/RC:C
Severity:	**3**
QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1

Bugtraq ID:	-
Last Update:	2021-07-12 22:18:19.0

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27)
PCI: Use of SSL Early TLS and ASV Scans

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:
Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

RESULT:
TLSv1.0 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level:	MED
FAIL	Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0 The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.9** E:F/RL:W/RC:C
Severity:	**3**
QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:18:19.0

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27)
PCI: Use of SSL Early TLS and ASV Scans

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:
Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

RESULT:
TLSv1.0 is supported

Web Server Uses Plain-Text Form Based Authentication — port 2086 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	MED
FAIL	The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.8** E:POC/RL:W/RC:UC
Severity:	**3**
QID:	86728
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-08-25 06:21:49.0

THREAT:
The Web server uses plain-text form based authentication. A web page exists on the target host which uses an HTML login form. This data is sent from the client to the server in plain-text.

IMPACT:

An attacker with access to the network traffic to and from the target host may be able to obtain login credentials for other users by sniffing the network traffic.

SOLUTION:

Please contact the vendor of the hardware/software for a possible fix for the issue. For custom applications, ensure that data sent via HTML login forms is encrypted before being sent from the client to the host.

RESULT:

GET /admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2086

<form novalidate id="login_form" action="/login/" method="post" target="_self" style="visibility:">
<label for="user">Username</label>

<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your username." class="std_textbox" type="text" tabindex="1" required>

<label for="pass">Password</label>

<input name="pass" id="pass" placeholder="Enter your account password." class="std_textbox" type="password" tabindex="2" required>

<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>

</form>

GET /w3-msql/index.html HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /session/adminlogin HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/.htaccess HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/nph-publish HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/nph-publish.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/pagelog.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2086

POST /login/newsup.pl HTTP/1.0
Host: server.northerngreenexpo.org:2086
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++POST /login/newsup.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2086
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++GET /login/subscribe.pl HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/whois.cgi?action=load&whois=%3Bcat+%2Fetc%2Fpasswd HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/gbook.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /default.asp\ HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/cgiforum.pl?thesection=../../../../../../etc/passwd%00 HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /loadpage.cgi?user_id=id&file=/ HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/cgiforum.cgi?thesection=../../../../../../etc/passwd%00 HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/bigconf.cgi?command=view_textfile&file=/etc/passwd&filters=; HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/QUALYS10197RSBD.pl HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/cachemgr.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2086

Web Server Uses Plain Text Basic Authentication — port 2079 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.3** E:U/RL:U/RC:UC
Severity:	**3**
QID:	86763
Category:	Web server
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-11-22 13:35:55.0

THREAT:

During Web server authentication, communication can take place with the user by Clear Text User Credentials.
This Qid detects the HTTP basic authentication by sending a request and looks for the value of "WWW-Authenticate: Basic realm=" header field in response.

IMPACT:

Using Readable Clear Text can help eavesdropping and thereby compromise confidentiality. An attacker can successfully exploit this issue when the 401 error is returned when authentication is required. Also, an attacker can find out that the Basic Authentication scheme is used using the WWW-authenticate header.

SOLUTION:

Please contact the vendor of the hardware/software for a possible fix for the issue. It is advisable to work with vendor to disable communication over HTTP and make sure that every sensitive information transmits over HTTPS.

RESULT:

GET /localstart.asp HTTP/1.0
Host: server.northerngreenexpo.org:2079
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)

<html>Authorization Required</html>Service Name: HTTP on TCP port 2079.
HTTP Service Accepting Basic Auth Credentials Detected

Same Site Scripting — port 2079 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.9** AV:L/AC:M/Au:N/C:C/I:P/A:P
CVSS Temporal Score:	**5.6** E:H/RL:W/RC:C
Severity:	**3**
QID:	150353
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-14 12:31:05.0

THREAT:

Most of the DNS servers include records of the form localhost. IN A 127.0.0.1 But if by mistake, the administrator misses the trailing dot, the record is not fully qualified. So if the domain is example.com, the queries for localhost.example.com would resolve to 127.0.0.1. Reference: https://seclists.org/bugtraq/2008/Jan/270

IMPACT:
The websites in affected domain cannot be securely accessed on multi-user system. The attacker can trick another user on the same system to access websites on affected domain in such a manner as to result in cross site scripting leaking cookies.

SOLUTION:
Non fully qualified localhost entries should not be present in the nameserver for domains that host websites with HTTP state management (cookies).

RESULT:
url: http://server.northerngreenexpo.org:2079/
matched: Same site scripting detected
Host: localhost.northerngreenexpo.org IP: 127.0.0.1

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level:	MED
FAIL	Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0 The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.9** E:F/RL:W/RC:C
Severity:	**3**
QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:18:19.0

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27)
PCI: Use of SSL Early TLS and ASV Scans

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

RESULT:

TLSv1.0 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level:	MED
FAIL	Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0 The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.9** E:F/RL:W/RC:C
Severity:	**3**
QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:18:19.0

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:

PCI: ASV Program Guide v3.1 (page 27)
PCI: Use of SSL Early TLS and ASV Scans

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

RESULT:

TLSv1.0 is supported

Same Site Scripting — port 2078 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.9** AV:L/AC:M/Au:N/C:C/I:P/A:P
CVSS Temporal Score:	**5.6** E:H/RL:W/RC:C
Severity:	**3**
QID:	150353
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-14 12:31:05.0

THREAT:

Most of the DNS servers include records of the form localhost. IN A 127.0.0.1 But if by mistake, the administrator misses the trailing dot, the record is not fully qualified. So if the domain is example.com, the queries for localhost.example.com would resolve to 127.0.0.1. Reference: https://seclists.org/bugtraq/2008/Jan/270

IMPACT:

The websites in affected domain cannot be securely accessed on multi-user system. The attacker can trick another user on the same system to access websites on affected domain in such a manner as to result in cross site scripting leaking cookies.

SOLUTION:

Non fully qualified localhost entries should not be present in the nameserver for domains that host websites with HTTP state management (cookies).

RESULT:

url: https://server.northerngreenexpo.org:2078/
matched: Same site scripting detected
Host: localhost.northerngreenexpo.org IP: 127.0.0.1

Session Cookie Does Not Contain the "Secure" Attribute — port 2095 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**4.3** E:U/RL:U/RC:C
Severity:	**2**
QID:	13162
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-29 13:30:31.0

THREAT:

The secure cookie flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text. By setting the secure flag, the browser will prevent the transmission of a cookie over an unencrypted channel.

A cookie with the secure attribute was not detected in the scan.

QID Detection Logic:
This unauthenticated QID checks for the existence of the "secure" cookie flag.

IMPACT:

Session cookies sent via HTTP expose users to sniffing attacks that could lead to user impersonation or account compromise.

SOLUTION:

Apply the "secure" attribute to session cookies to ensure that they are sent via HTTPS only. More information about this flag can be found here: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie.

RESULT:

HTTP Cookie missing Secure attribute on port 2095.
Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2095
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2095

SSH Server Public Key Too Small — port 22 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**3.6** E:U/RL:W/RC:UC
Severity:	**2**
QID:	38738

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-01-03 10:41:41.0

THREAT:

The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another.

The SSH Server is using a small Public Key.

Best practices require that RSA digital signatures be 2048 or more bits long to provide adequate security. Key lengths of 1024 are acceptable through 2013, but since 2011 they are considered deprecated.

For more information, please refer to NIST Special Publication 800-131A (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf).

Only server keys that are not part of a certificate are reported in this QID. OpenSSH certificates using short keys are reported in QID 38733. X.509 certificates using short keys are reported in QID 38171.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability to record the communication to decrypt the session key and even the messages.

SOLUTION:

DSA keys and RSA keys shorter than 2048 bits are considered vulnerable. It is recommended to install a RSA public key length of at least 2048 bits or greater, or to switch to ECDSA or EdDSA.

RESULT:

Algorithm	Length
ssh-dss	1024 bits

Session Cookie Does Not Contain the "Secure" Attribute — port 2082 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**4.3** E:U/RL:U/RC:C
Severity:	**2**
QID:	13162
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-29 13:30:31.0

THREAT:

The secure cookie flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure

flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text. By setting the secure flag, the browser will prevent the transmission of a cookie over an unencrypted channel.

A cookie with the secure attribute was not detected in the scan.

QID Detection Logic:
This unauthenticated QID checks for the existence of the "secure" cookie flag.

IMPACT:
Session cookies sent via HTTP expose users to sniffing attacks that could lead to user impersonation or account compromise.

SOLUTION:
Apply the "secure" attribute to session cookies to ensure that they are sent via HTTPS only. More information about this flag can be found here: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie.

RESULT:
HTTP Cookie missing Secure attribute on port 2082.
Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2082

HTTP Security Header Not Detected — port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**3.5** E:U/RL:U/RC:UR
Severity:	**2**
QID:	11827
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-01-27 06:59:20.0

THREAT:
This QID reports the absence of the following HTTP headers according to CWE-693: Protection Mechanism Failure:
X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.
Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:
This unauthenticated QID looks for the presence of the following HTTP responses:
The Valid directives are as belows: X-Content-Type-Options: nosniff

Strict-Transport-Security: max-age=< [;includeSubDomains]

IMPACT:
Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -lkL --verbose.

CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.

Customers are advised to set proper X-Content-Type-Options and Strict-Transport-Security HTTP response headers.

Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:

X-Content-Type-Options:
Apache: Header always set X-Content-Type-Options: nosniff

HTTP Strict-Transport-Security:
Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Nginx: add_header Strict-Transport-Security max-age=31536000;

Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

RESULT:

X-Content-Type-Options HTTP Header missing on port 80.

GET / HTTP/1.0
Host: server.northerngreenexpo.org

HTTP/1.1 200 OK
Date: Wed, 26 Jan 2022 12:43:52 GMT
Server: Apache
Last-Modified: Thu, 28 Oct 2021 14:25:02 GMT
Accept-Ranges: bytes
Content-Length: 163
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Session Cookie Does Not Contain the "Secure" Attribute — port 2086 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	**4.3** E:U/RL:U/RC:C
Severity:	**2**

QID:	13162
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-29 13:30:31.0

THREAT:
The secure cookie flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text. By setting the secure flag, the browser will prevent the transmission of a cookie over an unencrypted channel.

A cookie with the secure attribute was not detected in the scan.

QID Detection Logic:
This unauthenticated QID checks for the existence of the "secure" cookie flag.

IMPACT:
Session cookies sent via HTTP expose users to sniffing attacks that could lead to user impersonation or account compromise.

SOLUTION:
Apply the "secure" attribute to session cookies to ensure that they are sent via HTTPS only. More information about this flag can be found here: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie.

RESULT:
HTTP Cookie missing Secure attribute on port 2086.
Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2086

Directory Listing — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Directory traversal on web server

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.5** E:POC/RL:U/RC:C
Severity:	**2**
QID:	150023
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2018-09-13 03:30:54.0

THREAT:
The Web server presents a directory listing.

IMPACT:
All file names in this directory are exposed.

SOLUTION:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

RESULT:
url: https://northerngreen.org/wp-admin/js/
Payload: https://northerngreen.org/wp-admin/js/
comment: This directory was discovered during the path test phase.

Original URL is: https://northerngreen.org/wp-admin/

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/js</title>
</head>
<body>
<h1>Index of /wp-admin/js</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory </td><td>

url: https://northerngreen.org/wp-includes/php-compat/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/php-compat</title>
</head>
<body>
<h1>Index of /wp-includes/php-compat</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Dire

url: https://northerngreen.org/wp-includes/block-patterns/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/block-patterns</title>
</head>
<body>
<h1>Index of /wp-includes/block-patterns</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>

<tr><td valign="top"> </td><td><a href="/wp-includes/">Par

url: https://northerngreen.org/wp-includes/Requests/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/Requests</title>
</head>
<body>
<h1>Index of /wp-includes/Requests</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Director

url: https://northerngreen.org/wp-includes/assets/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/assets</title>
</head>
<body>
<h1>Index of /wp-includes/assets</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Directory</a

url: https://northerngreen.org/wp-includes/js/jcrop/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/jcrop</title>
</head>
<body>
<h1>Index of /wp-includes/js/jcrop</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent Direc

url: https://northerngreen.org/wp-includes/images/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>

<title>Index of /wp-includes/images</title>
</head>
<body>
<h1>Index of /wp-includes/images</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Directory</a

url: https://northerngreen.org/wp-includes/js/codemirror/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/codemirror</title>
</head>
<body>
<h1>Index of /wp-includes/js/codemirror</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Pa

url: https://northerngreen.org/wp-includes/js/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js</title>
</head>
<body>
<h1>Index of /wp-includes/js</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/block-supports/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/block-supports</title>
</head>
<body>
<h1>Index of /wp-includes/block-supports</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>

<tr><td valign="top"> </td><td><a href="/wp-includes/">Par

url: https://northerngreen.org/wp-includes/js/jquery/ui/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/jquery/ui</title>
</head>
<body>
<h1>Index of /wp-includes/js/jquery/ui</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/jquery

url: https://northerngreen.org/wp-content/uploads/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads</title>
</head>
<body>
<h1>Index of /wp-content/uploads</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/sitemaps/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/sitemaps</title>
</head>
<body>
<h1>Index of /wp-includes/sitemaps</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Director

url: https://northerngreen.org/wp-admin/images/
Payload: https://northerngreen.org/wp-admin/images/
comment: This directory was discovered during the path test phase.

Original URL is: https://northerngreen.org/wp-admin/

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/images</title>
</head>
<body>
<h1>Index of /wp-admin/images</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory <

url: https://northerngreen.org/wp-includes/PHPMailer/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/PHPMailer</title>
</head>
<body>
<h1>Index of /wp-includes/PHPMailer</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Direct

url: https://northerngreen.org/wp-includes/blocks/image/
Payload: https://northerngreen.org/wp-includes/blocks/image/
comment: This directory was discovered during the path test phase.

Original URL is: https://northerngreen.org/wp-includes/blocks/

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/blocks/image</title>
</head>
<body>
<h1>Index of /wp-includes/blocks/image</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/blocks/">

url: https://northerngreen.org/wp-includes/theme-compat/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/theme-compat</title>
</head>

<body>
<h1>Index of /wp-includes/theme-compat</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/icons/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/icons</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/icons</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan=

url: https://northerngreen.org/wp-includes/js/plupload/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/plupload</title>
</head>
<body>
<h1>Index of /wp-includes/js/plupload</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent

url: https://northerngreen.org/wp-includes/css/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/css</title>
</head>
<body>
<h1>Index of /wp-includes/css</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/Text/

comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/Text</title>
</head>
<body>
<h1>Index of /wp-includes/Text</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-admin/js/widgets/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/js/widgets</title>
</head>
<body>
<h1>Index of /wp-admin/js/widgets</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-admin/js/">Parent Directory<

url: https://northerngreen.org/wp-includes/js/crop/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/crop</title>
</head>
<body>
<h1>Index of /wp-includes/js/crop</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent Directo

url: https://northerngreen.org/wp-admin/includes/
Payload: https://northerngreen.org/wp-admin/includes/
comment: This directory was discovered during the path test phase.

Original URL is: https://northerngreen.org/wp-admin/

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>

<title>Index of /wp-admin/includes</title>
</head>
<body>
<h1>Index of /wp-admin/includes</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-admin/css/
Payload: https://northerngreen.org/wp-admin/css/
comment: This directory was discovered during the path test phase.

Original URL is: https://northerngreen.org/wp-admin/

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/css</title>
</head>
<body>
<h1>Index of /wp-admin/css</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory </td><t

url: https://northerngreen.org/wp-content/uploads/2021/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads/2021</title>
</head>
<body>
<h1>Index of /wp-content/uploads/2021</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-content/uploads/">Pa

url: https://northerngreen.org/wp-includes/js/imgareaselect/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/imgareaselect</title>
</head>
<body>
<h1>Index of /wp-includes/js/imgareaselect</h1>
<table>

<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/j

url: https://northerngreen.org/wp-includes/js/thickbox/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/thickbox</title>
</head>
<body>
<h1>Index of /wp-includes/js/thickbox</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th

url: https://northerngreen.org/wp-includes/rest-api/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/rest-api</title>
</head>
<body>
<h1>Index of /wp-includes/rest-api</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Director

url: https://northerngreen.org/wp-includes/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

<html>
<head>
<title>Index of /wp-includes</title>
</head>
<body>
<h1>Index of /wp-includes</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory </td><td> </t

url: https://northerngreen.org/wp-includes/IXR/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/IXR</title>
</head>
<body>
<h1>Index of /wp-includes/IXR</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/js/jquery/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/jquery</title>
</head>
<body>
<h1>Index of /wp-includes/js/jquery</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent Dir

url: https://northerngreen.org/wp-includes/SimplePie/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/SimplePie</title>
</head>
<body>
<h1>Index of /wp-includes/SimplePie</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<

/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Direct

url: https://northerngreen.org/wp-includes/pomo/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/pomo</title>
</head>
<body>
<h1>Index of /wp-includes/pomo</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/sodium_compat/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/sodium_compat</title>
</head>
<body>
<h1>Index of /wp-includes/sodium_compat</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Paren

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><

url: https://northerngreen.org/wp-includes/fonts/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

<html>
<head>
<title>Index of /wp-includes/fonts</title>
</head>
<body>
<h1>Index of /wp-includes/fonts</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/js/dist/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/dist</title>
</head>
<body>
<h1>Index of /wp-includes/js/dist</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent Directo

url: https://northerngreen.org/wp-includes/js/mediaelement/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/mediaelement</title>
</head>
<body>
<h1>Index of /wp-includes/js/mediaelement</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/

url: https://northerngreen.org/wp-includes/customize/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/customize</title>
</head>
<body>
<h1>Index of /wp-includes/customize</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<

/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Direct

url: https://northerngreen.org/wp-includes/random_compat/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/random_compat</title>
</head>
<body>
<h1>Index of /wp-includes/random_compat</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Paren

url: https://northerngreen.org/wp-includes/js/swfupload/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/swfupload</title>
</head>
<body>
<h1>Index of /wp-includes/js/swfupload</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Pare

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/images/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/images</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/images</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspa

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>

<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valig

url: https://northerngreen.org/wp-includes/certificates/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/certificates</title>
</head>
<body>
<h1>Index of /wp-includes/certificates</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent

url: https://northerngreen.org/wp-includes/ID3/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/ID3</title>
</head>
<body>
<h1>Index of /wp-includes/ID3</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/js/tinymce/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/tinymce</title>
</head>
<body>
<h1>Index of /wp-includes/js/tinymce</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>

<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent D

Directory Listing — port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — Automatic Failure: Directory traversal on web server

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.5** E:POC/RL:U/RC:C
Severity:	**2**
QID:	150023
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2018-09-13 03:30:54.0

THREAT:
The Web server presents a directory listing.

IMPACT:
All file names in this directory are exposed.

SOLUTION:
The presence of a browseable directory does not necessarily imply a vulnerability. Determine if the directory listing is intended to be displayed. Verify that no files in the directory contain content that should not be served by the Web application.

RESULT:
url: https://northerngreen.org/wp-admin/js/
Payload: https://northerngreen.org/wp-admin/js/
comment: This directory was discovered during the path test phase.

Original URL is: https://northerngreen.org/wp-admin/

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/js</title>
</head>
<body>
<h1>Index of /wp-admin/js</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory </td><td>

url: https://northerngreen.org/wp-includes/php-compat/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/php-compat</title>
</head>
<body>
<h1>Index of /wp-includes/php-compat</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Dire

url: https://northerngreen.org/wp-includes/block-patterns/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/block-patterns</title>
</head>
<body>
<h1>Index of /wp-includes/block-patterns</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Par

url: https://northerngreen.org/wp-includes/Requests/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/Requests</title>
</head>
<body>
<h1>Index of /wp-includes/Requests</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Director

url: https://northerngreen.org/wp-includes/assets/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/assets</title>

</head>
<body>
<h1>Index of /wp-includes/assets</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Directory</a

url: https://northerngreen.org/wp-includes/js/jcrop/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/jcrop</title>
</head>
<body>
<h1>Index of /wp-includes/js/jcrop</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent Direc

url: https://northerngreen.org/wp-includes/images/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/images</title>
</head>
<body>
<h1>Index of /wp-includes/images</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Directory</a

url: https://northerngreen.org/wp-includes/js/codemirror/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/codemirror</title>
</head>
<body>
<h1>Index of /wp-includes/js/codemirror</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Pa

url: https://northerngreen.org/wp-includes/js/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js</title>
</head>
<body>
<h1>Index of /wp-includes/js</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/block-supports/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/block-supports</title>
</head>
<body>
<h1>Index of /wp-includes/block-supports</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Par

url: https://northerngreen.org/wp-includes/js/jquery/ui/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/jquery/ui</title>
</head>
<body>
<h1>Index of /wp-includes/js/jquery/ui</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/jquery

url: https://northerngreen.org/wp-content/uploads/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads</title>

</head>
<body>
<h1>Index of /wp-content/uploads</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/sitemaps/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/sitemaps</title>
</head>
<body>
<h1>Index of /wp-includes/sitemaps</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Director

url: https://northerngreen.org/wp-admin/images/
Payload: https://northerngreen.org/wp-admin/images/
comment: This directory was discovered during the path test phase.

Original URL is: https://northerngreen.org/wp-admin/

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/images</title>
</head>
<body>
<h1>Index of /wp-admin/images</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory <

url: https://northerngreen.org/wp-includes/PHPMailer/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/PHPMailer</title>
</head>
<body>
<h1>Index of /wp-includes/PHPMailer</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<

/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Direct

url: https://northerngreen.org/wp-includes/blocks/image/
Payload: https://northerngreen.org/wp-includes/blocks/image/
comment: This directory was discovered during the path test phase.

Original URL is: https://northerngreen.org/wp-includes/blocks/

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/blocks/image</title>
</head>
<body>
<h1>Index of /wp-includes/blocks/image</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/blocks/">

url: https://northerngreen.org/wp-includes/theme-compat/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/theme-compat</title>
</head>
<body>
<h1>Index of /wp-includes/theme-compat</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/icons/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/icons</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/icons</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan=

url: https://northerngreen.org/wp-includes/js/plupload/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/plupload</title>
</head>
<body>
<h1>Index of /wp-includes/js/plupload</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent

url: https://northerngreen.org/wp-includes/css/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/css</title>
</head>
<body>
<h1>Index of /wp-includes/css</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/Text/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/Text</title>
</head>
<body>
<h1>Index of /wp-includes/Text</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-admin/js/widgets/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/js/widgets</title>
</head>
<body>
<h1>Index of /wp-admin/js/widgets</h1>

<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-admin/js/">Parent Directory<

url: https://northerngreen.org/wp-includes/js/crop/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/crop</title>
</head>
<body>
<h1>Index of /wp-includes/js/crop</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent Directo

url: https://northerngreen.org/wp-admin/includes/
Payload: https://northerngreen.org/wp-admin/includes/
comment: This directory was discovered during the path test phase.

Original URL is: https://northerngreen.org/wp-admin/

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/includes</title>
</head>
<body>
<h1>Index of /wp-admin/includes</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-admin/css/
Payload: https://northerngreen.org/wp-admin/css/
comment: This directory was discovered during the path test phase.

Original URL is: https://northerngreen.org/wp-admin/

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/css</title>
</head>
<body>
<h1>Index of /wp-admin/css</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<

/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory </td><t

url: https://northerngreen.org/wp-content/uploads/2021/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads/2021</title>
</head>
<body>
<h1>Index of /wp-content/uploads/2021</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-content/uploads/">Pa

url: https://northerngreen.org/wp-includes/js/imgareaselect/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/imgareaselect</title>
</head>
<body>
<h1>Index of /wp-includes/js/imgareaselect</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/j

url: https://northerngreen.org/wp-includes/js/thickbox/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/thickbox</title>
</head>
<body>
<h1>Index of /wp-includes/js/thickbox</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th

url: https://northerngreen.org/wp-includes/rest-api/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/rest-api</title>
</head>
<body>
<h1>Index of /wp-includes/rest-api</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Director

url: https://northerngreen.org/wp-includes/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes</title>
</head>
<body>
<h1>Index of /wp-includes</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory </td><td> </t

url: https://northerngreen.org/wp-includes/IXR/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/IXR</title>
</head>
<body>
<h1>Index of /wp-includes/IXR</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>

<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/js/jquery/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/jquery</title>
</head>
<body>
<h1>Index of /wp-includes/js/jquery</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent Dir

url: https://northerngreen.org/wp-includes/SimplePie/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/SimplePie</title>
</head>
<body>
<h1>Index of /wp-includes/SimplePie</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Direct

url: https://northerngreen.org/wp-includes/pomo/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/pomo</title>
</head>
<body>
<h1>Index of /wp-includes/pomo</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/sodium_compat/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>

<head>
<title>Index of /wp-includes/sodium_compat</title>
</head>
<body>
<h1>Index of /wp-includes/sodium_compat</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Paren

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><

url: https://northerngreen.org/wp-includes/fonts/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/fonts</title>
</head>
<body>
<h1>Index of /wp-includes/fonts</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/js/dist/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/dist</title>
</head>
<body>
<h1>Index of /wp-includes/js/dist</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>

<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent Directo

url: https://northerngreen.org/wp-includes/js/mediaelement/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/mediaelement</title>
</head>
<body>
<h1>Index of /wp-includes/js/mediaelement</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/

url: https://northerngreen.org/wp-includes/customize/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/customize</title>
</head>
<body>
<h1>Index of /wp-includes/customize</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Direct

url: https://northerngreen.org/wp-includes/random_compat/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/random_compat</title>
</head>
<body>
<h1>Index of /wp-includes/random_compat</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Paren

url: https://northerngreen.org/wp-includes/js/swfupload/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>

<head>
<title>Index of /wp-includes/js/swfupload</title>
</head>
<body>
<h1>Index of /wp-includes/js/swfupload</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Pare

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/images/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/images</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/images</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspa

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valig

url: https://northerngreen.org/wp-includes/certificates/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/certificates</title>
</head>
<body>
<h1>Index of /wp-includes/certificates</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>

<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent

url: https://northerngreen.org/wp-includes/ID3/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/ID3</title>
</head>
<body>
<h1>Index of /wp-includes/ID3</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/js/tinymce/
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/tinymce</title>
</head>
<body>
<h1>Index of /wp-includes/js/tinymce</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent D

WordPress XML-RPC Pingback Vulnerability — port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

The vulnerability is not included in the NVD.

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**4**
QID:	150362
Category:	Web Application
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Last Update:	2021-09-02 03:41:29.0

THREAT:
WordPress is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database.

XML-RPC in WordPress is an API which allows developers who make third party application and services the ability to interact to your WordPress site using features like Trackbacks and Pingbacks.

The Pingback feature of XML-RPC API allows attacks like DDOS and Server-Side Request Forgery (SSRF) either against the server hosting WordPress or against a target server.

QID Detection Logic:
This detection sends a POST request with XML data with invalid URL to verify the presence of vulnerability.

IMPACT:
On Successful exploitation, an attacker can control a WordPress site to conduct DDOS or Server-Side Request Forgery (SSRF) attack against a target server.

SOLUTION:
Remove "pingback.ping" method from XML-RPC.

RESULT:
url: https://northerngreen.org/xmlrpc.php
comment: WordPress XML-RPC Pingback Vulnerability detected at: 443

matched: 12:41:28 GMT
Transfer-Encoding: chunked
Content-Type: text/xml; charset=UTF-8

```
<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
<fault>
<value>
<struct>
<member>
<name>faultCode</name>
<value><int>0</int></value>
</member>
<member>
<name>faultString</name>
<value><string></string></value>
</member>
</struct>
</value>
</fault>
</methodResponse>
```

WordPress XML-RPC Pingback Vulnerability — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

The vulnerability is not included in the NVD.

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**4**
QID:	150362
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-09-02 03:41:29.0

THREAT:
WordPress is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database.

XML-RPC in WordPress is an API which allows developers who make third party application and services the ability to interact to your WordPress site using features like Trackbacks and Pingbacks.

The Pingback feature of XML-RPC API allows attacks like DDOS and Server-Side Request Forgery (SSRF) either against the server hosting WordPress or against a target server.

QID Detection Logic:
This detection sends a POST request with XML data with invalid URL to verify the presence of vulnerability.

IMPACT:
On Successful exploitation, an attacker can control a WordPress site to conduct DDOS or Server-Side Request Forgery (SSRF) attack against a target server.

SOLUTION:
Remove "pingback.ping" method from XML-RPC.

RESULT:
url: https://northerngreen.org/xmlrpc.php
form data: <?xml version="1.0" encoding="UTF-8"?> <methodCall> <methodName>pingback.ping</methodName> <params> <param> <value><string>http://127.0.0.1</string></value> </param> <param> <value><string> </string></value> </param> </params> </methodCall>
comment: WordPress XML-RPC Pingback Vulnerability detected at: 443

matched: 14:45:24 GMT
Transfer-Encoding: chunked
Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
<fault>
<value>
<struct>
<member>
<name>faultCode</name>
<value><int>0</int></value>
</member>
<member>
<name>faultString</name>
<value><string></string></value>
</member>
</struct>
</value>
</fault>
</methodResponse>

Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) — port 995 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS — ASV Score 2.6 : Currently PCI DSS reference "3DES" as a valid encryption cipher. 112-bit keys are acceptable until 2030 per document NIST SP800-57 part 1 Rev 4.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Last Update:	2021-09-20 15:31:22.0

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

Note: This CVE is patched at following versions

OPENSSL-0.9.8J-0.102.2

LIBOPENSSL0_9_8-0.9.8J-0.102.2

LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2

OPENSSL1-1.0.1G-0.52.1

OPENSSL1-DOC-1.0.1G-0.52.1

LIBOPENSSL1_0_0-1.0.1G-0.52.1

LIBOPENSSL1-DEVEL-1.0.1G-0.52.1

JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

More information can be found at Sweet32, Microsoft Windows TLS changes docs and Microsoft Transport Layer Security (TLS) registry settings

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM

Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) — port 143 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

ASV Score 2.6 : Currently PCI DSS reference "3DES" as a valid encryption cipher. 112-bit keys are acceptable until 2030 per document NIST SP800-57 part 1 Rev 4.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Last Update:	2021-09-20 15:31:22.0

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

Note: This CVE is patched at following versions

OPENSSL-0.9.8J-0.102.2

LIBOPENSSL0_9_8-0.9.8J-0.102.2

LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2

OPENSSL1-1.0.1G-0.52.1

OPENSSL1-DOC-1.0.1G-0.52.1

LIBOPENSSL1_0_0-1.0.1G-0.52.1

LIBOPENSSL1-DEVEL-1.0.1G-0.52.1

JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

More information can be found at Sweet32, Microsoft Windows TLS changes docs and Microsoft Transport Layer Security (TLS) registry settings

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM

Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) **port 2087 / tcp over ssl**

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

ASV Score 2.6 : Currently PCI DSS reference "3DES" as a valid encryption cipher. 112-bit keys are acceptable until 2030 per document NIST SP800-57 part 1 Rev 4.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Last Update:	2021-09-20 15:31:22.0

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

Note: This CVE is patched at following versions

OPENSSL-0.9.8J-0.102.2

LIBOPENSSL0_9_8-0.9.8J-0.102.2

LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2

OPENSSL1-1.0.1G-0.52.1

OPENSSL1-DOC-1.0.1G-0.52.1

LIBOPENSSL1_0_0-1.0.1G-0.52.1

LIBOPENSSL1-DEVEL-1.0.1G-0.52.1

JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

More information can be found at Sweet32, Microsoft Windows TLS changes docs and Microsoft Transport Layer Security (TLS) registry settings

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					

IDEA-CBC-SHA	RSA	RSA	SHA1 IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1 3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1 3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1 3DES(168)	MEDIUM

Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS — ASV Score 2.6 : Currently PCI DSS reference "3DES" as a valid encryption cipher. 112-bit keys are acceptable until 2030 per document NIST SP800-57 part 1 Rev 4.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Last Update:	2021-09-20 15:31:22.0

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

Note: This CVE is patched at following versions

OPENSSL-0.9.8J-0.102.2

LIBOPENSSL0_9_8-0.9.8J-0.102.2

LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2

OPENSSL1-1.0.1G-0.52.1

OPENSSL1-DOC-1.0.1G-0.52.1

LIBOPENSSL1_0_0-1.0.1G-0.52.1

LIBOPENSSL1-DEVEL-1.0.1G-0.52.1

JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

More information can be found at Sweet32, Microsoft Windows TLS changes docs and Microsoft Transport Layer Security (TLS) registry settings

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM

DES-CBC3-SHA	RSA	RSA	SHA1 3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1 3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1 3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED				
IDEA-CBC-SHA	RSA	RSA	SHA1 IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1 3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1 3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1 3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED				
IDEA-CBC-SHA	RSA	RSA	SHA1 IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1 3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1 3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1 3DES(168)	MEDIUM

Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) — port 993 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS — ASV Score 2.6 : Currently PCI DSS reference "3DES" as a valid encryption cipher. 112-bit keys are acceptable until 2030 per document NIST SP800-57 part 1 Rev 4.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Last Update:	2021-09-20 15:31:22.0

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

Note: This CVE is patched at following versions

OPENSSL-0.9.8J-0.102.2

LIBOPENSSL0_9_8-0.9.8J-0.102.2

LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2

OPENSSL1-1.0.1G-0.52.1

OPENSSL1-DOC-1.0.1G-0.52.1

LIBOPENSSL1_0_0-1.0.1G-0.52.1

LIBOPENSSL1-DEVEL-1.0.1G-0.52.1

JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

More information can be found at Sweet32, Microsoft Windows TLS changes docs and Microsoft Transport Layer Security (TLS) registry settings

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM

Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) — port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS — ASV Score 2.6 : Currently PCI DSS reference "3DES" as a valid encryption cipher. 112-bit keys are acceptable until 2030 per document NIST SP800-57 part 1 Rev 4.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Last Update:	2021-09-20 15:31:22.0

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

Note: This CVE is patched at following versions

OPENSSL-0.9.8J-0.102.2

LIBOPENSSL0_9_8-0.9.8J-0.102.2

LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2

OPENSSL1-1.0.1G-0.52.1

OPENSSL1-DOC-1.0.1G-0.52.1

LIBOPENSSL1_0_0-1.0.1G-0.52.1

LIBOPENSSL1-DEVEL-1.0.1G-0.52.1

JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

More information can be found at Sweet32, Microsoft Windows TLS changes docs and Microsoft Transport Layer Security (TLS) registry settings

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM

Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) — port 110 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS — ASV Score 2.6 : Currently PCI DSS reference "3DES" as a valid encryption cipher. 112-bit keys are acceptable until 2030 per document NIST SP800-57 part 1 Rev 4.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Last Update:	2021-09-20 15:31:22.0

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

Note: This CVE is patched at following versions

OPENSSL-0.9.8J-0.102.2

LIBOPENSSL0_9_8-0.9.8J-0.102.2

LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2

OPENSSL1-1.0.1G-0.52.1

OPENSSL1-DOC-1.0.1G-0.52.1

LIBOPENSSL1_0_0-1.0.1G-0.52.1

LIBOPENSSL1-DEVEL-1.0.1G-0.52.1

JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

More information can be found at Sweet32, Microsoft Windows TLS changes docs and Microsoft Transport Layer Security (TLS) registry settings

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM

Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) — port 21 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS — ASV Score 2.6 : Currently PCI DSS reference "3DES" as a valid encryption cipher. 112-bit keys are acceptable until 2030 per document NIST SP800-57 part 1 Rev 4.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.3** E:POC/RL:W/RC:C
Severity:	**3**
QID:	38657
Category:	General remote services
CVE ID:	CVE-2016-2183
Vendor Reference:	-
Bugtraq ID:	92630, 95568
Last Update:	2021-09-20 15:31:22.0

THREAT:

Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

Note: This CVE is patched at following versions

OPENSSL-0.9.8J-0.102.2

LIBOPENSSL0_9_8-0.9.8J-0.102.2

LIBOPENSSL0_9_8-32BIT-0.9.8J-0.102.2

OPENSSL1-1.0.1G-0.52.1

OPENSSL1-DOC-1.0.1G-0.52.1

LIBOPENSSL1_0_0-1.0.1G-0.52.1

LIBOPENSSL1-DEVEL-1.0.1G-0.52.1

JAVA-1_6_0-IBM-1.6.0_SR16.41-81.1

IMPACT:

Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:

Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

More information can be found at Sweet32, Microsoft Windows TLS changes docs and Microsoft Transport Layer Security (TLS) registry settings

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ADH-DES-CBC3-SHA	DH	None	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM

Path-Based Vulnerability — port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.1** AV:L/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**1.9** E:F/RL:W/RC:C
Severity:	**2**
QID:	150004
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Last Update:	2021-09-21 01:03:33.0

THREAT:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i. e. Explicit URI) this same link will no longer be reported for 150004.

IMPACT:
The contents of this file or directory may disclose sensitive information.

SOLUTION:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

RESULT:
url: https://server.northerngreenexpo.org:2096/
Payload: http://server.northerngreenexpo.org/webmail/
comment: Found this Vulnerability for redirect link: https://server.northerngreenexpo.org:2096/. It was redirected from: http://server.northerngreenexpo.org/webmail/.

Original URL is: http://server.northerngreenexpo.org/

matched: HTTP/1.1 200 OK

Path-Based Vulnerability — port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.1** AV:L/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**1.9** E:F/RL:W/RC:C
Severity:	**2**
QID:	150004
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-09-21 01:03:33.0

THREAT:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i. e. Explicit URI) this same link will no longer be reported for 150004.

IMPACT:
The contents of this file or directory may disclose sensitive information.

SOLUTION:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

RESULT:
url: https://northerngreen.org/wp-includes/SimplePie/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/SimplePie</title>
</head>
<body>
<h1>Index of /wp-includes/SimplePie</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Direct

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th

url: https://northerngreen.org/wp-login.php?redirect_to=https%3A%2F%2Fnortherngreen.org%2Fwp-admin%2Fadmin.php&reauth=1
Payload: https://northerngreen.org/wp-admin/admin.php
comment: Found this Vulnerability for redirect link: https://northerngreen.org/wp-login.php?redirect_to=https%3A%2F%2Fnortherngreen.org%2Fwp-admin%2Fadmin.
php&reauth=1. It was redirected from: https://northerngreen.org/wp-admin/admin.php.

Original URL is: https://northerngreen.org/wp-admin/

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<

/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><

url: https://northerngreen.org/wp-content/uploads/2016/08/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads/2016/08</title>
</head>
<body>
<h1>Index of /wp-content/uploads/2016/08</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-content/upload

url: https://northerngreen.org/wp-includes/images/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/images</title>
</head>
<body>
<h1>Index of /wp-includes/images</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Directory</a

url: https://northerngreen.org/wp-includes/js/dist/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/dist</title>
</head>
<body>
<h1>Index of /wp-includes/js/dist</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent Directo

url: https://northerngreen.org/wp-includes/css/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

<html>
<head>
<title>Index of /wp-includes/css</title>
</head>
<body>
<h1>Index of /wp-includes/css</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/Text/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/Text</title>
</head>
<body>
<h1>Index of /wp-includes/Text</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/customize/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/customize</title>
</head>
<body>
<h1>Index of /wp-includes/customize</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Direct

url: https://northerngreen.org/wp-admin/images/
Payload: https://northerngreen.org/wp-admin/images/
comment:
Original URL is: https://northerngreen.org/wp-admin/

matched: HTTP/1.1 200 OK

url: http://northerngreen.org/internet/
Payload: http://northerngreen.org/internet/
comment:
Original URL is: http://northerngreen.org/

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-includes/blocks/image/
Payload: https://northerngreen.org/wp-includes/blocks/image/
comment:
Original URL is: https://northerngreen.org/wp-includes/blocks/

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-includes/js/jquery/ui/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/jquery/ui</title>
</head>
<body>
<h1>Index of /wp-includes/js/jquery/ui</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/jquery

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td

url: https://northerngreen.org/wp-content/uploads/fusion-scripts/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads/fusion-scripts</title>
</head>
<body>
<h1>Index of /wp-content/uploads/fusion-scripts</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-

url: https://northerngreen.org/wp-admin/includes/
Payload: https://northerngreen.org/wp-admin/includes/
comment:
Original URL is: https://northerngreen.org/wp-admin/

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-admin/css/
Payload: https://northerngreen.org/wp-admin/css/
comment:
Original URL is: https://northerngreen.org/wp-admin/

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-includes/js/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js</title>
</head>
<body>
<h1>Index of /wp-includes/js</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/our-activities/classes/
Payload: http://northerngreen.org/classes/
comment: Found this Vulnerability for redirect link: https://northerngreen.org/our-activities/classes/. It was redirected from: http://northerngreen.org/classes/.

Original URL is: http://northerngreen.org/

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-admin/js/widgets/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/js/widgets</title>
</head>
<body>
<h1>Index of /wp-admin/js/widgets</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-admin/js/">Parent Directory<

url: https://northerngreen.org/wp-includes/block-supports/.

comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/block-supports</title>
</head>
<body>
<h1>Index of /wp-includes/block-supports</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Par

url: https://northerngreen.org/wp-content/uploads/2021/11/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads/2021/11</title>
</head>
<body>
<h1>Index of /wp-content/uploads/2021/11</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-content/upload

url: https://northerngreen.org/wp-includes/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes</title>
</head>
<body>
<h1>Index of /wp-includes</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory </td><td> </t

url: https://northerngreen.org/wp-content/uploads/2021/06/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads/2021/06</title>
</head>
<body>

<h1>Index of /wp-content/uploads/2021/06</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-content/upload

url: https://northerngreen.org/wp-content/uploads/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads</title>
</head>
<body>
<h1>Index of /wp-content/uploads</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-admin/js/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/js</title>
</head>
<body>
<h1>Index of /wp-admin/js</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory </td><td>

Sensitive form field has not disabled autocomplete — port 2082 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: **0** AV:N/AC:L/Au:S/C:N/I:N/A:N

CVSS Temporal Score: **0** E:POC/RL:U/RC:C

Severity:	**2**
QID:	150112
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-10-06 22:01:46.0

THREAT:
An HTML form that collects sensitive information does not prevent the browser from prompting the user to save the populated values for later reuse. Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:
If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be submitted by an unauthorized user.

SOLUTION:
Add the following attribute to the form or input element: autocomplete="off" This attribute prevents the browser from prompting the user to save the populated form values for later reuse. Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment. Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:
url: http://server.northerngreenexpo.org:2082/login/
Payload: N/A
matched: The following password field(s) in the form do not set autocomplete="off":
(Field name: pass, Field id: pass)
Parent URL of form is: http://server.northerngreenexpo.org:2082/

UDP Constant IP Identification Field Fingerprinting Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS — ASV Score = 0. The information obtained (i.e. operating system name) is not relevant to PCI.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.8** E:H/RL:U/RC:UR
Severity:	**2**
QID:	82024
Category:	TCP/IP
CVE ID:	CVE-2002-0510
Vendor Reference:	-
Bugtraq ID:	4314
Last Update:	2008-05-07 18:23:49.0

THREAT:
The host transmits UDP packets with a constant IP Identification field. This behavior may be exploited to discover the operating system and approximate kernel version of the vulnerable system.

Normally, the IP Identification field is intended to be a reasonably unique value, and is used to reconstruct fragmented packets. It has been reported that in some versions of the Linux kernel IP stack implementation as well as other operating systems, UDP packets are transmitted with a constant IP Identification field of 0.

IMPACT:
By exploiting this vulnerability, a malicious user can discover the operating system and approximate kernel version of the host. This information can then be used in further attacks against the host.

SOLUTION:
We are not currently aware of any fixes for this issue.

RESULT:
IP_ID=0

Sensitive form field has not disabled autocomplete — port 2095 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**0** AV:N/AC:L/Au:S/C:N/I:N/A:N
CVSS Temporal Score:	**0** E:POC/RL:U/RC:C
Severity:	**2**
QID:	150112
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-10-06 22:01:46.0

THREAT:
An HTML form that collects sensitive information does not prevent the browser from prompting the user to save the populated values for later reuse. Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:
If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be submitted by an unauthorized user.

SOLUTION:
Add the following attribute to the form or input element: autocomplete="off" This attribute prevents the browser from prompting the user to save the populated form values for later reuse. Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment. Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:
url: http://server.northerngreenexpo.org:2095/login/
Payload: N/A
matched: The following password field(s) in the form do not set autocomplete="off":

(Field name: pass, Field id: pass)
Parent URL of form is: http://server.northerngreenexpo.org:2095/

Sensitive form field has not disabled autocomplete — port 2086 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**0** AV:N/AC:L/Au:S/C:N/I:N/A:N
CVSS Temporal Score:	**0** E:POC/RL:U/RC:C
Severity:	**2**
QID:	150112
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-10-06 22:01:46.0

THREAT:
An HTML form that collects sensitive information does not prevent the browser from prompting the user to save the populated values for later reuse. Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:
If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be submitted by an unauthorized user.

SOLUTION:
Add the following attribute to the form or input element: autocomplete="off" This attribute prevents the browser from prompting the user to save the populated form values for later reuse. Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment. Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:
url: http://server.northerngreenexpo.org:2086/login/
Payload: N/A
matched: The following password field(s) in the form do not set autocomplete="off":
(Field name: pass, Field id: pass)
Parent URL of form is: http://server.northerngreenexpo.org:2086/

AutoComplete Attribute Not Disabled for Password in Form Based Authentication — port 2095 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.0** E:U/RL:U/RC:UC
Severity:	**2**
QID:	86729
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-01 13:30:46.0

THREAT:

The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be retrieved or submitted by an unauthorized user.

SOLUTION:

Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

Developers can add the following attribute to the form or input element: autocomplete="off"
This attribute prevents the browser from prompting the user to save the populated form values for later reuse.
Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera
However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment.
Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:

GET /admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2095

<form novalidate id="login_form" action="/login/" method="post" target="_self" style="visibility:">
<label for="user">Email Address</label>

<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your email address." class="std_textbox" type="text" tabindex="1" required>

<label for="pass">Password</label>

<input name="pass" id="pass" placeholder="Enter your email password." class="std_textbox" type="password" tabindex="2" required>

<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>

</form>

GET /w3-msql/index.html HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /session/adminlogin HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /default.asp\ HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /loadpage.cgi?user_id=id&file=/ HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /commerce.cgi?page=../../../../../etc/passwd%00index.html HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /commerce.cgi?page=../../../../../../windows/system32/drivers/etc/hosts%00index.html HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /index.php3 HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/.htaccess HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/nph-publish HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/nph-publish.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/pagelog.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /nph-maillist.pl HTTP/1.0
Host: server.northerngreenexpo.org:2095

POST /login/newsup.pl HTTP/1.0
Host: server.northerngreenexpo.org:2095
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++POST /login/newsup.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2095
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++GET /login/subscribe.pl HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /login/whois.cgi?action=load&whois=%3Bcat+%2Fetc%2Fpasswd HTTP/1.0
Host: server.northerngreenexpo.org:2095

GET /stats.php HTTP/1.0

Host: server.northerngreenexpo.org:2095

GET /login/gbook.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2095

Path-Based Vulnerability — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.1** AV:L/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**1.9** E:F/RL:W/RC:C
Severity:	**2**
QID:	150004
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-09-21 01:03:33.0

THREAT:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i. e. Explicit URI) this same link will no longer be reported for 150004.

IMPACT:
The contents of this file or directory may disclose sensitive information.

SOLUTION:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

RESULT:
url: https://northerngreen.org/wp-includes/SimplePie/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/SimplePie</title>
</head>
<body>
<h1>Index of /wp-includes/SimplePie</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>

<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Direct

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th

url: https://northerngreen.org/wp-login.php?redirect_to=https%3A%2F%2Fnortherngreen.org%2Fwp-admin%2Fadmin.php&reauth=1
Payload: https://northerngreen.org/wp-admin/admin.php
comment: Found this Vulnerability for redirect link: https://northerngreen.org/wp-login.php?redirect_to=https%3A%2F%2Fnortherngreen.org%2Fwp-admin%2Fadmin.
php&reauth=1. It was redirected from: https://northerngreen.org/wp-admin/admin.php.

Original URL is: https://northerngreen.org/wp-admin/

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><

url: https://northerngreen.org/wp-content/uploads/2016/08/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads/2016/08</title>
</head>
<body>
<h1>Index of /wp-content/uploads/2016/08</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>

<tr><td valign="top"> </td><td><a href="/wp-content/upload

url: https://northerngreen.org/wp-includes/images/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/images</title>
</head>
<body>
<h1>Index of /wp-includes/images</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Directory</a

url: https://northerngreen.org/wp-includes/js/dist/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/dist</title>
</head>
<body>
<h1>Index of /wp-includes/js/dist</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/">Parent Directo

url: https://northerngreen.org/wp-includes/css/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/css</title>
</head>
<body>
<h1>Index of /wp-includes/css</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/Text/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>

<title>Index of /wp-includes/Text</title>
</head>
<body>
<h1>Index of /wp-includes/Text</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-includes/customize/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/customize</title>
</head>
<body>
<h1>Index of /wp-includes/customize</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Parent Direct

url: https://northerngreen.org/wp-admin/images/
Payload: https://northerngreen.org/wp-admin/images/
comment:
Original URL is: https://northerngreen.org/wp-admin/

matched: HTTP/1.1 200 OK

url: http://northerngreen.org/internet/
Payload: http://northerngreen.org/internet/
comment:
Original URL is: http://northerngreen.org/?sid=1&bsa_pro_id=12&bsa_pro_url=1

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-includes/blocks/image/
Payload: https://northerngreen.org/wp-includes/blocks/image/
comment:
Original URL is: https://northerngreen.org/wp-includes/blocks/

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-includes/js/jquery/ui/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js/jquery/ui</title>
</head>
<body>

<h1>Index of /wp-includes/js/jquery/ui</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/js/jquery

url: https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js</title>
</head>
<body>
<h1>Index of /wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td

url: https://northerngreen.org/wp-content/uploads/fusion-scripts/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads/fusion-scripts</title>
</head>
<body>
<h1>Index of /wp-content/uploads/fusion-scripts</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-

url: https://northerngreen.org/wp-admin/includes/
Payload: https://northerngreen.org/wp-admin/includes/
comment:
Original URL is: https://northerngreen.org/wp-admin/

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-admin/css/
Payload: https://northerngreen.org/wp-admin/css/
comment:
Original URL is: https://northerngreen.org/wp-admin/

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-includes/js/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/js</title>
</head>
<body>
<h1>Index of /wp-includes/js</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/wp-admin/js/widgets/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/js/widgets</title>
</head>
<body>
<h1>Index of /wp-admin/js/widgets</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-admin/js/">Parent Directory<

url: https://northerngreen.org/wp-includes/block-supports/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes/block-supports</title>
</head>
<body>
<h1>Index of /wp-includes/block-supports</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-includes/">Par

url: https://northerngreen.org/wp-content/uploads/2021/11/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads/2021/11</title>
</head>
<body>
<h1>Index of /wp-content/uploads/2021/11</h1>
<table>

<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-content/upload

url: https://northerngreen.org/wp-includes/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-includes</title>
</head>
<body>
<h1>Index of /wp-includes</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory </td><td> </t

url: https://northerngreen.org/wp-content/uploads/2021/06/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads/2021/06</title>
</head>
<body>
<h1>Index of /wp-content/uploads/2021/06</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td><a href="/wp-content/upload

url: https://northerngreen.org/wp-content/uploads/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-content/uploads</title>
</head>
<body>
<h1>Index of /wp-content/uploads</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory

url: https://northerngreen.org/our-activities/classes/
Payload: https://northerngreen.org/classes/
comment: Found this Vulnerability for redirect link: https://northerngreen.org/our-activities/classes/. It was redirected from: https://northerngreen.org/classes/.

Original URL is: https://northerngreen.org/

matched: HTTP/1.1 200 OK

url: https://northerngreen.org/wp-admin/js/.
comment: This directory was discovered during the crawl phase.

matched: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /wp-admin/js</title>
</head>
<body>
<h1>Index of /wp-admin/js</h1>
<table>
<tr><th valign="top"> </th><th>Name</th><th>Last modified</th><th>Size<
/th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"> </td><td>Parent Directory </td><td>

Path-Based Vulnerability — port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.1** AV:L/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**1.9** E:F/RL:W/RC:C
Severity:	**2**
QID:	150004
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-09-21 01:03:33.0

THREAT:
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i. e. Explicit URI) this same link will no longer be reported for 150004.

IMPACT:
The contents of this file or directory may disclose sensitive information.

SOLUTION:
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

RESULT:
url: https://server.northerngreenexpo.org:2096/
Payload: https://server.northerngreenexpo.org/webmail/
comment: Found this Vulnerability for redirect link: https://server.northerngreenexpo.org:2096/. It was redirected from: https://server.northerngreenexpo.org/webmail/.

Original URL is: https://server.northerngreenexpo.org/

matched: HTTP/1.1 200 OK

AutoComplete Attribute Not Disabled for Password in Form Based Authentication — port 2082 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.0** E:U/RL:U/RC:UC
Severity:	**2**
QID:	86729
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-01 13:30:46.0

THREAT:
The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:
If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be retrieved or submitted by an unauthorized user.

SOLUTION:
Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

Developers can add the following attribute to the form or input element: autocomplete="off"
This attribute prevents the browser from prompting the user to save the populated form values for later reuse.
Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera
However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment.
Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:
GET /admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2082

<form novalidate id="login_form" action="/login/" method="post" target="_self" style="visibility:">
<label for="user">Username</label>

<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your username." class="std_textbox" type="text" tabindex="1" required>

<label for="pass">Password</label>

<input name="pass" id="pass" placeholder="Enter your account password." class="std_textbox" type="password" tabindex="2" required>

<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>

</form>

GET /login/admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/.htaccess HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/nph-publish HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/nph-publish.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/pagelog.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082

POST /login/newsup.pl HTTP/1.0
Host: server.northerngreenexpo.org:2082
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++POST /login/newsup.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++GET /login/subscribe.pl HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/whois.cgi?action=load&whois=%3Bcat+%2Fetc%2Fpasswd HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/gbook.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/cgiforum.pl?thesection=../../../../../../etc/passwd%00 HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/cgiforum.cgi?thesection=../../../../../../etc/passwd%00 HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/bigconf.cgi?command=view_textfile&file=/etc/passwd&filters=; HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/QUALYS10197RSBD.pl HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/cachemgr.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/bb-hist.sh?HISTFILE=/home/* HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/unlg1.1 HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/unlg1.2 HTTP/1.0
Host: server.northerngreenexpo.org:2082

GET /login/AT-generate.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2082

AutoComplete Attribute Not Disabled for Password in Form Based Authentication — port 2086 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.0** E:U/RL:U/RC:UC
Severity:	**2**
QID:	86729
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-01 13:30:46.0

THREAT:

The Web server allows form based authentication without disabling the AutoComplete feature for the password field.

Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:
If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be retrieved or submitted by an unauthorized user.
SOLUTION:
Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.

Developers can add the following attribute to the form or input element: autocomplete="off"
This attribute prevents the browser from prompting the user to save the populated form values for later reuse.
Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera
However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment.
Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.
RESULT:
GET /admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2086

<form novalidate id="login_form" action="/login/" method="post" target="_self" style="visibility:">
<label for="user">Username</label>

<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your username." class="std_textbox" type="text" tabindex="1" required>

<label for="pass">Password</label>

<input name="pass" id="pass" placeholder="Enter your account password." class="std_textbox" type="password" tabindex="2" required>

<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>

</form>

GET /w3-msql/index.html HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /session/adminlogin HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/admin.php3?admin=YmxhYmxhOg%3D%3D&op=mod_authors HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/.htaccess HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/nph-publish HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/nph-publish.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/pagelog.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2086

POST /login/newsup.pl HTTP/1.0
Host: server.northerngreenexpo.org:2086
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++POST /login/newsup.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2086
Content-type: application/x-www-form-urlencoded
Content-Length: 68

password=NeIn&picdesc=titi&update=super&parse=Update+News&%24date=++GET /login/subscribe.pl HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/whois.cgi?action=load&whois=%3Bcat+%2Fetc%2Fpasswd HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/gbook.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /default.asp\ HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/cgiforum.pl?thesection=../../../../../../etc/passwd%00 HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /loadpage.cgi?user_id=id&file=/ HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/cgiforum.cgi?thesection=../../../../../../etc/passwd%00 HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/bigconf.cgi?command=view_textfile&file=/etc/passwd&filters=; HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/QUALYS10197RSBD.pl HTTP/1.0
Host: server.northerngreenexpo.org:2086

GET /login/cachemgr.cgi HTTP/1.0
Host: server.northerngreenexpo.org:2086

ICMP Timestamp Request

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score: **0** AV:L/AC:L/Au:N/C:N/I:N/A:N

CVSS Temporal Score:	**0** E:F/RL:W/RC:C
Severity:	**1**
QID:	82003
Category:	TCP/IP
CVE ID:	CVE-1999-0524
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-04-29 03:59:17.0

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:
You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the *Ping of Death* or *Smurf* attacks.

However, you should never filter **ALL** ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

RESULT:
Timestamp of host (network byte ordering): 12:23:00 GMT

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)

port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.2** E:U/RL:U/RC:C
Severity:	**1**
QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:12:51.0

THREAT:
The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.

This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:
Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1_1 If the test is successful, then the target support TLSv1.1

RESULT:
TLSv1.1 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)

port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.2** E:U/RL:U/RC:C
Severity:	**1**
QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:12:51.0

THREAT:
The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.

This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:
Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1_1 If the test is successful, then the target support TLSv1.1

RESULT:
TLSv1.1 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)

port 26 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.2** E:U/RL:U/RC:C
Severity:	**1**
QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:12:51.0

THREAT:
The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.

This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:
Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1_1 If the test is successful, then the target support TLSv1.1

RESULT:
TLSv1.1 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)

port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.2** E:U/RL:U/RC:C
Severity:	**1**
QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:12:51.0

THREAT:

The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.

This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:

Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:

Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1_1 If the test is successful, then the target support TLSv1.1

RESULT:

TLSv1.1 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)

port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.2** E:U/RL:U/RC:C

Severity:	**1**
QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:12:51.0

THREAT:
The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.

This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:
Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1_1 If the test is successful, then the target support TLSv1.1

RESULT:
TLSv1.1 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)

port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.2** E:U/RL:U/RC:C
Severity:	**1**
QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:12:51.0

THREAT:
The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.

This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:
Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1_1 If the test is successful, then the target support TLSv1.1

RESULT:
TLSv1.1 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)

port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level:	LOW
PASS	The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.2** E:U/RL:U/RC:C
Severity:	**1**
QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:12:51.0

THREAT:
The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.

This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:
Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1_1 If the test is successful, then the target support TLSv1.1

RESULT:
TLSv1.1 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)
port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.2** E:U/RL:U/RC:C
Severity:	**1**
QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:12:51.0

THREAT:
The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.

This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:
Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1_1 If the test is successful, then the target support TLSv1.1

RESULT:
TLSv1.1 is supported

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)
port 587 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.2** E:U/RL:U/RC:C
Severity:	**1**
QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2021-07-12 22:12:51.0

THREAT:

The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.

This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:

Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:

Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1_1 If the test is successful, then the target support TLSv1.1

RESULT:

TLSv1.1 is supported

Potential Vulnerabilities (20)

ISC BIND DDNS Privilege Escalation Vulnerability(cve-2018-5741) — port 53 / udp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**4** AV:N/AC:L/Au:S/C:N/I:P/A:N

CVSS Temporal Score:	**3** E:U/RL:OF/RC:C
Severity:	**3**
QID:	15111
Category:	DNS and BIND
CVE ID:	CVE-2018-5741
Vendor Reference:	cve-2018-5741
Bugtraq ID:	-
Last Update:	2020-05-18 13:20:21.0

THREAT:
ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
Affected Software:
BIND 9 prior to releases, BIND 9.11.5 and 9.12.3.

QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:
Malicious users could use this vulnerability to change partial contents or configuration on the system.

SOLUTION:
Customers are advised to upgrade to the latest supported version of ISC BIND.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

ISC BIND

RESULT:
Vulnerable ISC BIND - 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 detected on port 53 over UDP.

OpenSSH J-PAKE Session Key Retrieval Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**7.5** AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	**5.5** E:U/RL:OF/RC:C
Severity:	**3**
QID:	42384
Category:	General remote services
CVE ID:	CVE-2010-4478
Vendor Reference:	OpenSSH J-PAKE
Bugtraq ID:	45304
Last Update:	2021-06-16 12:29:48.0

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

OpenSSH, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol. This allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.

Affected Software:
OpenSSH versions 5.6 and prior.

IMPACT:
Successful exploitation allows attacker to get access to the remote system.

SOLUTION:
Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

OpenSSH J-PAKE

RESULT:
SSH-2.0-OpenSSH_5.3

Web Server Stopped Responding — port 2095 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**6.4** AV:N/AC:L/Au:N/C:N/I:P/A:P
CVSS Temporal Score:	**6.1** E:H/RL:W/RC:C
Severity:	**3**
QID:	86476
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-02-28 20:51:45.0

THREAT:
The Web server stopped responding to 3 consecutive connection attempts and/or more than 3 consecutive HTTP / HTTPS requests. Consequently, the service aborted testing for HTTP / HTTPS vulnerabilities. The vulnerabilities already detected are still posted.

IMPACT:
The service was unable to complete testing for HTTP / HTTPS vulnerabilities since the Web server stopped responding.

SOLUTION:
Check the Web server status.

If the Web server was crashed during the scan, please restart the server, report the incident to Customer Support and stop scanning the Web server until the issue is resolved.

If the Web server is unable to process multiple concurrent HTTP / HTTPS requests, please lower the scan harshness level and launch another scan. If this vulnerability continues to be reported, please contact Customer Support.

RESULT:
The web server did not respond for 4 consecutive HTTP requests.

After these, the service was still unable to connect to the web server 2 minutes later.

ISC BIND DDNS Privilege Escalation Vulnerability(cve-2018-5741) — port 53 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**4** AV:N/AC:L/Au:S/C:N/I:P/A:N
CVSS Temporal Score:	**3** E:U/RL:OF/RC:C
Severity:	**3**
QID:	15111
Category:	DNS and BIND
CVE ID:	CVE-2018-5741
Vendor Reference:	cve-2018-5741
Bugtraq ID:	-
Last Update:	2020-05-18 13:20:21.0

THREAT:
ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
Affected Software:
BIND 9 prior to releases, BIND 9.11.5 and 9.12.3.

QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:
Malicious users could use this vulnerability to change partial contents or configuration on the system.

SOLUTION:
Customers are advised to upgrade to the latest supported version of ISC BIND.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

ISC BIND

RESULT:
Vulnerable ISC BIND - 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 detected on port 53 over TCP.

Database Instance Detected — port 3306 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Open access to databases from the Internet

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.8** E:U/RL:U/RC:UC
Severity:	**2**
QID:	19568
Category:	Database
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-12-03 07:29:16.0

THREAT:

The service detected a database installation on the target. Databases like Oracle, MS-SQL, MySQL, IBM DB2, PostGgresql, Firebird and other are detected. The database instance is listed in the result section below.

IMPACT:

Information disclosing database type will lead attacker to perform more targeted attacks.

SOLUTION:

Users are recommended to encrypt the database information and handle the situations where any error is leading to disclose some sensitive information like database type and its version.

RESULT:

MYSQL server instance detected

Global User List Found Using Other QIDS

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Built-in or default accounts and passwords

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**4.8** E:H/RL:W/RC:C
Severity:	**2**
QID:	45002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-11-23 09:43:19.0

THREAT:

This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities or via authentication provided by user. The Qualys IDs for

the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.

Note: We did not exploit any vulnerabilities to gather this information in QID 90266, 45027 or 45032.

IMPACT:
These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:
To prevent your host from being attacked, do one or more of the following:

- Remove (or rename) unnecessary accounts
- Shutdown unnecessary network services
- Ensure the passwords to these accounts are kept secret
- Use a firewall to restrict access to your hosts from unauthorized domains

RESULT:

User Name	Source Vulnerability (QualysID)
root	5001
operator	5001

ISC BIND Query Processing Denial of Service Vulnerability — port 53 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

PASS — The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** AV:N/AC:L/Au:N/C:N/I:N/A:C
CVSS Temporal Score:	**6.1** E:POC/RL:OF/RC:C
Severity:	**4**
QID:	15083
Category:	DNS and BIND
CVE ID:	CVE-2012-4244
Vendor Reference:	ISC BIND CVE-2012-4244
Bugtraq ID:	55522
Last Update:	2013-04-16 18:40:20.0

THREAT:
ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.

If a record with RDATA in excess of 65535 bytes is loaded into a nameserver, a subsequent query for that record will cause named to exit with an assertion failure.

Affected Software:
BIND 9.x before 9.7.6-P3
BIND 9.8.x before 9.8.3-P3
BIND 9.9.x before 9.9.1-P3

BIND 9.4-ESV before 9.4-ESV-R5-P1
BIND 9.6-ESV before 9.6-ESV-R7-P3

IMPACT:
This vulnerability can be exploited remotely against recursive servers by inducing them to query for records provided by an authoritative server. It affects authoritative servers if a zone containing this type of resource record is loaded from file or provided via zone transfer.

SOLUTION:
Vendor has released updated patches to resolve this issue.Refer to ISC BIND CVE-2012-4244 to address this issue and obtain details on the fixes.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

ISC Bind cve-2012-4244

RESULT:
9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8

ISC BIND DNS64 REQUIRE Assertion Failure Denial of Service Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level:	HIGH
PASS	The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** AV:N/AC:L/Au:N/C:N/I:N/A:C
CVSS Temporal Score:	**5.8** E:U/RL:OF/RC:C
Severity:	**3**
QID:	15078
Category:	DNS and BIND
CVE ID:	CVE-2012-5688
Vendor Reference:	ISC CVE-2012-5688
Bugtraq ID:	-
Last Update:	2012-12-06 21:56:34.0

THREAT:
ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.

The software is exposed to a security vulnerability which is caused due to an error in the DNS64 IPv6 transition mechanism.

Affected Software:
ISC BIND versions 9.8.0 through 9.8.4 and 9.9.0 through 9.9.2.

IMPACT:
Successful exploitation allows attackers cause a denial of dervice.

SOLUTION:
The vendor has released advisories and updates to fix these vulnerabilities. Refer to the following link for further details: CVE-2012-5688

Patch:
Following are links for downloading patches to fix the vulnerabilities:

ISC CVE-2012-5688 (BIND 9 version 9.8.4-P1)

ISC CVE-2012-5688 (BIND 9 version 9.9.2-P1)

RESULT:
9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8

Host is Vulnerable to Extended Master Secret TLS Extension (TLS triple handshake) — port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.1** E:U/RL:W/RC:C
Severity:	**3**
QID:	13607
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-12-03 04:37:54.0

THREAT:
The Transport Layer Security (TLS) master secret is not cryptographically bound to important session parameters such as the server certificate. Consequently, it is possible for an active attacker to set up two sessions, one with a client and another with a server, such that the master secrets on the two sessions are the same.

Note: this attacks are reminiscent of the renegotiation attacks of 2009 [Ray, Rex] (CVE-2009-3555).

QID Detection Logic(Un-Authenticated):
This QID checks for web response coming from vulnerable host.

Note:Please refer Detection POC for more details of the detection logic

IMPACT:
On successful exploitation it becomes vulnerable to a man-in-the-middle attack, where the attacker can simply forward messages back and forth between the client and server.

SOLUTION:
Refer to the Workarounds available.

Workaround:
To re-mediate this vulnerability these bug workaround options are available.

RESULT:
Host:162.144.102.68:2087 is vulnerable to TLS triple handshake

ISC BIND Assertion Failure Vulnerability — port 53 / udp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	**4** AV:N/AC:L/Au:S/C:N/I:N/A:P
CVSS Temporal Score:	**3** E:U/RL:OF/RC:C
Severity:	**3**
QID:	15120
Category:	DNS and BIND
CVE ID:	CVE-2020-8622
Vendor Reference:	BIND cve-2020-8622
Bugtraq ID:	-
Last Update:	2020-12-07 12:09:46.0

THREAT:
ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.

Affected software:
BIND 9.0.0 -> 9.11.21
BIND 9.12.0 -> 9.16.5
BIND 9.17.0 -> 9.17.3
BIND 9.9.3-S1 -> 9.11.21-S1

Patched version:
BIND 9.11.22
BIND 9.16.6
BIND 9.17.4
BIND 9.11.22-S1

QID Detection Logic:
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:
An attacker on the network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that request, triggering an assertion failure, causing the server to exit.

SOLUTION:
Customers are advised to upgrade to the patched version 9.11.22, 9.16.6, 9.17.4, 9.11.22-S1 or latest release of ISC BIND.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

cve-2020-8622

RESULT:
Vulnerable ISC BIND - 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 detected on port 53 over TCP.

Host is Vulnerable to Extended Master Secret TLS Extension (TLS triple handshake) port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.1** E:U/RL:W/RC:C
Severity:	**3**
QID:	13607
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-12-03 04:37:54.0

THREAT:
The Transport Layer Security (TLS) master secret is not cryptographically bound to important session parameters such as the server certificate. Consequently, it is possible for an active attacker to set up two sessions, one with a client and another with a server, such that the master secrets on the two sessions are the same.

Note: this attacks are reminiscent of the renegotiation attacks of 2009 [Ray, Rex] (CVE-2009-3555).

QID Detection Logic(Un-Authenticated):
This QID checks for web response coming from vulnerable host.

Note:Please refer Detection POC for more details of the detection logic

IMPACT:
On successful exploitation it becomes vulnerable to a man-in-the-middle attack, where the attacker can simply forward messages back and forth between the client and server.

SOLUTION:
Refer to the Workarounds available.

Workaround:
To re-mediate this vulnerability these bug workaround options are available.

RESULT:
Host:162.144.102.68:465 is vulnerable to TLS triple handshake

Host is Vulnerable to Extended Master Secret TLS Extension (TLS triple handshake) port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.1** E:U/RL:W/RC:C
Severity:	**3**
QID:	13607
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-12-03 04:37:54.0

THREAT:
The Transport Layer Security (TLS) master secret is not cryptographically bound to important session parameters such as the server certificate. Consequently, it is possible for an active attacker to set up two sessions, one with a client and another with a server, such that the master secrets on the two sessions are the same.

Note: this attacks are reminiscent of the renegotiation attacks of 2009 [Ray, Rex] (CVE-2009-3555).

QID Detection Logic(Un-Authenticated):
This QID checks for web response coming from vulnerable host.

Note:Please refer Detection POC for more details of the detection logic

IMPACT:
On successful exploitation it becomes vulnerable to a man-in-the-middle attack, where the attacker can simply forward messages back and forth between the client and server.

SOLUTION:
Refer to the Workarounds available.

Workaround:
To re-mediate this vulnerability these bug workaround options are available.

RESULT:
Host:162.144.102.68:2078 is vulnerable to TLS triple handshake

Host is Vulnerable to Extended Master Secret TLS Extension (TLS triple handshake) port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.1** E:U/RL:W/RC:C
Severity:	**3**
QID:	13607
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-12-03 04:37:54.0

THREAT:
The Transport Layer Security (TLS) master secret is not cryptographically bound to important session parameters such as the server certificate. Consequently, it is possible for an active attacker to set up two sessions, one with a client and another with a server, such that the master secrets on the two sessions are the same.

Note: this attacks are reminiscent of the renegotiation attacks of 2009 [Ray, Rex] (CVE-2009-3555).

QID Detection Logic(Un-Authenticated):
This QID checks for web response coming from vulnerable host.

Note:Please refer Detection POC for more details of the detection logic

IMPACT:
On successful exploitation it becomes vulnerable to a man-in-the-middle attack, where the attacker can simply forward messages back and forth between the client and server.
SOLUTION:
Refer to the Workarounds available.

Workaround:
To re-mediate this vulnerability these bug workaround options are available.
RESULT:
Host:162.144.102.68:2083 is vulnerable to TLS triple handshake

ISC BIND NXNSAttack Vulnerability — port 53 / udp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS — The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Temporal Score:	**3.9** E:POC/RL:OF/RC:C
Severity:	**3**
QID:	15114
Category:	DNS and BIND
CVE ID:	CVE-2020-8617, CVE-2020-8616
Vendor Reference:	CVE-2020-8616,CVE-2020-8617
Bugtraq ID:	-
Last Update:	2020-06-10 12:27:59.0

THREAT:
ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. This has at least two potential effects: The performance of the recursing server can potentially be degraded by the additional work required to perform these fetches, and The attacker can exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor.

Affected Software:
BIND 9.4.0-to 9.8.8 .
BIND 9.0.0 -> 9.11.18, 9.12.0 -> 9.12.4-P2, 9.14.0 -> 9.14.11, 9.16.0 -> 9.16.2, and releases 9.17.0 -> 9.17.1 of the 9.17

QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:
A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals.
SOLUTION:
Customers are advised to upgrade to the latest supported version of ISC BIND.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2020-8617, CVE-2020-8616

RESULT:
Vulnerable ISC BIND - 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 detected on port 53 over UDP.

ISC BIND NXNSAttack Vulnerability — port 53 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS — The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	**5** AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Temporal Score:	**3.9** E:POC/RL:OF/RC:C
Severity:	**3**
QID:	15114
Category:	DNS and BIND
CVE ID:	CVE-2020-8617, CVE-2020-8616
Vendor Reference:	CVE-2020-8616,CVE-2020-8617
Bugtraq ID:	-
Last Update:	2020-06-10 12:27:59.0

THREAT:
ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.
A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. This has at least two potential effects: The performance of the recursing server can potentially be degraded by the additional work required to perform these fetches, and The attacker can exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor.

Affected Software:
BIND 9.4.0-to 9.8.8 .
BIND 9.0.0 -> 9.11.18, 9.12.0 -> 9.12.4-P2, 9.14.0 -> 9.14.11, 9.16.0 -> 9.16.2, and releases 9.17.0 -> 9.17.1 of the 9.17

QID Detection Logic (Unauthenticated):
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.

IMPACT:
A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals.

SOLUTION:
Customers are advised to upgrade to the latest supported version of ISC BIND.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2020-8617, CVE-2020-8616

RESULT:
Vulnerable ISC BIND - 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 detected on port 53 over TCP.

Host is Vulnerable to Extended Master Secret TLS Extension (TLS triple handshake) — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.1** E:U/RL:W/RC:C
Severity:	**3**
QID:	13607
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-12-03 04:37:54.0

THREAT:
The Transport Layer Security (TLS) master secret is not cryptographically bound to important session parameters such as the server certificate. Consequently, it is possible for an active attacker to set up two sessions, one with a client and another with a server, such that the master secrets on the two sessions are the same.

Note: this attacks are reminiscent of the renegotiation attacks of 2009 [Ray, Rex] (CVE-2009-3555).

QID Detection Logic(Un-Authenticated):
This QID checks for web response coming from vulnerable host.

Note:Please refer Detection POC for more details of the detection logic

IMPACT:
On successful exploitation it becomes vulnerable to a man-in-the-middle attack, where the attacker can simply forward messages back and forth between the client and server.

SOLUTION:
Refer to the Workarounds available.

Workaround:
To re-mediate this vulnerability these bug workaround options are available.

RESULT:
Host:162.144.102.68:2096 is vulnerable to TLS triple handshake

ISC BIND Assertion Failure Vulnerability — port 53 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS — The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	**4** AV:N/AC:L/Au:S/C:N/I:N/A:P
CVSS Temporal Score:	**3** E:U/RL:OF/RC:C
Severity:	**3**
QID:	15120
Category:	DNS and BIND
CVE ID:	CVE-2020-8622
Vendor Reference:	BIND cve-2020-8622
Bugtraq ID:	-
Last Update:	2020-12-07 12:09:46.0

THREAT:
ISC BIND (Berkley Internet Domain Name) is an implementation of DNS protocols.

Affected software:
BIND 9.0.0 -> 9.11.21
BIND 9.12.0 -> 9.16.5
BIND 9.17.0 -> 9.17.3
BIND 9.9.3-S1 -> 9.11.21-S1

Patched version:
BIND 9.11.22
BIND 9.16.6
BIND 9.17.4
BIND 9.11.22-S1

QID Detection Logic:
This unauthenticated check detects vulnerable systems by fetching the version information from the BIND service.
IMPACT:
An attacker on the network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that request, triggering an assertion failure, causing the server to exit.
SOLUTION:
Customers are advised to upgrade to the patched version 9.11.22, 9.16.6, 9.17.4, 9.11.22-S1 or latest release of ISC BIND.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

cve-2020-8622

RESULT:
Vulnerable ISC BIND - 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8 detected on port 53 over TCP.

Host is Vulnerable to Extended Master Secret TLS Extension (TLS triple handshake) — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS — The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.1** E:U/RL:W/RC:C
Severity:	**3**

QID:	13607
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-12-03 04:37:54.0

THREAT:
The Transport Layer Security (TLS) master secret is not cryptographically bound to important session parameters such as the server certificate. Consequently, it is possible for an active attacker to set up two sessions, one with a client and another with a server, such that the master secrets on the two sessions are the same.

Note: this attacks are reminiscent of the renegotiation attacks of 2009 [Ray, Rex] (CVE-2009-3555).

QID Detection Logic(Un-Authenticated):
This QID checks for web response coming from vulnerable host.

Note:Please refer Detection POC for more details of the detection logic

IMPACT:
On successful exploitation it becomes vulnerable to a man-in-the-middle attack, where the attacker can simply forward messages back and forth between the client and server.

SOLUTION:
Refer to the Workarounds available.

Workaround:
To re-mediate this vulnerability these bug workaround options are available.

RESULT:
Host:162.144.102.68:2080 is vulnerable to TLS triple handshake

OpenSSH Commands Information Disclosure Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**3.5** AV:N/AC:M/Au:S/C:P/I:N/A:N
CVSS Temporal Score:	**2.6** E:U/RL:OF/RC:C
Severity:	**3**
QID:	42382
Category:	General remote services
CVE ID:	CVE-2012-0814
Vendor Reference:	OpenSSH Forced Command Information Disclosure
Bugtraq ID:	51702
Last Update:	2020-07-18 03:30:52.0

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

Openssh-server could allow a remote attacker to obtain sensitive information because of the improper handling of forced commands.

IMPACT:
Only authenticated users can exploit this vulnerability to obtain usernames and other sensitive information.

SOLUTION:
Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

OpenSSH 5.7 (OpenSSH)

RESULT:
SSH-2.0-OpenSSH_5.3

OpenSSH Information Disclosure Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**2.1** AV:L/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**1.6** E:U/RL:OF/RC:C
Severity:	**2**
QID:	38788
Category:	General remote services
CVE ID:	CVE-2011-4327
Vendor Reference:	Openssh
Bugtraq ID:	-
Last Update:	2021-01-13 04:30:36.0

THREAT:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.

Affected Versions:
OpenSSH before 5.8p2

QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:
Successful exploitation could disclose sensitive information.

SOLUTION:
Customers are advised to upgrade to OpenSSH 5.8p2 or later to remediate these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

CVE-2011-4327

RESULT:
Vulnerable SSH-2.0-OpenSSH_5.3 detected on port 22 over TCP.

Information Gathered (292)

Content-Security-Policy HTTP Security Header Not Detected — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3
QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Last Update:	2019-03-11 17:50:46.0

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Content-Security-Policy HTTP Header missing on port 2086.
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2086

Remote Access or Management Service Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3
QID:	42017
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-02 13:31:47.0

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:
Service name: SSH on TCP port 22.
Service name: FTP on TCP port 21.

Content-Security-Policy HTTP Security Header Not Detected — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**3**
QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Last Update:	2019-03-11 17:50:46.0

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Content-Security-Policy HTTP Header missing on port 80.
GET / HTTP/1.0
Host: server.northerngreenexpo.org

MYSQL User Account Bruteforce Not Done Due to Denied Access — port 3306 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**3**
QID:	19087
Category:	Database
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-06-25 20:23:56.0

THREAT:

The scanner has been denied access to the MYSQL database on the host.

IMPACT:

The scanner is not able to perform user account bruteforcing against the database.

SOLUTION:

To grant access to the scanner, log onto the MYSQL host and enter the command "mysqladmin flush-hosts".

RESULT:

Host '64.39.98.8' is not allowed to connect to this MySQL server

Content-Security-Policy HTTP Security Header Not Detected — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**3**
QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Last Update:	2019-03-11 17:50:46.0

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Content-Security-Policy HTTP Header missing on port 2082.
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2082

Server Returns HTTP 500 Message For Request — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**3**
QID:	150042
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-06-29 22:50:55.0

THREAT:
During the scanning engine's crawl phase, the Web server responded with an HTTP 500 message for each link listed below. The HTTP 500 message indicates a server error.

IMPACT:
The presence of an HTTP 500 error during the crawl phase indicates that some problem exists in the Web site that will be encountered during normal usage of the Web application.

SOLUTION:
Review each link to determine why the server encountered an error when responding to the link.

RESULT:
https://northerngreen.org/wp-includes/block-patterns.php
https://northerngreen.org/wp-includes/blocks.php
https://northerngreen.org/wp-includes/blocks/
https://northerngreen.org/wp-includes/cache.php
https://northerngreen.org/wp-includes/class-IXR.php
https://northerngreen.org/wp-includes/class-feed.php
https://northerngreen.org/wp-includes/class-http.php
https://northerngreen.org/wp-includes/class-json.php
https://northerngreen.org/wp-includes/class-oembed.php

https://northerngreen.org/wp-includes/class-smtp.php
https://northerngreen.org/wp-includes/class-simplepie.php
https://northerngreen.org/wp-includes/class-snoopy.php
https://northerngreen.org/wp-includes/class-walker-category-dropdown.php
https://northerngreen.org/wp-includes/class-walker-category.php
https://northerngreen.org/wp-includes/class-walker-comment.php
https://northerngreen.org/wp-includes/class-walker-page-dropdown.php
https://northerngreen.org/wp-includes/class-walker-nav-menu.php
https://northerngreen.org/wp-includes/class-walker-page.php
https://northerngreen.org/wp-includes/class-wp-customize-control.php
https://northerngreen.org/wp-includes/class-wp-customize-section.php
https://northerngreen.org/wp-includes/class-wp-customize-setting.php
https://northerngreen.org/wp-includes/class-wp-customize-panel.php
https://northerngreen.org/wp-includes/class-wp-feed-cache.php
https://northerngreen.org/wp-includes/class-wp-http-ixr-client.php
https://northerngreen.org/wp-includes/class-wp-http-requests-hooks.php
https://northerngreen.org/wp-includes/class-wp-http-requests-response.php
https://northerngreen.org/wp-includes/class-wp-image-editor-gd.php
https://northerngreen.org/wp-includes/class-wp-http.php
https://northerngreen.org/wp-includes/class-wp-image-editor-imagick.php
https://northerngreen.org/wp-includes/class-wp-simplepie-file.php
https://northerngreen.org/wp-includes/class-wp-simplepie-sanitize-kses.php
https://northerngreen.org/wp-includes/class-wp-text-diff-renderer-inline.php
https://northerngreen.org/wp-includes/class-wp-text-diff-renderer-table.php
https://northerngreen.org/wp-includes/class-wp-user-meta-session-tokens.php
https://northerngreen.org/wp-includes/class-wp-xmlrpc-server.php
https://northerngreen.org/wp-includes/class.wp-scripts.php
https://northerngreen.org/wp-includes/class.wp-styles.php
https://northerngreen.org/wp-includes/compat.php
https://northerngreen.org/wp-includes/date.php
https://northerngreen.org/wp-includes/default-widgets.php
https://northerngreen.org/wp-includes/default-filters.php
https://northerngreen.org/wp-includes/embed-template.php
https://northerngreen.org/wp-includes/feed-atom-comments.php
https://northerngreen.org/wp-includes/feed-atom.php
https://northerngreen.org/wp-includes/feed-rdf.php
https://northerngreen.org/wp-includes/feed-rss.php
https://northerngreen.org/wp-includes/feed-rss2-comments.php
https://northerngreen.org/wp-includes/feed-rss2.php
https://northerngreen.org/wp-includes/functions.php
https://northerngreen.org/wp-includes/locale.php
https://northerngreen.org/wp-includes/ms-blogs.php
https://northerngreen.org/wp-includes/media.php
https://northerngreen.org/wp-includes/ms-default-filters.php
https://northerngreen.org/wp-includes/ms-settings.php
https://northerngreen.org/wp-includes/nav-menu-template.php
https://northerngreen.org/wp-includes/registration-functions.php
https://northerngreen.org/wp-includes/registration.php
https://northerngreen.org/wp-includes/rss.php
https://northerngreen.org/wp-includes/script-loader.php
https://northerngreen.org/wp-includes/session.php
https://northerngreen.org/wp-includes/spl-autoload-compat.php
https://northerngreen.org/wp-includes/template-loader.php
https://northerngreen.org/wp-includes/template-canvas.php
https://northerngreen.org/wp-includes/update.php
https://northerngreen.org/wp-includes/vars.php

Content-Security-Policy HTTP Security Header Not Detected — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3
QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Last Update:	2019-03-11 17:50:46.0

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:

This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Content-Security-Policy HTTP Header missing on port 2095.

GET / HTTP/1.0

Host: server.northerngreenexpo.org:2095

DEFLATE Data Compression Algorithm Used for HTTPS

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3
QID:	42416
Category:	General remote services
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Last Update:	2013-08-10 00:02:05.0

THREAT:

HTTP data is compressed before it is sent from the server. DEFLATE data compression algorithm uses the LZ77 algorithm which takes advantage of repeated strings to more efficiently compress output.

DEFLATE data compression algorithm is prone to be unsafe as described in the BREACH attack. If an attacker can inject a string into a HTTPS response intended to match another unknown string (the target secret), they can iteratively guess the secret value by monitoring the compressed size of the responses for different guesses. Note: The attacker needs the capability of reading responses received by the user's browser and the capability of cause the victim to send requests from their browser to perform BREACH attack.

This QID detects that the remote HTTP server is using a gzip or DEFLATE (zlib) compression format which is using DEFLATE data compression algorithm.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP/1.1 401 Unauthorized
Date: Wed, 26 Jan 2022 13:10:19 GMT
Server: cPanel
Persistent-Auth: false
Host: 162.144.102.68:2080
Cache-Control: no-cache, no-store, must-revalidate, private
Connection: close
Vary: Accept-Encoding
WWW-Authenticate: Basic realm="Horde DAV Server"
Content-Encoding: gzip
Content-Length: 52
Content-Type: text/html; charset="utf-8"
Expires: Fri, 01 Jan 1990 00:00:00 GMT

_1F_8B_08_00;H_F1a_00_03_B3_C9(_C9_CD_B1s,-_C9_C8/_CA_ACJ,_C9_CC_CFS_08J-,_CD,JM_B1_D1_07K_02_00ESr^#

HTTP/1.1 401 Unauthorized
Date: Wed, 26 Jan 2022 13:10:20 GMT
Server: cPanel
Persistent-Auth: false
Host: 162.144.102.68:2080
Cache-Control: no-cache, no-store, must-revalidate, private
Connection: close
Vary: Accept-Encoding
WWW-Authenticate: Basic realm="Horde DAV Server"
Content-Encoding: gzip
Content-Length: 52
Content-Type: text/html; charset="utf-8"
Expires: Fri, 01 Jan 1990 00:00:00 GMT

_1F_8B_08_00<H_F1a_00_03_B3_C9(_C9_CD_B1s,-_C9_C8/_CA_ACJ,_C9_CC_CFS_08J-,_CD,JM_B1_D1_07K_02_00ESr^#

HTTP/1.1 401 Unauthorized
Date: Wed, 26 Jan 2022 14:24:44 GMT
Server: cPanel
Persistent-Auth: false
Host: 162.144.102.68:2078
Cache-Control: no-cache, no-store, must-revalidate, private

Connection: close
Vary: Accept-Encoding
WWW-Authenticate: Basic realm="Restricted Area"
Content-Encoding: gzip
Content-Length: 52
Content-Type: text/html; charset="utf-8"
Expires: Fri, 01 Jan 1990 00:00:00 GMT

_1F_8B_08_00_ACY_F1a_00_03_B3_C9(_C9_CD_B1s,-_C9_C8/_CA_ACJ,_C9_CC_CFS_08J-,_CD,JM_B1_D1_07K_02_00ESr^#

HTTP/1.1 301 Moved Permanently
Date: Wed, 26 Jan 2022 14:28:27 GMT
Server: Apache
X-Redirect-By: WordPress
Content-Encoding: gzip
Vary: Accept-Encoding
Location: https://northerngreen.org/
Cache-Control: max-age=604800
Expires: Wed, 02 Feb 2022 14:28:27 GMT
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

HTTP/1.1 301 Moved Permanently
Date: Wed, 26 Jan 2022 14:28:28 GMT
Server: Apache
X-Redirect-By: WordPress
Content-Encoding: gzip
Vary: Accept-Encoding
Location: https://northerngreen.org/
Cache-Control: max-age=604800
Expires: Wed, 02 Feb 2022 14:28:28 GMT
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

HTTP/1.1 301 Moved Permanently
Date: Wed, 26 Jan 2022 14:28:28 GMT
Server: Apache
X-Redirect-By: WordPress
Content-Encoding: deflate
Vary: Accept-Encoding
Location: https://northerngreen.org/
Cache-Control: max-age=604800
Expires: Wed, 02 Feb 2022 14:28:28 GMT
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

Server Returns HTTP 500 Message For Request **port 80 / tcp**

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**3**
QID:	150042
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-06-29 22:50:55.0

THREAT:

During the scanning engine's crawl phase, the Web server responded with an HTTP 500 message for each link listed below. The HTTP 500 message indicates a server error.

IMPACT:

The presence of an HTTP 500 error during the crawl phase indicates that some problem exists in the Web site that will be encountered during normal usage of the Web application.

SOLUTION:

Review each link to determine why the server encountered an error when responding to the link.

RESULT:

https://northerngreen.org/wp-includes/block-patterns.php
https://northerngreen.org/wp-includes/blocks.php
https://northerngreen.org/wp-includes/blocks/
https://northerngreen.org/wp-includes/cache.php
https://northerngreen.org/wp-includes/class-IXR.php
https://northerngreen.org/wp-includes/class-feed.php
https://northerngreen.org/wp-includes/class-json.php
https://northerngreen.org/wp-includes/class-http.php
https://northerngreen.org/wp-includes/class-oembed.php
https://northerngreen.org/wp-includes/class-simplepie.php
https://northerngreen.org/wp-includes/class-smtp.php
https://northerngreen.org/wp-includes/class-snoopy.php
https://northerngreen.org/wp-includes/class-walker-category-dropdown.php
https://northerngreen.org/wp-includes/class-walker-comment.php
https://northerngreen.org/wp-includes/class-walker-category.php
https://northerngreen.org/wp-includes/class-walker-nav-menu.php
https://northerngreen.org/wp-includes/class-walker-page-dropdown.php
https://northerngreen.org/wp-includes/class-walker-page.php
https://northerngreen.org/wp-includes/class-wp-customize-control.php
https://northerngreen.org/wp-includes/class-wp-customize-section.php
https://northerngreen.org/wp-includes/class-wp-customize-setting.php
https://northerngreen.org/wp-includes/class-wp-customize-panel.php
https://northerngreen.org/wp-includes/class-wp-feed-cache.php
https://northerngreen.org/wp-includes/class-wp-http-ixr-client.php
https://northerngreen.org/wp-includes/class-wp-http-requests-response.php
https://northerngreen.org/wp-includes/class-wp-http-requests-hooks.php
https://northerngreen.org/wp-includes/class-wp-http.php
https://northerngreen.org/wp-includes/class-wp-image-editor-gd.php
https://northerngreen.org/wp-includes/class-wp-image-editor-imagick.php
https://northerngreen.org/wp-includes/class-wp-simplepie-file.php

https://northerngreen.org/wp-includes/class-wp-simplepie-sanitize-kses.php
https://northerngreen.org/wp-includes/class-wp-text-diff-renderer-inline.php
https://northerngreen.org/wp-includes/class-wp-text-diff-renderer-table.php
https://northerngreen.org/wp-includes/class-wp-user-meta-session-tokens.php
https://northerngreen.org/wp-includes/class-wp-xmlrpc-server.php
https://northerngreen.org/wp-includes/class.wp-styles.php
https://northerngreen.org/wp-includes/class.wp-scripts.php
https://northerngreen.org/wp-includes/compat.php
https://northerngreen.org/wp-includes/date.php
https://northerngreen.org/wp-includes/default-widgets.php
https://northerngreen.org/wp-includes/default-filters.php
https://northerngreen.org/wp-includes/embed-template.php
https://northerngreen.org/wp-includes/feed-atom.php
https://northerngreen.org/wp-includes/feed-atom-comments.php
https://northerngreen.org/wp-includes/feed-rdf.php
https://northerngreen.org/wp-includes/feed-rss.php
https://northerngreen.org/wp-includes/feed-rss2-comments.php
https://northerngreen.org/wp-includes/feed-rss2.php
https://northerngreen.org/wp-includes/functions.php
https://northerngreen.org/wp-includes/locale.php
https://northerngreen.org/wp-includes/media.php
https://northerngreen.org/wp-includes/ms-blogs.php
https://northerngreen.org/wp-includes/ms-default-filters.php
https://northerngreen.org/wp-includes/ms-settings.php
https://northerngreen.org/wp-includes/nav-menu-template.php
https://northerngreen.org/wp-includes/registration-functions.php
https://northerngreen.org/wp-includes/registration.php
https://northerngreen.org/wp-includes/rss.php
https://northerngreen.org/wp-includes/script-loader.php
https://northerngreen.org/wp-includes/session.php
https://northerngreen.org/wp-includes/spl-autoload-compat.php
https://northerngreen.org/wp-includes/template-canvas.php
https://northerngreen.org/wp-includes/template-loader.php
https://northerngreen.org/wp-includes/update.php
https://northerngreen.org/wp-includes/vars.php

POP3 Banner — port 995 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	50000
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Last Update:	2020-11-02 08:21:29.0

THREAT:
Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline.

IMPACT:
NA

SOLUTION:
NA

RESULT:
+OK Dovecot ready.

Web Server HTTP Protocol Versions — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-24 10:47:04.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 2086 port.GET / HTTP/1.1

Web Server HTTP Protocol Versions — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-24 10:47:04.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 2095 port.GET / HTTP/1.1

Connection Error Occurred During Web Application Scan — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	150018
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:24:58.0

THREAT:
The following are some of the possible reasons for the timeouts or connection errors:

1. A disturbance in network connectivity between the scanner and the web application occurred.
2. The web server or application server hosting the application was taken down in the midst of a scan.
3. The web application experienced an overload, possibly due to load generated by the scan.
4. An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only).
5. A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner.
6. Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

IMPACT:
Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

SOLUTION:
First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure exclude lists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

RESULT:
Total number of unique links that encountered timeout errors: 1
Links with highest number of timeouts:
3 https://northerngreen.org/?sid=1&bsa_pro_id=12%20%2B%20(SELECT%200%20FROM%20(SELECT%20SLEEP(29))qsqli_1111)%20&bsa_pro_url=1

Phase wise summary of timeout and connection errors encountered:
ePhaseTimeBasedTests : 3 0

Server Returned Unexpected Response Code — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	150019
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:34.0

THREAT:
The Web server returned an HTTP response code that was unexpected or not handled by the Web application scanning engine. The scan continued, but the response may be indicative of connection or Web server errors.

IMPACT:
An unexpected or unhandled response code might be indicative of a problem in the Web server or the crawling process.

SOLUTION:
Verify that the HTTP response code is not the result of a Web server error.

RESULT:
308: http://server.northerngreenexpo.org:2095/?locale=ar

FTP Server Banner — port 21 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	27113
Category:	File Transfer Protocol
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-04-30 06:01:51.0

THREAT:
The following message is shown to all users logging on to your FTP server, including anonymous logins if they are allowed on your server.

IMPACT:
Unauthorized users can obtain sensitive information about your server, such as the version or type of server you are running, and use this information to implement specific attacks against the server.

SOLUTION:
If possible, edit the configuration files or recompile the server to restrict the type of information disclosed.

RESULT:
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 05:24. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.

SMTP Banner — port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	74042
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-02 08:52:43.0

THREAT:
The Simple Mail Transfer Protocol is a communication protocol for electronic mail transmission.

QID Detection Logic:
The QID checks for 220 status code in the banner of the response.

IMPACT:
NA

SOLUTION:
NA

RESULT:
220-server.northerngreenexpo.org ESMTP Exim 4.94.2 #2 Wed, 26 Jan 2022 05:26:26 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

Web Server HTTP Protocol Versions — port 2078 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-24 10:47:04.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 2078 port.GET / HTTP/1.1

Web Server HTTP Protocol Versions — port 2079 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-24 10:47:04.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 2079 port.GET / HTTP/1.1

IMAP Banner — port 143 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	50010
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-02 08:31:22.0

THREAT:
IMAP (Internet Message Access Protocol) is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages as though they were stored locally on the end user's computing device(s).

QID Detection Logic:
The QID checks for IMAP in the banner of the response.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.

SMTP Banner — port 587 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	74042
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-02 08:52:43.0

THREAT:
The Simple Mail Transfer Protocol is a communication protocol for electronic mail transmission.

QID Detection Logic:
The QID checks for 220 status code in the banner of the response.

IMPACT:
NA

SOLUTION:
NA

RESULT:
220-server.northerngreenexpo.org ESMTP Exim 4.94.2 #2 Wed, 26 Jan 2022 05:38:19 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

SMTP Banner — port 26 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	74042
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-02 08:52:43.0

THREAT:

The Simple Mail Transfer Protocol is a communication protocol for electronic mail transmission.

QID Detection Logic:

The QID checks for 220 status code in the banner of the response.

IMPACT:

NA

SOLUTION:

NA

RESULT:

220-server.northerngreenexpo.org ESMTP Exim 4.94.2 #2 Wed, 26 Jan 2022 05:37:25 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

Web Server HTTP Protocol Versions — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-24 10:47:04.0

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

Connection Error Occurred During Web Application Scan — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	150018
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:24:58.0

THREAT:
The following are some of the possible reasons for the timeouts or connection errors:

1. A disturbance in network connectivity between the scanner and the web application occurred.
2. The web server or application server hosting the application was taken down in the midst of a scan.
3. The web application experienced an overload, possibly due to load generated by the scan.
4. An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only).
5. A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner.
6. Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

IMPACT:
Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

SOLUTION:
First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure exclude lists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

RESULT:
Total number of unique links that encountered timeout errors: 1
Links with highest number of timeouts:
3 https://northerngreen.org/?sid=1&bsa_pro_id=12%20%2B%20(SELECT%200%20FROM%20(SELECT%20SLEEP(29))qsqli_1111)%20&bsa_pro_url=1

Phase wise summary of timeout and connection errors encountered:
ePhaseTimeBasedTests : 3 0

SMTP Banner — port 25 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**

QID:	74042
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-02 08:52:43.0

THREAT:
The Simple Mail Transfer Protocol is a communication protocol for electronic mail transmission.

QID Detection Logic:
The QID checks for 220 status code in the banner of the response.

IMPACT:
NA

SOLUTION:
NA

RESULT:
220-server.northerngreenexpo.org ESMTP Exim 4.94.2 #2 Wed, 26 Jan 2022 05:24:58 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

Web Server HTTP Protocol Versions — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-24 10:47:04.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-27 12:31:58.0

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) **TCP/IP Fingerprint**: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) **NetBIOS**: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) **PHP Info**: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) **SNMP**: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

RESULT:

Operating System	Technique	ID
Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP	TCP/IP Fingerprint	M4856:7259:: 21

Server Returned Unexpected Response Code — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	150019
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:34.0

THREAT:
The Web server returned an HTTP response code that was unexpected or not handled by the Web application scanning engine. The scan continued, but the response may be indicative of connection or Web server errors.

IMPACT:
An unexpected or unhandled response code might be indicative of a problem in the Web server or the crawling process.

SOLUTION:
Verify that the HTTP response code is not the result of a Web server error.

RESULT:
308: http://server.northerngreenexpo.org:2082/?locale=ar

Web Server HTTP Protocol Versions — port 2080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-24 10:47:04.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 2080 port.GET / HTTP/1.1

POP3 Banner — port 110 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	50000
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-02 08:21:29.0

THREAT:
Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline.

IMPACT:
NA

SOLUTION:
NA

RESULT:
+OK Dovecot ready.

Web Server HTTP Protocol Versions — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-24 10:47:04.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 2082 port.GET / HTTP/1.1

IMAP Banner — port 993 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	50010
Category:	Mail services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-02 08:31:22.0

THREAT:
IMAP (Internet Message Access Protocol) is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages as though they were stored locally on the end user's computing device(s).

QID Detection Logic:
The QID checks for IMAP in the banner of the response.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN AUTH=LOGIN] Dovecot ready.

Named Daemon Version Number Disclosure Vulnerability — port 53 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	15001
Category:	DNS and BIND
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2003-02-10 18:41:21.0

THREAT:
Named is the daemon used to provide the DNS translation service.

IMPACT:
If successfully exploited, unauthorized users can determine which version of "named" is running on this host. This is very dangerous since it enables aggressive intruders to prepare a specific attack for the version being used.

SOLUTION:
Unless it is required on this host, disable this feature.

RESULT:
9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6_10.8

Server Returned Unexpected Response Code — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	150019
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:34.0

THREAT:
The Web server returned an HTTP response code that was unexpected or not handled by the Web application scanning engine. The scan continued, but the response may be indicative of connection or Web server errors.

IMPACT:
An unexpected or unhandled response code might be indicative of a problem in the Web server or the crawling process.

SOLUTION:
Verify that the HTTP response code is not the result of a Web server error.

RESULT:
308: http://server.northerngreenexpo.org:2086/?locale=ar

Connection Error Occurred During Web Application Scan — port 2077 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2
QID:	150018
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:24:58.0

THREAT:
The following are some of the possible reasons for the timeouts or connection errors:

1. A disturbance in network connectivity between the scanner and the web application occurred.
2. The web server or application server hosting the application was taken down in the midst of a scan.
3. The web application experienced an overload, possibly due to load generated by the scan.
4. An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only).
5. A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner.
6. Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

IMPACT:
Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

SOLUTION:
First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure exclude lists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

RESULT:
Total number of unique links that encountered connection errors: 1
Links with highest number of connection errors:
1 http://server.northerngreenexpo.org:2077/tziJ53E2I252.html

Phase wise summary of timeout and connection errors encountered:
ePhaseCrawl : 0 1

Web Server HTTP Protocol Versions — port 2077 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-24 10:47:04.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 2077 port.GET / HTTP/1.1

Web Server HTTP Protocol Versions — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-24 10:47:04.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

Web Server HTTP Protocol Versions — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2017-04-24 10:47:04.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

Default Web Page — port 2077 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2077

<html>Authorization Required</html>

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 143 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2018-01-04 17:39:37.0

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

IP address	Host name
162.144.102.68	server.northerngreenexpo.org

SSL Certificate - Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	03:f9:f7:a2:22:6e:a7:3a:e6:ac:8f:02:ff:9d:bd:5e:c0:33
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
organizationName	Let's Encrypt
commonName	R3
(0)SUBJECT NAME	
commonName	www.build.northerngreen.org
(0)Valid From	Nov 30 16:52:29 2021 GMT
(0)Valid Till	Feb 28 16:52:28 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:d8:87:6f:fb:fa:ff:ec:1e:4f:78:de:9b:01:d0:
(0)	20:96:09:7b:84:d3:8f:28:11:00:d2:f4:43:06:b4:
(0)	88:e9:d2:50:48:40:b6:ab:3f:30:7c:f4:ca:41:74:
(0)	4f:9d:e9:46:ba:57:99:37:ed:8a:e9:df:91:b5:2c:
(0)	a9:b8:2c:b5:8e:1d:d7:d1:8f:41:3c:51:0e:1f:86:
(0)	b1:c8:b7:8e:38:37:aa:4c:30:d9:58:59:d4:33:41:
(0)	22:26:59:18:8c:08:12:d7:46:5d:b9:9c:32:15:db:
(0)	1e:15:0e:b3:03:a7:62:4d:f2:13:ba:4c:bf:77:8b:
(0)	80:06:35:53:32:70:ba:23:a3:a0:38:05:a2:ef:f9:
(0)	7d:09:0c:45:54:ed:d5:c7:1c:ac:13:18:b8:a5:f8:
(0)	8e:8e:e3:34:d8:9d:82:ec:2d:64:73:11:8f:1a:a8:
(0)	bf:4b:70:d8:9c:8b:bd:9b:56:06:be:81:28:f0:9f:
(0)	1b:4b:79:81:01:c8:0b:97:e6:d5:69:b2:78:26:4a:
(0)	9d:0f:74:a2:df:88:0b:97:7e:dc:b7:c7:58:18:d3:
(0)	b9:7d:e2:90:22:cd:e3:13:fa:a5:8c:08:ea:ef:39:
(0)	5f:fe:79:e2:66:db:8b:a2:f1:e4:04:46:e6:bf:35:
(0)	15:7a:d8:99:ec:c5:ca:45:b0:0b:5d:02:cd:2b:94:
(0)	44:e1
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3	

Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Subject Key Identifier	A7:FB:18:91:24:3B:CA:83:7D:05:05:EC:6F:2D:C3:63:1A:8D:85:17
(0)X509v3 Authority Key Identifier	keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
(0)Authority Information Access	OCSP - URI:http://r3.o.lencr.org
(0)	CA Issuers - URI:http://r3.i.lencr.org/
(0)X509v3 Subject Alternative Name	DNS:build.northerngreen.org, DNS:mail.northerngreen.org, DNS:new.northerngreen.org, DNS:new.northerngreenexpo.org, DNS:northerngreen.org, DNS:www.build.northerngreen.org, DNS:www.new.northerngreen.org, DNS:www.new.northerngreenexpo.org, DNS:www.northerngreen.org
(0)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(0)	Policy: 1.3.6.1.4.1.44947.1.1.1
(0)	CPS: http://cps.letsencrypt.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Nov 30 17:52:29.631 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:2B:60:04:5C:CC:C7:41:70:2F:AC:45:A9:
(0)	46:6B:44:C8:2A:00:D0:C6:E8:0D:24:26:9B:80:EC:F5:
(0)	C3:BB:32:90:02:21:00:E4:72:67:6C:BB:03:32:9C:46:
(0)	91:49:84:D3:7E:AD:7D:96:6B:5A:2A:4B:AE:D9:71:16:
(0)	23:EF:02:0F:FC:78:CA
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : DF:A5:5E:AB:68:82:4F:1F:6C:AD:EE:B8:5F:4E:3E:5A:
(0)	EA:CD:A2:12:A4:6A:5E:8E:3B:12:C0:20:44:5C:2A:73
(0)	Timestamp : Nov 30 17:52:30.186 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:DF:1B:5F:9F:B0:70:1E:1B:08:CE:65:
(0)	E4:BD:1B:8D:D0:8B:B5:DF:83:B7:10:7D:B9:A5:28:BD:
(0)	A6:68:6F:E3:95:02:20:4C:38:2A:E6:81:59:E8:B9:32:
(0)	70:11:39:81:61:57:97:CA:CD:04:51:47:42:14:5F:23:
(0)	D1:48:A9:A3:10:A6:4A
(0)Signature	(256 octets)
(0)	59:bd:11:f4:70:03:55:f4:9c:82:e9:b3:5c:cd:1d:73
(0)	e5:82:98:74:4d:b6:c3:94:bc:f6:93:d1:e6:a4:c4:81
(0)	07:67:3f:2c:d9:21:42:5b:73:85:ed:6a:e2:01:60:8d
(0)	92:2c:65:27:b3:10:8c:ce:b5:5e:82:cb:80:20:35:f4
(0)	e1:51:b3:7f:f8:7d:bd:c4:01:11:2f:fa:eb:af:48:7a
(0)	3a:15:cb:ed:85:fc:96:dc:74:5c:68:14:bc:1e:df:d9
(0)	c8:67:24:30:7b:20:b0:9a:5b:ee:fe:59:6e:0f:58:04

(0)	66:26:fe:6f:ed:7b:78:10:f1:c1:a1:e0:4c:56:82:c1
(0)	93:d6:4c:ba:46:83:3a:1b:f3:6d:1a:bb:70:be:1e:bf
(0)	07:76:b0:bc:99:c3:c5:50:8f:b2:22:87:7b:ae:fd:49
(0)	66:66:d8:17:94:f6:23:20:c8:8e:0b:ca:d2:cc:34:a6
(0)	bf:07:6f:59:5b:b8:d8:96:22:fe:39:d6:b0:fc:9f:cd
(0)	6f:7c:30:ee:d8:6a:87:10:f0:03:e2:76:5a:2f:99:e4
(0)	0c:bf:ed:28:7c:ee:a1:58:73:b6:cb:e8:3c:dc:d2:4c
(0)	45:7e:eb:65:36:c3:09:06:a9:f6:25:77:7c:e5:f8:48
(0)	9c:9c:4c:10:0e:08:25:6b:a5:53:ae:ad:d9:8e:72:80
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	91:2b:08:4a:cf:0c:18:a7:53:f6:d6:2e:25:a7:5f:5a
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
organizationName	Internet Security Research Group
commonName	ISRG Root X1
(1)SUBJECT NAME	
countryName	US
organizationName	Let's Encrypt
commonName	R3
(1)Valid From	Sep 4 00:00:00 2020 GMT
(1)Valid Till	Sep 15 16:00:00 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55:
(1)	92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:
(1)	2b:b9:c5:4c:b1:af:8e:6b:f9:75:c8:a3:d7:0f:47:
(1)	94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42:
(1)	a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38:
(1)	e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa:
(1)	37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52:
(1)	45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de:
(1)	60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b:
(1)	d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8:
(1)	30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17:
(1)	c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46:
(1)	e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7:
(1)	a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98:
(1)	09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af:
(1)	63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d:
(1)	a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b:
(1)	db:15
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign

(1)X509v3 Extended Key Usage	TLS Web Client Authentication, TLS Web Server Authentication
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Subject Key Identifier	14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
(1)X509v3 Authority Key Identifier	keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
(1)Authority Information Access	CA Issuers - URI:http://x1.i.lencr.org/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://x1.c.lencr.org/
(1)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(1)	Policy: 1.3.6.1.4.1.44947.1.1.1
(1)Signature	(512 octets)
(1)	85:ca:4e:47:3e:a3:f7:85:44:85:bc:d5:67:78:b2:98
(1)	63:ad:75:4d:1e:96:3d:33:65:72:54:2d:81:a0:ea:c3
(1)	ed:f8:20:bf:5f:cc:b7:70:00:b7:6e:3b:f6:5e:94:de
(1)	e4:20:9f:a6:ef:8b:b2:03:e7:a2:b5:16:3c:91:ce:b4
(1)	ed:39:02:e7:7c:25:8a:47:e6:65:6e:3f:46:f4:d9:f0
(1)	ce:94:2b:ee:54:ce:12:bc:8c:27:4b:b8:c1:98:2f:a2
(1)	af:cd:71:91:4a:08:b7:c8:b8:23:7b:04:2d:08:f9:08
(1)	57:3e:83:d9:04:33:0a:47:21:78:09:82:27:c3:2a:c8
(1)	9b:b9:ce:5c:f2:64:c8:c0:be:79:c0:4f:8e:6d:44:0c
(1)	5e:92:bb:2e:f7:8b:10:e1:e8:1d:44:29:db:59:20:ed
(1)	63:b9:21:f8:12:26:94:93:57:a0:1d:65:04:c1:0a:22
(1)	ae:10:0d:43:97:a1:18:1f:7e:e0:e0:86:37:b5:5a:b1
(1)	bd:30:bf:87:6e:2b:2a:ff:21:4e:1b:05:c3:f5:18:97
(1)	f0:5e:ac:c3:a5:b8:6a:f0:2e:bc:3b:33:b9:ee:4b:de
(1)	cc:fc:e4:af:84:0b:86:3f:c0:55:43:36:f6:68:e1:36
(1)	17:6a:8e:99:d1:ff:a5:40:a7:34:b7:c0:d0:63:39:35
(1)	39:75:6e:f2:ba:76:c8:93:02:e9:a9:4b:6c:17:ce:0c
(1)	02:d9:bd:81:fb:9f:b7:68:d4:06:65:b3:82:3d:77:53
(1)	f8:8e:79:03:ad:0a:31:07:75:2a:43:d8:55:97:72:c4
(1)	29:0e:f7:c4:5d:4e:c8:ae:46:84:30:d7:f2:85:5f:18
(1)	a1:79:bb:e7:5e:70:8b:07:e1:86:93:c3:b9:8f:dc:61
(1)	71:25:2a:af:df:ed:25:50:52:68:8b:92:dc:e5:d6:b5
(1)	e3:da:7d:d0:87:6c:84:21:31:ae:82:f5:fb:b9:ab:c8
(1)	89:17:3d:e1:4c:e5:38:0e:f6:bd:2b:bd:96:81:14:eb
(1)	d5:db:3d:20:a7:7e:59:d3:e2:f8:58:f9:5b:b8:48:cd
(1)	fe:5c:4f:16:29:fe:1e:55:23:af:c8:11:b0:8d:ea:7c
(1)	93:90:17:2f:fd:ac:a2:09:47:46:3f:f0:e9:b0:b7:ff
(1)	28:4d:68:32:d6:67:5e:1e:69:a3:93:b8:f5:9d:8b:2f
(1)	0b:d2:52:43:a6:6f:32:57:65:4d:32:81:df:38:53:85
(1)	5d:7e:5d:66:29:ea:b8:dd:e4:95:b5:cd:b5:56:12:42
(1)	cd:c4:4e:c6:25:38:44:50:6d:ec:ce:00:55:18:fe:e9
(1)	49:64:d4:4e:ca:97:9c:b4:5b:c0:73:a8:ab:b8:47:c2
NAME	VALUE

(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	03:04:c2:9a:3f:a3:27:34:12:1b:64:1e:da:08:e1:9b:90:71
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
organizationName	Let's Encrypt
commonName	R3
(0)SUBJECT NAME	
commonName	wordpress.northerngreenexpo.org
(0)Valid From	Nov 30 16:52:34 2021 GMT
(0)Valid Till	Feb 28 16:52:33 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:98:fd:8f:5e:9e:9e:df:37:e6:f3:ad:92:44:fb:
(0)	e7:c6:75:14:b6:d4:b6:ae:d7:5e:30:cc:ba:e9:a7:
(0)	f1:fb:97:46:20:5e:75:d7:e7:39:7d:f3:70:e4:d6:
(0)	47:84:53:91:58:c3:b0:de:4a:93:16:bf:94:d9:d8:
(0)	75:7c:1c:dc:a4:fd:ae:df:d8:11:e3:a3:64:ad:d4:
(0)	3c:c9:2d:93:64:e6:bb:57:1c:bb:85:a3:b4:25:34:
(0)	72:4d:93:61:dd:b0:ce:63:88:20:22:97:a5:50:91:
(0)	62:f2:3e:df:3e:56:51:c7:d1:39:a5:77:e9:9b:ea:
(0)	26:99:a4:8e:d8:04:f7:f3:98:81:26:b5:37:b9:40:
(0)	95:2a:60:bd:55:ab:63:1a:8d:e4:2b:46:2b:3d:31:
(0)	01:63:d2:17:91:67:be:7e:76:9e:3f:63:09:b5:6d:
(0)	c5:ab:01:17:eb:2a:7a:da:45:ca:2d:1a:e4:ce:ae:
(0)	bf:03:64:b2:54:fb:81:7c:4c:ad:a3:71:0e:69:bb:
(0)	a9:26:6a:aa:7f:fe:84:5d:b3:d2:86:f1:69:42:3b:
(0)	3b:93:87:d2:e2:8a:43:80:f3:f6:ca:06:8b:2b:47:
(0)	63:79:c5:fe:94:27:df:6a:ba:ca:06:a7:87:47:fc:
(0)	ee:a2:8a:29:4c:9b:89:b6:4a:d2:1f:a3:ef:36:93:
(0)	14:7b
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Subject Key Identifier	8E:FF:D4:2A:84:19:5B:E1:85:79:83:DF:FF:1A:EA:2C:A8:41:A6:4F
(0)X509v3 Authority Key	keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6

Identifier	
(0)Authority Information Access	OCSP - URI:http://r3.o.lencr.org
(0)	CA Issuers - URI:http://r3.i.lencr.org/
(0)X509v3 Subject Alternative Name	DNS:nor.northerngreenexpo.org, DNS:wordpress.northerngreenexpo.org, DNS:www.nor.northerngreenexpo.org, DNS:www.wordpress.northerngreenexpo.org
(0)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(0)	Policy: 1.3.6.1.4.1.44947.1.1.1
(0)	CPS: http://cps.letsencrypt.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Nov 30 17:52:34.698 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:21:00:9B:B1:10:3E:50:95:55:2A:29:B7:D9:
(0)	AB:46:78:24:D8:96:9C:52:6D:F0:D9:A4:F9:95:E1:5A:
(0)	0F:B4:FD:3E:AC:02:20:7B:70:5B:3C:A6:44:34:DA:1C:
(0)	18:6C:AF:36:F9:28:20:8D:FA:62:42:21:6D:9F:8C:84:
(0)	5B:F5:14:7C:F4:19:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : DF:A5:5E:AB:68:82:4F:1F:6C:AD:EE:B8:5F:4E:3E:5A:
(0)	EA:CD:A2:12:A4:6A:5E:8E:3B:12:C0:20:44:5C:2A:73
(0)	Timestamp : Nov 30 17:52:34.797 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:53:58:36:0E:4E:E4:C9:4E:21:99:EE:65:
(0)	65:1B:DB:3C:DA:9D:FB:F0:14:D6:5E:A1:A2:A3:1C:F5:
(0)	62:DF:BB:79:02:21:00:FC:50:7C:23:69:40:2C:63:CB:
(0)	A4:32:14:BF:1A:8D:32:DF:FB:07:7C:C4:BE:79:1E:3B:
(0)	44:38:B9:AA:4D:AD:F2
(0)Signature	(256 octets)
(0)	76:c3:12:19:b7:b3:18:49:af:2a:68:dd:4d:af:57:e7
(0)	90:f0:0e:62:32:44:bb:73:02:c0:49:62:b5:85:0d:e4
(0)	da:9b:b0:db:eb:6f:8e:fa:68:02:3e:bb:c5:74:30:6c
(0)	04:91:e9:87:67:db:4f:49:bf:09:d1:83:50:4a:20:95
(0)	f5:d1:f6:22:bf:fe:aa:19:f8:ef:3f:8f:af:22:24:c8
(0)	62:37:c4:79:49:52:c3:66:8f:36:11:28:3c:7b:67:36
(0)	e6:d1:1d:5a:15:3e:72:2f:9f:28:07:47:5c:f9:df:72
(0)	35:03:6e:c3:9a:8f:1b:03:23:f6:95:bf:44:18:78:ba
(0)	6a:25:9f:6a:bb:c4:49:c8:58:57:ef:dc:c4:09:54:a2
(0)	7a:56:fe:b9:04:28:01:58:a7:19:38:47:51:6c:a8:50
(0)	da:47:71:be:ce:6b:2e:fd:b2:66:bf:b2:88:81:2b:8f
(0)	cc:86:23:18:5c:c3:74:3e:72:06:91:36:39:1b:9d:a0
(0)	3a:0e:e3:02:3a:90:ab:50:80:37:cb:d2:3f:54:76:eb
(0)	26:63:c1:2c:f0:cc:85:70:39:e1:c2:61:4f:30:b4:4c
(0)	ec:7d:0c:f5:78:15:09:b1:47:dc:e4:9c:f7:89:7b:3d
(0)	76:ae:f6:9e:7a:b3:b4:02:eb:15:e3:2d:00:af:5d:02
(1)CERTIFICATE	

1	
(1)Version	3 (0x2)
(1)Serial Number	91:2b:08:4a:cf:0c:18:a7:53:f6:d6:2e:25:a7:5f:5a
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
organizationName	Internet Security Research Group
commonName	ISRG Root X1
(1)SUBJECT NAME	
countryName	US
organizationName	Let's Encrypt
commonName	R3
(1)Valid From	Sep 4 00:00:00 2020 GMT
(1)Valid Till	Sep 15 16:00:00 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55:
(1)	92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:
(1)	2b:b9:c5:4c:b1:af:8e:6b:f9:75:c8:a3:d7:0f:47:
(1)	94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42:
(1)	a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38:
(1)	e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa:
(1)	37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52:
(1)	45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de:
(1)	60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b:
(1)	d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8:
(1)	30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17:
(1)	c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46:
(1)	e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7:
(1)	a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98:
(1)	09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af:
(1)	63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d:
(1)	a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b:
(1)	db:15
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Extended Key Usage	TLS Web Client Authentication, TLS Web Server Authentication
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Subject Key Identifier	14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
(1)X509v3	

Authority Key Identifier	keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
(1)Authority Information Access	CA Issuers - URI:http://x1.i.lencr.org/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://x1.c.lencr.org/
(1)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(1)	Policy: 1.3.6.1.4.1.44947.1.1.1
(1)Signature	(512 octets)
(1)	85:ca:4e:47:3e:a3:f7:85:44:85:bc:d5:67:78:b2:98
(1)	63:ad:75:4d:1e:96:3d:33:65:72:54:2d:81:a0:ea:c3
(1)	ed:f8:20:bf:5f:cc:b7:70:00:b7:6e:3b:f6:5e:94:de
(1)	e4:20:9f:a6:ef:8b:b2:03:e7:a2:b5:16:3c:91:ce:b4
(1)	ed:39:02:e7:7c:25:8a:47:e6:65:6e:3f:46:f4:d9:f0
(1)	ce:94:2b:ee:54:ce:12:bc:8c:27:4b:b8:c1:98:2f:a2
(1)	af:cd:71:91:4a:08:b7:c8:b8:23:7b:04:2d:08:f9:08
(1)	57:3e:83:d9:04:33:0a:47:21:78:09:82:27:c3:2a:c8
(1)	9b:b9:ce:5c:f2:64:c8:c0:be:79:c0:4f:8e:6d:44:0c
(1)	5e:92:bb:2e:f7:8b:10:e1:e8:1d:44:29:db:59:20:ed
(1)	63:b9:21:f8:12:26:94:93:57:a0:1d:65:04:c1:0a:22
(1)	ae:10:0d:43:97:a1:18:1f:7e:e0:e0:86:37:b5:5a:b1
(1)	bd:30:bf:87:6e:2b:2a:ff:21:4e:1b:05:c3:f5:18:97
(1)	f0:5e:ac:c3:a5:b8:6a:f0:2e:bc:3b:33:b9:ee:4b:de
(1)	cc:fc:e4:af:84:0b:86:3f:c0:55:43:36:f6:68:e1:36
(1)	17:6a:8e:99:d1:ff:a5:40:a7:34:b7:c0:d0:63:39:35
(1)	39:75:6e:f2:ba:76:c8:93:02:e9:a9:4b:6c:17:ce:0c
(1)	02:d9:bd:81:fb:9f:b7:68:d4:06:65:b3:82:3d:77:53
(1)	f8:8e:79:03:ad:0a:31:07:75:2a:43:d8:55:97:72:c4
(1)	29:0e:f7:c4:5d:4e:c8:ae:46:84:30:d7:f2:85:5f:18
(1)	a1:79:bb:e7:5e:70:8b:07:e1:86:93:c3:b9:8f:dc:61
(1)	71:25:2a:af:df:ed:25:50:52:68:8b:92:dc:e5:d6:b5
(1)	e3:da:7d:d0:87:6c:84:21:31:ae:82:f5:fb:b9:ab:c8
(1)	89:17:3d:e1:4c:e5:38:0e:f6:bd:2b:bd:96:81:14:eb
(1)	d5:db:3d:20:a7:7e:59:d3:e2:f8:58:f9:5b:b8:48:cd
(1)	fe:5c:4f:16:29:fe:1e:55:23:af:c8:11:b0:8d:ea:7c
(1)	93:90:17:2f:fd:ac:a2:09:47:46:3f:f0:e9:b0:b7:ff
(1)	28:4d:68:32:d6:67:5e:1e:69:a3:93:b8:f5:9d:8b:2f
(1)	0b:d2:52:43:a6:6f:32:57:65:4d:32:81:df:38:53:85
(1)	5d:7e:5d:66:29:ea:b8:dd:e4:95:b5:cd:b5:56:12:42
(1)	cd:c4:4e:c6:25:38:44:50:6d:ec:ce:00:55:18:fe:e9
(1)	49:64:d4:4e:ca:97:9c:b4:5b:c0:73:a8:ab:b8:47:c2

SSL Certificate - Information — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:

(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256

(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07
(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:

(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6
(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	

(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:
(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53

(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b
(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

SSL Certificate - Information — port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52

(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07

(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication

(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6
(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority

(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:
(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b

(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

Default Web Page — port 2079 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

GET / HTTP/1.0

Host: server.northerngreenexpo.org:2079

<html>Authorization Required</html>

Default Web Page — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>421 Misdirected Request</title>
</head><body>
<h1>Misdirected Request</h1>
The client needs a new connection for this
request as the requested host name does not match
the Server Name Indication (SNI) in use for this
connection.
</body></html>
GET / HTTP/1.0
Host: northerngreen.org

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 995 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2				
RSA	2048	no	110	low
DHE	1024	yes	80	low
ECDHE secp384r1	384	yes	192	low

SSL/TLS Server supports TLS_FALLBACK_SCSV — port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38610
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-06-08 22:10:22.0

THREAT:

TLS cipher suite TLS_FALLBACK_SCSV is a signaling cipher suite value (SCSV). TLS servers support TLS_FALLBACK_SCSV will prevent downgrade attack.

IMPACT:

N/A

SOLUTION:
N/A

RESULT:
TLS_FALLBACK_SCSV is supported on port 465.

SSL Server default Diffie-Hellman prime information — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38609
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-05-26 22:09:34.0

THREAT:
Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS. - For fixed primes: 1024 and below are considered unsafe. - For variable primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
SSL server default to use Diffie-Hellman key exchange method with variable 2048(bits) prime

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS
TLSv1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

Default Web Page (Follow HTTP Redirection) — port 2079 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:

nas-201911-01

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2079

<html>Authorization Required</html>

Links Crawled — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Duration of crawl phase (seconds): 933.00
Number of links: 300
(This number excludes form requests and links re-requested during authentication.)

https://northerngreen.org/
https://northerngreen.org/author/ng-staff/
https://northerngreen.org/awards-celebration/
https://northerngreen.org/book-your-booth/
https://northerngreen.org/booth-display-rules/
https://northerngreen.org/ceo-mgmt-track/
https://northerngreen.org/ceus/
https://northerngreen.org/comments/feed/
https://northerngreen.org/contact-us/
https://northerngreen.org/covid-safety/
https://northerngreen.org/digital-swag-bag/
https://northerngreen.org/education/
https://northerngreen.org/exhibitor-registration/
https://northerngreen.org/facts-figures/
https://northerngreen.org/feed/
https://northerngreen.org/home/feed/
https://northerngreen.org/hotels/
https://northerngreen.org/interactive-track/
https://northerngreen.org/internet/
https://northerngreen.org/keynote-address/
https://northerngreen.org/marketing-opportunities/
https://northerngreen.org/marshaling-yard-parking/
https://northerngreen.org/master-classes/
https://northerngreen.org/move-in-and-move-out/
https://northerngreen.org/northern-green-app/
https://northerngreen.org/parking-directions/
https://northerngreen.org/policies-disclaimers/
https://northerngreen.org/registration/

https://northerngreen.org/silent-auction/
https://northerngreen.org/speakers/
https://northerngreen.org/trade-show-floor/
https://northerngreen.org/wp-admin/
https://northerngreen.org/wp-admin/js/widgets/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/icons/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/images/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/template.css.php
https://northerngreen.org/wp-content/uploads/
https://northerngreen.org/wp-content/uploads/2016/08/avada-slider-bg-beer.jpg
https://northerngreen.org/wp-content/uploads/2021/
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-150x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-177x142.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-200x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-300x214.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-300x225.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-320x202.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-400x300.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-460x295.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-540x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-600x450.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-669x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-66x66.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-700x441.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-768x576.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-800x400.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-150x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-177x142.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-200x167.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-300x214.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-300x250.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-320x202.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-400x333.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-460x295.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-510x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-510x400.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-66x66.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA.jpg
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-120-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-120.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-152-150x150.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-152-152x142.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-152-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-152.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-167-150x150.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-167-167x142.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-167-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-167.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-180-150x150.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-180-177x142.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-180-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-180.png

https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-150x150.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-177x142.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-200x200.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-300x214.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-300x300.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-320x202.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-400x400.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-460x295.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-512x272.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-512x400.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-512x441.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-64.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-150x50.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-177x50.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-66x50.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-150x100.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-177x100.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-200x50.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-300x100.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-300x75.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-320x100.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina.png
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-1024x614.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-1200x720.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-150x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-1536x922.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-177x142.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-200x120.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-300x180.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-300x214.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-320x202.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-400x240.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-460x295.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-540x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-600x360.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-669x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-66x66.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-700x441.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-768x461.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-800x480.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-940x400.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people.jpg
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-150x150.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-177x142.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-180x180.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-192x192.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-200x200.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-270x270.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-300x214.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-300x300.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-320x202.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-32x32.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-400x400.png

https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-460x295.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-512x272.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-512x400.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-512x441.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512.png
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-1024x683.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-150x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-177x142.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-200x133.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-300x200.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-300x214.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-320x202.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-400x267.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-460x295.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-540x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-600x400.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-669x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-66x66.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-700x441.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-768x512.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-800x533.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-940x400.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-1024x323.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-1200x379.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-150x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-1536x485.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-177x142.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-200x63.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-300x214.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-300x95.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-320x202.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-400x126.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-460x295.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-540x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-600x189.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-669x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-66x66.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-700x441.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-768x243.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-800x253.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-940x400.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top.jpg
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-1-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-1.png
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-2-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-2.png
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-3-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-3.png
https://northerngreen.org/wp-content/uploads/2021/11/NG22-Advance-Program-download.pdf
https://northerngreen.org/wp-includes/
https://northerngreen.org/wp-includes/ID3/
https://northerngreen.org/wp-includes/IXR/
https://northerngreen.org/wp-includes/PHPMailer/
https://northerngreen.org/wp-includes/Requests/

https://northerngreen.org/wp-includes/SimplePie/
https://northerngreen.org/wp-includes/Text/
https://northerngreen.org/wp-includes/admin-bar.php
https://northerngreen.org/wp-includes/assets/
https://northerngreen.org/wp-includes/atomlib.php
https://northerngreen.org/wp-includes/author-template.php
https://northerngreen.org/wp-includes/block-editor.php
https://northerngreen.org/wp-includes/block-i18n.json
https://northerngreen.org/wp-includes/block-patterns.php
https://northerngreen.org/wp-includes/block-patterns/
https://northerngreen.org/wp-includes/block-supports/
https://northerngreen.org/wp-includes/block-template-utils.php
https://northerngreen.org/wp-includes/block-template.php
https://northerngreen.org/wp-includes/blocks.php
https://northerngreen.org/wp-includes/blocks/
https://northerngreen.org/wp-includes/bookmark-template.php
https://northerngreen.org/wp-includes/bookmark.php
https://northerngreen.org/wp-includes/cache-compat.php
https://northerngreen.org/wp-includes/cache.php
https://northerngreen.org/wp-includes/canonical.php
https://northerngreen.org/wp-includes/capabilities.php
https://northerngreen.org/wp-includes/category-template.php
https://northerngreen.org/wp-includes/category.php
https://northerngreen.org/wp-includes/certificates/
https://northerngreen.org/wp-includes/class-IXR.php
https://northerngreen.org/wp-includes/class-feed.php
https://northerngreen.org/wp-includes/class-http.php
https://northerngreen.org/wp-includes/class-json.php
https://northerngreen.org/wp-includes/class-oembed.php
https://northerngreen.org/wp-includes/class-phpass.php
https://northerngreen.org/wp-includes/class-phpmailer.php
https://northerngreen.org/wp-includes/class-pop3.php
https://northerngreen.org/wp-includes/class-requests.php
https://northerngreen.org/wp-includes/class-simplepie.php
https://northerngreen.org/wp-includes/class-smtp.php
https://northerngreen.org/wp-includes/class-snoopy.php
https://northerngreen.org/wp-includes/class-walker-category-dropdown.php
https://northerngreen.org/wp-includes/class-walker-category.php
https://northerngreen.org/wp-includes/class-walker-comment.php
https://northerngreen.org/wp-includes/class-walker-nav-menu.php
https://northerngreen.org/wp-includes/class-walker-page-dropdown.php
https://northerngreen.org/wp-includes/class-walker-page.php
https://northerngreen.org/wp-includes/class-wp-admin-bar.php
https://northerngreen.org/wp-includes/class-wp-ajax-response.php
https://northerngreen.org/wp-includes/class-wp-application-passwords.php
https://northerngreen.org/wp-includes/class-wp-block-editor-context.php
https://northerngreen.org/wp-includes/class-wp-block-list.php
https://northerngreen.org/wp-includes/class-wp-block-parser.php
https://northerngreen.org/wp-includes/class-wp-block-pattern-categories-registry.php
https://northerngreen.org/wp-includes/class-wp-block-patterns-registry.php
https://northerngreen.org/wp-includes/class-wp-block-styles-registry.php
https://northerngreen.org/wp-includes/class-wp-block-supports.php
https://northerngreen.org/wp-includes/class-wp-block-template.php
https://northerngreen.org/wp-includes/class-wp-block-type-registry.php
https://northerngreen.org/wp-includes/class-wp-block-type.php
https://northerngreen.org/wp-includes/class-wp-block.php

https://northerngreen.org/wp-includes/class-wp-comment-query.php
https://northerngreen.org/wp-includes/class-wp-comment.php
https://northerngreen.org/wp-includes/class-wp-customize-control.php
https://northerngreen.org/wp-includes/class-wp-customize-manager.php
https://northerngreen.org/wp-includes/class-wp-customize-nav-menus.php
https://northerngreen.org/wp-includes/class-wp-customize-panel.php
https://northerngreen.org/wp-includes/class-wp-customize-section.php
https://northerngreen.org/wp-includes/class-wp-customize-setting.php
https://northerngreen.org/wp-includes/class-wp-customize-widgets.php
https://northerngreen.org/wp-includes/class-wp-date-query.php
https://northerngreen.org/wp-includes/class-wp-dependency.php
https://northerngreen.org/wp-includes/class-wp-editor.php
https://northerngreen.org/wp-includes/class-wp-embed.php
https://northerngreen.org/wp-includes/class-wp-error.php
https://northerngreen.org/wp-includes/class-wp-fatal-error-handler.php
https://northerngreen.org/wp-includes/class-wp-feed-cache-transient.php
https://northerngreen.org/wp-includes/class-wp-feed-cache.php
https://northerngreen.org/wp-includes/class-wp-hook.php
https://northerngreen.org/wp-includes/class-wp-http-cookie.php
https://northerngreen.org/wp-includes/class-wp-http-curl.php
https://northerngreen.org/wp-includes/class-wp-http-encoding.php
https://northerngreen.org/wp-includes/class-wp-http-ixr-client.php
https://northerngreen.org/wp-includes/class-wp-http-proxy.php
https://northerngreen.org/wp-includes/class-wp-http-requests-hooks.php
https://northerngreen.org/wp-includes/class-wp-http-requests-response.php
https://northerngreen.org/wp-includes/class-wp-http-response.php
https://northerngreen.org/wp-includes/class-wp-http-streams.php
https://northerngreen.org/wp-includes/class-wp-http.php
https://northerngreen.org/wp-includes/class-wp-image-editor-gd.php
https://northerngreen.org/wp-includes/class-wp-image-editor-imagick.php
https://northerngreen.org/wp-includes/class-wp-image-editor.php
https://northerngreen.org/wp-includes/class-wp-list-util.php
https://northerngreen.org/wp-includes/class-wp-locale-switcher.php
https://northerngreen.org/wp-includes/class-wp-locale.php
https://northerngreen.org/wp-includes/class-wp-matchesmapregex.php
https://northerngreen.org/wp-includes/class-wp-meta-query.php
https://northerngreen.org/wp-includes/class-wp-metadata-lazyloader.php
https://northerngreen.org/wp-includes/class-wp-network-query.php
https://northerngreen.org/wp-includes/class-wp-network.php
https://northerngreen.org/wp-includes/class-wp-object-cache.php
https://northerngreen.org/wp-includes/class-wp-oembed-controller.php
https://northerngreen.org/wp-includes/class-wp-oembed.php
https://northerngreen.org/wp-includes/class-wp-paused-extensions-storage.php
https://northerngreen.org/wp-includes/class-wp-post-type.php
https://northerngreen.org/wp-includes/class-wp-post.php
https://northerngreen.org/wp-includes/class-wp-query.php
https://northerngreen.org/wp-includes/class-wp-recovery-mode-cookie-service.php
https://northerngreen.org/wp-includes/class-wp-recovery-mode-email-service.php

Scan Diagnostics — port 2079 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page http://server.northerngreenexpo.org:2079/ fetched. Status code:401, Content-Type:text/html, load time:104 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 0 requests, 4 seconds. Completed 0 requests of 38 estimated requests (0%). All tests completed.
HSTS Analysis no tests enabled.
Collected 1 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(9 x 1) + paths:(0 x 1) = total (9)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 1 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 9 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #4 WebCgiOob: estimated time < 1 minute (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 58 estimated requests (1.72414%). All tests completed.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (46 tests, 0 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (46 tests, 1 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 59 requests, 1 seconds. Completed 59 requests of 126 estimated requests (46.8254%). XSS optimization removed 29 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
cve_2017_9805 no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(4 x 1) + paths:(11 x 1) = total (15)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 1 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 14 requests, 1 seconds. Completed 14 requests of 15 estimated requests (93.3333%). All tests completed.
Tomcat Vuln manipulation no tests enabled.
Time based path manipulation no tests enabled.
Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 0) + files:(10 x 0) + directories:(94 x 1) + paths:(9 x 1) = total (103)
Batch #5 Path manipulation: estimated time < 1 minute (116 tests, 1 inputs)
Batch #5 Path manipulation: 116 vulnsigs tests, completed 102 requests, 1 seconds. Completed 102 requests of 103 estimated requests (99.0291%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 1 minute (125 tests, 1 inputs)
Batch #5 WebCgiGeneric: 125 vulnsigs tests, completed 56 requests, 1 seconds. Completed 56 requests of 173 estimated requests (32.3699%). All tests completed.
Total requests made: 285
Average server response time: 0.11 seconds

Average browser load time: 0.12 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

SSL Certificate - Information — port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:

N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl

(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07
(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d

(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl

(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6
(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)

(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:
(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b
(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4

(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

Scan Diagnostics — port 2077 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page http://server.northerngreenexpo.org:2077/ fetched. Status code:401, Content-Type:text/html, load time:105 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 0 requests, 4 seconds. Completed 0 requests of 38 estimated requests (0%). All tests completed.
HSTS Analysis no tests enabled.
Collected 1 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(9 x 1) + paths:(0 x 1) = total (9)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 1 inputs)

WS Directory Path manipulation: 9 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 9 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #4 WebCgiOob: estimated time < 1 minute (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 58 estimated requests (1.72414%). All tests completed.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (46 tests, 0 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (46 tests, 1 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 59 requests, 1 seconds. Completed 59 requests of 126 estimated requests (46.8254%). XSS optimization removed 29 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
cve_2017_9805 no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(4 x 1) + paths:(11 x 1) = total (15)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 1 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 14 requests, 0 seconds. Completed 14 requests of 15 estimated requests (93.3333%). All tests completed.
Tomcat Vuln manipulation no tests enabled.
Time based path manipulation no tests enabled.
Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 0) + files:(10 x 0) + directories:(94 x 1) + paths:(9 x 1) = total (103)
Batch #5 Path manipulation: estimated time < 1 minute (116 tests, 1 inputs)
Batch #5 Path manipulation: 116 vulnsigs tests, completed 102 requests, 1 seconds. Completed 102 requests of 103 estimated requests (99.0291%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 1 minute (125 tests, 1 inputs)
Batch #5 WebCgiGeneric: 125 vulnsigs tests, completed 54 requests, 2 seconds. Completed 54 requests of 173 estimated requests (31.2139%). All tests completed.
Total requests made: 283
Average server response time: 0.12 seconds

Average browser load time: 0.12 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

SSL Server Information Retrieval — port 587 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH

DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH

TLSv1.3 PROTOCOL IS DISABLED

Links Rejected By Crawl Scope or Exclusion List — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:26:14.0

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

External links discovered:
https://book.passkey.com/go/NorthernGreen2022
https://spothero.com/minneapolis-parking?sha_affiliate=meetmn
https://www.biddingforgood.com/auction/item/browse.action?auctionId=341698447
https://www.biddingforgood.com/auction/item/donate.action?auctionId=341698447
https://www.irrigation.org/IA/Certification/Maintain-Your-Certification/IA/Certification/Maintain-Your-Certification.aspx?hkey=94f8c009-ef08-4c73-b44e-e70f486c282f
https://www.gertenswholesale.com/
https://www.ihg.com/holidayinnexpress/hotels/us/en/minneapolis/mspdt/hoteldetail?fromRedirect=true&qSrt=sBR&qIta=99801505&icdv=99801505&qSIH=MSPDT&qGrpCd=MNL&setPMCookies=true&qSHBrC=EX&qDest=225%20South%20Eleventh%20Street,%20Minneapolis,%20MN,%20US&srb_u=1
https://e.issuu.com/embed.html?backgroundColor=%23f3f3f3&backgroundColorFullscreen=%23f3f3f3&d=ng22-advance-program-web&doAutoflipPages=true&hideIssuuLogo=true&logoImageUrl=https%3A%2F%2Fnortherngreen.org%2Fwp-content%2Fuploads%2F2021%2F11%2FNorthernGreenLogo-issuu.png&u=northerngreenexpo
https://e.issuu.com/embed.html?d=ng22-quick-guide-web&u=northerngreenexpo
https://whova.com/
https://whova.com/hybrid-event-platform/
https://whova.com/static/frontend/agenda_webpage/js/embedagenda.js?eid=north1_202201&host=https://whova.com
https://whova.com/static/frontend/xems/js/whova-speaker-widget.js?eid=north1_202201&
https://www.circlekfleetcards.com/
https://mtgf.org/
https://www.dot.state.mn.us/35w94/
https://mnla.biz/
https://www.minneapolis.org/minneapolis-convention-center/about/cleaning-protocols/
https://www.minneapolis.org/minneapolis-convention-center/attendees/
https://gravatar.com/
https://www.bachmanswholesale.com/departments
https://www.zieglercat.com/specials
https://www.zieglercat.com/specials/
https://www.hunterindustries.com/
https://www.rivercitylawnscape.com/careers
https://res.windsurfercrs.com/ibe/details.aspx?propertyid=13527&nights=5&checkin=01/09/2022&group=2201GREENE
https://www.hlsoutdoor.com/en
https://www.baileynurseries.com/
https://www.googletagmanager.com/gtag/js?id=UA-54228640-1
https://s3.amazonaws.com/meet-minneapolis/craft/cms/Attendee-Safety-Security-KBYG.pdf?mtime=20210922113243
https://maps.google.com/maps/embed/v1/place?q=Minneapolis%20Convention%20Center,1301%202nd%20Ave%20S%2C%20Minneapolis%2C%20MN%2C%2055404%2C%20US&center=44.9688369%2C-93.273865&zoom=14&key=AIzaSyAz-iChz547udxDFQBQrRwP3TJMIg0e8xY
https://ncma.org/education/segmental-retaining-walls/srw-installer/
https://ncma.org/programs/srw-certifications/basic-srw-installer-certification/
https://itunes.apple.com/app/apple-store/id716979741?pt=1944835&ct=&mt=8
https://www.apld.org/certification/
https://www.youtube.com/embed/KMTBQVupzbk?wmode=transparent&autoplay=0
https://www.youtube.com/user/NorthernGreenExpo
https://www.hyatt.com/en-US/group-booking/MSPRM/G-MNUR
https://www.turfsupradio.com/
https://play.google.com/store/apps/details?id=com.whova.event&referrer=utm_source%3D%26utm_medium%3Dportal%26utm_content%3Dnorth1_202201
https://www.expocad.com/host/fx/northerngreen/2022ngw/exfx.html
https://www.siteone.com/
https://www.isa-arbor.com/Credentials/Maintaining-Credentials/Post-Approved-CEUs
https://www.mtgf.org/
https://urldefense.com/v3/__https:/gbac.issa.com/issa-gbac-star-facility-accreditation/__;!!EB7VV9psZ_sHly7zVFY!AkPXxwixCvj_A8ekqRrCNS-FXxGLsM7mE8FgdwZ_5cUYTzHBWT5RGX6vIxmBygWWJwr40XWgbNJg7w$

https://s.w.org/
https://www.mnla.biz/
https://youtu.be/DuyC6MiGZIc
https://globalplasmasolutions.com/how-it-works
https://twitter.com/NorthernGreenMN
https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html
https://www.cdc.gov/coronavirus/2019-ncov/vaccines/fully-vaccinated.html
https://www.bartlett.com/
http://mn.gov/aelslagid/continuinged.html
http://mn.gov/aelslagid/forms/ceform.pdf
http://www.gbac.org/
http://cdn.minneapolis.org/digital_files/154/downtown_minneapolis_parking_map.pdf
http://www.provenwinners-shrubs.com/
http://www.mtgf.org/
http://www.mnla.biz/
http://www.metrotransit.org/ride-free-on-nicollet-mall.aspx
tel:6516334987
tel:763-295-5420

IP based excluded links:

WordPress Present — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13061
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2014-10-27 23:53:36.0

THREAT:
WordPress is an open source blogging tool and a content management system (CMS). WordPress is present on the target.

IMPACT:
n/a

SOLUTION:
n/a

RESULT:
WordPress 5.9 was detected at https://northerngreen.org/

SSL Server default Diffie-Hellman prime information — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38609
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-05-26 22:09:34.0

THREAT:

Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS. - For fixed primes: 1024 and below are considered unsafe. - For variable primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

SSL server default to use Diffie-Hellman key exchange method with variable 2048(bits) prime

TLS Secure Renegotiation Extension Support Information — port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and

thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 995 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

Default Web Page (Follow HTTP Redirection) — port 2077 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:

nas-201911-01

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2077

<html>Authorization Required</html>

Links Rejected By Crawl Scope or Exclusion List — port 2080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:26:14.0

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

RESULT:

Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

IP based excluded links:

Web Server Supports HTTP Request Pipelining — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	86565
Category:	Web server
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2005-02-23 00:25:38.0

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker, it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:
N/A

RESULT:
GET / HTTP/1.1
Host:162.144.102.68:443

GET /Q_Evasive/ HTTP/1.1
Host:162.144.102.68:443

HTTP/1.1 200 OK
Date: Wed, 26 Jan 2022 14:27:26 GMT
Server: Apache
Link: <https://northerngreen.org/wp-json/>; rel="https://api.w.org/", <https://northerngreen.org/wp-json/wp/v2/pages/21>; rel="alternate"; type="application/json", <https://northerngreen.org/>; rel=shortlink
Cache-Control: max-age=604800
Expires: Wed, 02 Feb 2022 14:27:26 GMT
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

0

HTTP/1.1 301 Moved Permanently
Date: Wed, 26 Jan 2022 14:27:27 GMT
Server: Apache
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Redirect-By: WordPress
Location: https://162.144.102.68/Q_Evasive/
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

GET / HTTP/1.1
Host:162.144.102.68:443

GET /Q_Evasive/ HTTP/1.1
Host:162.144.102.68:443

HTTP/1.1 200 OK
Date: Wed, 26 Jan 2022 14:27:28 GMT
Server: Apache
Link: <https://northerngreen.org/wp-json/>; rel="https://api.w.org/", <https://northerngreen.org/wp-json/wp/v2/pages/21>; rel="alternate"; type="application/json", <https://northerngreen.org/>; rel=shortlink
Cache-Control: max-age=604800
Expires: Wed, 02 Feb 2022 14:27:28 GMT
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

0

HTTP/1.1 301 Moved Permanently
Date: Wed, 26 Jan 2022 14:27:28 GMT
Server: Apache
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Redirect-By: WordPress
Location: https://162.144.102.68/Q_Evasive/
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 143 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.					

2				
RSA	2048	no	110	low
DHE	1024	yes	80	low
ECDHE secp384r1	384	yes	192	low

Operating Systems Detected on Redirected TCP Open Ports

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	82038
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2003-04-08 20:21:12.0

THREAT:

A redirected TCP open port is a port that is not native to the host scanned. It may belong to another host that is either closer to or further away from the scanner.

The service detected one or more redirected TCP open ports and finger-printed the operating systems these ports belong to.

When a redirected TCP open port is detected, it may be difficult for the service to determine whether the port is native to the host. Ports displayed as "redirected" may actually be native and vice versa.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Redirected Port	OS
465	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
2079	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
2096	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
3306	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
995	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
993	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-

26	IP
587	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
2095	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 21 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no

Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 993 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS

TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

SSL Server Information Retrieval — port 993 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM

AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH

TLSv1.3 PROTOCOL IS DISABLED

Default Web Page — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

GET / HTTP/1.0

Host: server.northerngreenexpo.org:2080

<html>Authorization Required</html>

Links Crawled — port 2080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 8.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

https://server.northerngreenexpo.org:2080/

SSL Session Caching Information — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1 session caching is enabled on the target.
TLSv1.1 session caching is enabled on the target.
TLSv1.2 session caching is enabled on the target.

Referrer-Policy HTTP Security Header Not Detected — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:26.0

THREAT:
No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:
The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:
Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

RESULT:
Referrer-Policy HTTP Header missing on 2082 port.

Maximum Number of Links Reached During Crawl — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150026
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:46.0

THREAT:
The maximum number of links specified for this scan has been reached. The links crawled to reach this threshold can include requests made via HTML form submissions and links requested in anonymous and authenticated states. Consequently, the list of links crawled (QID 150009) may reflect a lower number than the combination of links and forms requested during the crawl.

IMPACT:
Some links that lead to different areas of the site's functionality may have been missed.

SOLUTION:
Increase the maximum number of links in order to ensure broader coverage of the Web application. It is important to note that increasing the number of links crawled can dramatically increase the time required to test the Web application.

RESULT:
Maximum request count reached: 300

Links Crawled — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 1475.00
Number of links: 300
(This number excludes form requests and links re-requested during authentication.)

https://northerngreen.org/
https://northerngreen.org/author/ng-staff/
https://northerngreen.org/awards-celebration/
https://northerngreen.org/book-your-booth/
https://northerngreen.org/booth-display-rules/
https://northerngreen.org/ceo-mgmt-track/
https://northerngreen.org/ceus/
https://northerngreen.org/comments/feed/
https://northerngreen.org/contact-us/
https://northerngreen.org/covid-safety/
https://northerngreen.org/digital-swag-bag/
https://northerngreen.org/education/
https://northerngreen.org/exhibitor-registration/
https://northerngreen.org/facts-figures/
https://northerngreen.org/feed/

https://northerngreen.org/home/feed/
https://northerngreen.org/hotels/
https://northerngreen.org/interactive-track/
https://northerngreen.org/internet/
https://northerngreen.org/keynote-address/
https://northerngreen.org/marketing-opportunities/
https://northerngreen.org/marshaling-yard-parking/
https://northerngreen.org/master-classes/
https://northerngreen.org/move-in-and-move-out/
https://northerngreen.org/northern-green-app/
https://northerngreen.org/parking-directions/
https://northerngreen.org/policies-disclaimers/
https://northerngreen.org/registration/
https://northerngreen.org/silent-auction/
https://northerngreen.org/speakers/
https://northerngreen.org/trade-show-floor/
https://northerngreen.org/wp-admin/
https://northerngreen.org/wp-admin/js/widgets/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/icons/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/images/
https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/template.css.php
https://northerngreen.org/wp-content/uploads/
https://northerngreen.org/wp-content/uploads/2016/08/avada-slider-bg-beer.jpg
https://northerngreen.org/wp-content/uploads/2021/
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-150x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-177x142.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-200x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-300x214.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-300x225.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-320x202.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-400x300.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-460x295.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-540x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-600x450.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-669x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-66x66.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-700x441.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-768x576.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile-800x400.jpg
https://northerngreen.org/wp-content/uploads/2021/06/800x600-heart-smile.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-150x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-177x142.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-200x167.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-300x214.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-300x250.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-320x202.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-400x333.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-460x295.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-510x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-510x400.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA-66x66.jpg
https://northerngreen.org/wp-content/uploads/2021/06/Bachmans-June-MNLA.jpg
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-120-66x66.png

https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-120.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-152-150x150.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-152-152x142.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-152-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-152.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-167-150x150.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-167-167x142.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-167-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-167.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-180-150x150.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-180-177x142.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-180-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-180.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-150x150.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-177x142.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-200x200.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-300x214.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-300x300.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-320x202.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-400x400.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-460x295.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-512x272.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-512x400.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-512x441.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-512.png
https://northerngreen.org/wp-content/uploads/2021/06/NG-favicon-64.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-150x50.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-177x50.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-66x50.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-150x100.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-177x100.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-200x50.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-300x100.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-300x75.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-320x100.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/NorthernGreenLogo-horiz-short-lgtype-retina.png
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-1024x614.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-1200x720.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-150x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-1536x922.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-177x142.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-200x120.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-300x180.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-300x214.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-320x202.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-400x240.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-460x295.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-540x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-600x360.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-669x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-66x66.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-700x441.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-768x461.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-800x480.jpg

https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people-940x400.jpg
https://northerngreen.org/wp-content/uploads/2021/06/avada-slider-bg-GC-people.jpg
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-150x150.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-177x142.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-180x180.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-192x192.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-200x200.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-270x270.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-300x214.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-300x300.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-320x202.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-32x32.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-400x400.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-460x295.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-512x272.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-512x400.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-512x441.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/cropped-NG-favicon-512.png
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-1024x683.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-150x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-177x142.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-200x133.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-300x200.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-300x214.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-320x202.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-400x267.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-460x295.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-540x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-600x400.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-669x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-66x66.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-700x441.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-768x512.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-800x533.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG-940x400.jpg
https://northerngreen.org/wp-content/uploads/2021/06/heart-smile-LG.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-1024x323.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-1200x379.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-150x150.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-1536x485.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-177x142.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-200x63.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-300x214.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-300x95.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-320x202.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-400x126.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-460x295.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-540x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-600x189.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-669x272.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-66x66.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-700x441.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-768x243.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-800x253.jpg
https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top-940x400.jpg

https://northerngreen.org/wp-content/uploads/2021/06/page-bar-top.jpg
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-1-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-1.png
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-2-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-2.png
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-3-66x66.png
https://northerngreen.org/wp-content/uploads/2021/06/testimonial-pic-3.png
https://northerngreen.org/wp-content/uploads/2021/11/NG22-Advance-Program-download.pdf
https://northerngreen.org/wp-includes/
https://northerngreen.org/wp-includes/ID3/
https://northerngreen.org/wp-includes/IXR/
https://northerngreen.org/wp-includes/PHPMailer/
https://northerngreen.org/wp-includes/Requests/
https://northerngreen.org/wp-includes/SimplePie/
https://northerngreen.org/wp-includes/Text/
https://northerngreen.org/wp-includes/admin-bar.php
https://northerngreen.org/wp-includes/assets/
https://northerngreen.org/wp-includes/atomlib.php
https://northerngreen.org/wp-includes/author-template.php
https://northerngreen.org/wp-includes/block-editor.php
https://northerngreen.org/wp-includes/block-i18n.json
https://northerngreen.org/wp-includes/block-patterns.php
https://northerngreen.org/wp-includes/block-patterns/
https://northerngreen.org/wp-includes/block-supports/
https://northerngreen.org/wp-includes/block-template-utils.php
https://northerngreen.org/wp-includes/block-template.php
https://northerngreen.org/wp-includes/blocks.php
https://northerngreen.org/wp-includes/blocks/
https://northerngreen.org/wp-includes/bookmark-template.php
https://northerngreen.org/wp-includes/bookmark.php
https://northerngreen.org/wp-includes/cache-compat.php
https://northerngreen.org/wp-includes/cache.php
https://northerngreen.org/wp-includes/canonical.php
https://northerngreen.org/wp-includes/capabilities.php
https://northerngreen.org/wp-includes/category-template.php
https://northerngreen.org/wp-includes/category.php
https://northerngreen.org/wp-includes/certificates/
https://northerngreen.org/wp-includes/class-IXR.php
https://northerngreen.org/wp-includes/class-feed.php
https://northerngreen.org/wp-includes/class-http.php
https://northerngreen.org/wp-includes/class-json.php
https://northerngreen.org/wp-includes/class-oembed.php
https://northerngreen.org/wp-includes/class-phpass.php
https://northerngreen.org/wp-includes/class-phpmailer.php
https://northerngreen.org/wp-includes/class-pop3.php
https://northerngreen.org/wp-includes/class-requests.php
https://northerngreen.org/wp-includes/class-simplepie.php
https://northerngreen.org/wp-includes/class-smtp.php
https://northerngreen.org/wp-includes/class-snoopy.php
https://northerngreen.org/wp-includes/class-walker-category-dropdown.php
https://northerngreen.org/wp-includes/class-walker-category.php
https://northerngreen.org/wp-includes/class-walker-comment.php
https://northerngreen.org/wp-includes/class-walker-nav-menu.php
https://northerngreen.org/wp-includes/class-walker-page-dropdown.php
https://northerngreen.org/wp-includes/class-walker-page.php
https://northerngreen.org/wp-includes/class-wp-admin-bar.php

https://northerngreen.org/wp-includes/class-wp-ajax-response.php
https://northerngreen.org/wp-includes/class-wp-application-passwords.php
https://northerngreen.org/wp-includes/class-wp-block-editor-context.php
https://northerngreen.org/wp-includes/class-wp-block-list.php
https://northerngreen.org/wp-includes/class-wp-block-parser.php
https://northerngreen.org/wp-includes/class-wp-block-pattern-categories-registry.php
https://northerngreen.org/wp-includes/class-wp-block-patterns-registry.php
https://northerngreen.org/wp-includes/class-wp-block-styles-registry.php
https://northerngreen.org/wp-includes/class-wp-block-supports.php
https://northerngreen.org/wp-includes/class-wp-block-template.php
https://northerngreen.org/wp-includes/class-wp-block-type-registry.php
https://northerngreen.org/wp-includes/class-wp-block-type.php
https://northerngreen.org/wp-includes/class-wp-block.php
https://northerngreen.org/wp-includes/class-wp-comment-query.php
https://northerngreen.org/wp-includes/class-wp-comment.php
https://northerngreen.org/wp-includes/class-wp-customize-control.php
https://northerngreen.org/wp-includes/class-wp-customize-manager.php
https://northerngreen.org/wp-includes/class-wp-customize-nav-menus.php
https://northerngreen.org/wp-includes/class-wp-customize-panel.php
https://northerngreen.org/wp-includes/class-wp-customize-section.php
https://northerngreen.org/wp-includes/class-wp-customize-setting.php
https://northerngreen.org/wp-includes/class-wp-customize-widgets.php
https://northerngreen.org/wp-includes/class-wp-date-query.php
https://northerngreen.org/wp-includes/class-wp-dependency.php
https://northerngreen.org/wp-includes/class-wp-editor.php
https://northerngreen.org/wp-includes/class-wp-embed.php
https://northerngreen.org/wp-includes/class-wp-error.php
https://northerngreen.org/wp-includes/class-wp-fatal-error-handler.php
https://northerngreen.org/wp-includes/class-wp-feed-cache-transient.php
https://northerngreen.org/wp-includes/class-wp-feed-cache.php
https://northerngreen.org/wp-includes/class-wp-hook.php
https://northerngreen.org/wp-includes/class-wp-http-cookie.php
https://northerngreen.org/wp-includes/class-wp-http-curl.php
https://northerngreen.org/wp-includes/class-wp-http-encoding.php
https://northerngreen.org/wp-includes/class-wp-http-ixr-client.php
https://northerngreen.org/wp-includes/class-wp-http-proxy.php
https://northerngreen.org/wp-includes/class-wp-http-requests-hooks.php
https://northerngreen.org/wp-includes/class-wp-http-requests-response.php
https://northerngreen.org/wp-includes/class-wp-http-response.php
https://northerngreen.org/wp-includes/class-wp-http-streams.php
https://northerngreen.org/wp-includes/class-wp-http.php
https://northerngreen.org/wp-includes/class-wp-image-editor-gd.php
https://northerngreen.org/wp-includes/class-wp-image-editor-imagick.php
https://northerngreen.org/wp-includes/class-wp-image-editor.php
https://northerngreen.org/wp-includes/class-wp-list-util.php
https://northerngreen.org/wp-includes/class-wp-locale-switcher.php
https://northerngreen.org/wp-includes/class-wp-locale.php
https://northerngreen.org/wp-includes/class-wp-matchesmapregex.php
https://northerngreen.org/wp-includes/class-wp-meta-query.php
https://northerngreen.org/wp-includes/class-wp-metadata-lazyloader.php
https://northerngreen.org/wp-includes/class-wp-network-query.php
https://northerngreen.org/wp-includes/class-wp-network.php
https://northerngreen.org/wp-includes/class-wp-object-cache.php
https://northerngreen.org/wp-includes/class-wp-oembed-controller.php
https://northerngreen.org/wp-includes/class-wp-oembed.php
https://northerngreen.org/wp-includes/class-wp-paused-extensions-storage.php

https://northerngreen.org/wp-includes/class-wp-post-type.php
https://northerngreen.org/wp-includes/class-wp-post.php
https://northerngreen.org/wp-includes/class-wp-query.php
https://northerngreen.org/wp-includes/class-wp-recovery-mode-cookie-service.php
https://northerngreen.org/wp-includes/class-wp-recovery-mode-email-service.php

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 587 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1					
RSA		2048	no	110	low
DHE		2048	yes	110	low
ECDHE	secp256r1	256	yes	128	low
TLSv1.1					
RSA		2048	no	110	low
DHE		2048	yes	110	low
ECDHE	secp256r1	256	yes	128	low
TLSv1.2					
RSA		2048	no	110	low
DHE		2048	yes	110	low
ECDHE	secp256r1	256	yes	128	low

Links Crawled — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Duration of crawl phase (seconds): 16.00
Number of links: 18
(This number excludes form requests and links re-requested during authentication.)

http://server.northerngreenexpo.org:2095/
http://server.northerngreenexpo.org:2095/?locale=ar
http://server.northerngreenexpo.org:2095/?locale=bg
http://server.northerngreenexpo.org:2095/?locale=cs
http://server.northerngreenexpo.org:2095/?locale=da
http://server.northerngreenexpo.org:2095/?locale=de
http://server.northerngreenexpo.org:2095/?locale=el
http://server.northerngreenexpo.org:2095/?locale=en
http://server.northerngreenexpo.org:2095/?locale=es
http://server.northerngreenexpo.org:2095/?locale=es_419
http://server.northerngreenexpo.org:2095/?locale=es_es
http://server.northerngreenexpo.org:2095/?locale=fi
http://server.northerngreenexpo.org:2095/?locale=fil
http://server.northerngreenexpo.org:2095/?locale=fr
http://server.northerngreenexpo.org:2095/?locale=he

http://server.northerngreenexpo.org:2095/?locale=hu
http://server.northerngreenexpo.org:2095/?locale=i_cpanel_snowmen
http://server.northerngreenexpo.org:2095/crossdomain.xml

Apache Web Server Detected — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86496
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-10-03 12:30:55.0

THREAT:
Apache, the open source web server software that is developed and maintained by Apache Software Foundation is detected on the host.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
Apache web server detected on port 80 - Apache/2.x

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	yes
SCT extension	no
TLSv1.3	
Heartbeat	no
Cipher priority controlled by	client
OCSP stapling	yes
SCT extension	no

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1				
RSA	2048	no	110	low
ECDHE secp256r1	256	yes	128	low
ECDHA secp256r1	256	yes	128	low
TLSv1. 1				
RSA	2048	no	110	low
ECDHE secp256r1	256	yes	128	low
ECDHA secp256r1	256	yes	128	low
TLSv1. 2				
RSA	2048	no	110	low
ECDHE secp256r1	256	yes	128	low
ECDHA secp256r1	256	yes	128	low

Links Rejected By Crawl Scope or Exclusion List — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Last Update:	2021-03-16 23:26:14.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

External links discovered:
https://go.cpanel.net/ie11deprecation
https://go.cpanel.net/privacy
http://wikipedia.org/wiki/Case_sensitivity

IP based excluded links:

List of Web Directories — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Directory	Source
/cgi-bin/	brute force
/webmail/	brute force
/login/	brute force
/wp-content/plugins/	brute force
/social/	brute force
/admin/	brute force
/2/	brute force
/3/	brute force
/mailman/listinfo/	brute force
/basilix/class/	brute force
/admin	brute force
/wordpress//	brute force
/wp-content/	brute force
/wp-login.php/	brute force
/wp-content/	web page
/wp-content/uploads/	web page
/wp-content/uploads/2021/	web page
/wp-content/uploads/2021/06/	web page
/wp-content/plugins/	web page
/wp-content/plugins/bsa-plugin-pro-scripteo/	web page
/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/	web page
/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/	web page
/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/	web page
/wp-includes/	web page
/wp-includes/js/	web page
/wp-includes/js/jquery/	web page
/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/	web page
/wp-content/uploads/2021/07/	web page
/wp-content/uploads/2021/12/	web page
/m/	brute force
/joomla/index.php	brute force
/drupal/index.php	brute force
/training/	brute force
	brute

/Training/	force
/2016/	brute force
/designs/imm/index.php	brute force
/index.php	brute force
/wp-admin	brute force
/login	brute force
/img-sys/	web page
/wp-content/uploads/fusion-styles/	web page
/wp-json/	web page
/wp-json/wp/	web page
/wp-json/wp/v2/	web page
/wp-json/wp/v2/pages/	web page
/wp-json/oembed/	web page
/wp-json/oembed/1.0/	web page
/wp-content/uploads/fusion-scripts/	web page
/wp-content/uploads/2016/	web page
/wp-content/uploads/2016/08/	web page
/wp-login.php/	web page

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

Default Web Page — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2095

<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">
<meta name="google" content="notranslate" />
<meta name="apple-itunes-app" content="app-id=1188352635" />
<title>Webmail Login</title>
<link rel="shortcut icon" href="
AAABAAEAICAAAAEAIADSAgAAFgAAAIlQTkcNChoKAAAADUlIRFIAAAAgAAAAIAgGAAAAc3p69AAAAplJREFUWIXt1j2IHGUYB

/DfOzdnjIKFkECIVWIKvUFsIkRExa9KJCLaWAgWJx4DilZWgpDDiI0wiViIoGATP1CCEDYHSeCwUBBkgiiKURQJFiLo4d0eOxYzC8nsO9m9XcXC+8MW+3z+9
/l6l2383xH+iSBpElyTdoda26xsDqp/h0CVZ3vwKm7tMBngAs7h7eRYebG6hMtMBHbMBX89vfARHprQ5U8cwdFQlIOZCVR5di1+w/wWXT
/EY6EoN5NZCODuKZLDwzgSMCuBe2fwfX6QZwtpWzqfBBtLC3txF/ZhxKbBGx0EfsTJS77vwmGjlZrD4mUzUOXZjVjGI65cnTXchB8iupdDUb7QinsQZ7GzZftdQj2JVZ49iC
/w6JjksIo7OnS9tiA5Vn6GtyK2+1MY5NkhfGDygVrBAxH5WkPuMjR7/3UsUFLl2Q68s4XkA3ws3v9zoSjX28Kr5wL1xrTxa6ou+f6OZGvqPg9v1wZeaUjcELE/DVfNhWFSvy
/enOIZ9eq1sTokEMNLWI79oirP8g6fXpVnh7GEvY1sV/OJ4f0UhyKKk6EoX4x5pEkgXv6L6OM99YqNw
/c4kXSwG5nkIfpLCynuiahW1GWeJHkfT4aiXO9atz1XcD6I6yLyHu6bIPk6Hg9FeYZ63y9EjBarPDvQ8VJ1nd9V3D4m+RncForyxFCQ4hSeahlej88Hefauurdwaufr5z/F
/ZHAX6nL+mZE18e36IWiHLkFocqzW9QXcNz1+wUHxJ/f10JRPjvGP4pk/vj5L3F8AtufdD+/p6dJDknzX+05fDLGtife
/766t9MRgFCUffWTudwE3AqBlVCUf0xLYGTQqzzbhydwJ3Y34g318J1tmX+DPBTlz9MS2MY2/nP8DTGaqeTDf30rAAAAAElFTkSuQmCC" type="image/x-icon" />

<!-- EXTERNAL CSS -->
<link href="/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css" rel="stylesheet" type="text/css" />
<link href="/cPanel_magic_revision_1626170558/unprotected/cpanel/style_v2_optimized.css" rel="stylesheet" type="text/css" />

<style type="text/css">
/*
This css is included in the base template in case the css cannot be loaded because of access restrictions
If this css is updated, please update securitypolicy_header.html.tmpl as well
*/
.copyright {
background: url(
PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIzNTlwdCIgaGVpZ2h0PSIzMjAiIHZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xp

background-size: 25px auto;
}
</style>
<!--[if IE 6]>
<style type="text/css">
img {
behavior: url(/cPanel_magic_revision_1367939018/unprotected/cp_pngbehavior_login.htc);
}
</style>
<![endif]-->

<script>
window.DOM = { get: function(id) { return document.getElementById(id) } };
</script>
</head>
<body class="wm">

<input type="hidden" id="goto_uri" value="/" />
<input type="hidden" id="goto_app" value="" />
<!-- Do not remove msg_code as it is needed for automated testing - msg_code:[] -->

<noscript>

JavaScript is disabled in your browser.
For Webmail to function properly, you must enable JavaScript.
If you do not enable JavaScript, certain features in Webmail will not function correctly.

</noscript>

You have logged out.

The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the cPanel Blog.

Please select a locale:
X Close

etina

dansk

Deutsch

English

espaol

espaol latinoamericano

espaol de Espaa

suomi

Filipino

franais

magyar

 cPanel Snowmen - i_cpanel_snowmen

i_en

Bahasa Indonesia

italiano

Bahasa Melayu

norsk bokml

Nederlands

Norwegian

polski

portugus

portugus do Brasil

romn

slovenina

svenska

Trke

Ting Vit


```
</div>
</div>
<div id="content-container">
<div id="login-container">

<div id="login-sub-container">
<div id="login-sub-header">

<img class="main-logo" src="/cPanel_magic_revision_1454480643/unprotected/cpanel/images/webmail-logo.svg" alt="logo" />

</div>
<div id="login-sub"
>
<div id="clickthrough_form" style="visibility:hidden">
<form action="javascript:void(0)">
<div class="notices"></div>
<button type="submit" class="clickthrough-cont-btn">Continue</button>
</form>
</div>
<div id="forms">
<form novalidate id="login_form" action="/login/" method="post" target="_top" style="visibility:">
<div class="input-req-login"><label for="user">Email Address</label></div>
<div class="input-field-login icon username-container">
<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your email address." class="std_textbox" type="text" tabindex="1" required>
</div>
<div class="input-req-login login-password-field-label"><label for="pass">Password</label></div>
<div class="input-field-login icon password-container">
<input name="pass" id="pass" placeholder="Enter your email password." class="std_textbox" type="password" tabindex="2" required>
</div>
<div class="controls">
<div class="login-btn">
<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>
</div>

</div>
<div class="clear" id="push"></div>
</form>
<!--CLOSE forms -->
</div>
<!--CLOSE login-sub -->
</div>



<!--CLOSE wrapper -->
</div>
<!--CLOSE login-sub-container -->
</div>
<!--CLOSE login-container -->
</div>

<div id="locale-footer">
<div class="locale-container">
<noscript>
<form method="get" action=".">
<select name="locale">
<option value="">Change locale</option>
```

<option value='ar'></option><option value='bg'></option><option value='cs'>etina</option><option value='da'>dansk</option><option value='de'>Deutsch</option><option value='el'></option><option value='en'>English</option><option value='es'>espaol</option><option value='es_419'>espaol latinoamericano</option><option value='es_es'>espaol de Espaa</option><option value='fi'>suomi</option><option value='fil'>Filipino</option><option value='fr'>franais</option><option value='he'></option><option value='hu'>magyar</option><option value='i_cpanel_snowmen'> cPanel Snowmen - i_cpanel_snowmen</option><option value='i_en'>i_en</option><option value='id'>Bahasa Indonesia</option><option value='it'>italiano</option><option value='ja'></option><option value='ko'></option><option value='ms'>Bahasa Melayu</option><option value='nb'>norsk bokml</option><option value='nl'>Nederlands</option><option value='no'>Norwegian</option><option value='pl'>polski</option><option value='pt'>portugus</option><option value='pt_br'>portugus do Brasil</option><option value='ro'>romn</option><option value='ru'></option><option value='sl'>slovenina</option><option value='sv'>svenska</option><option value='th'></option><option value='tr'>Trke</option><option value='uk'></option><option value='vi'>Ting Vit</option><option value='zh'></option><option value='zh_cn'></option><option value='zh_tw'></option> </select>
<button style="margin-left: 10px" type="submit">Change</button>
</form>
<style type="text/css">#mobilelocalemenu, #locales_list {display:none}</style>
</noscript>
<ul id="locales_list">

etina

dansk

Deutsch

English

espaol

Select a locale:
English

<!--Close login-wrapper -->

<script>
var MESSAGES = {"invalid_login":"The login is invalid.","success":"Login successful. Redirecting ","ajax_timeout":"The connection timed out. Please try again.","internal_error":"An internal error occurred. If this condition persists, contact the system administrator.","read_below":"Read the important information below.","

session_locale":"The desired locale has been saved to your browser. To change the locale in this browser again, select another locale on this screen.","no_username":" You must specify a username to log in.","authenticating":"Authenticating ","network_error":"A network error occurred during your login request. Please try again. If this condition persists, contact your network service provider."};

window.IS_LOGOUT = false;

//login.js
"use strict";var FADE_DURATION=.45;var FADE_DELAY=20;var AJAX_TIMEOUT=3e4;var LOCALE_FADES=[];var HAS_CSS_OPACITY="opacity"in document.body.style;var login_form=DOM.get("login_form");var login_username_el=DOM.get("user");var login_password_el=DOM.get("pass");var login_submit_el=DOM.get("login_submit");var goto_app=DOM.get("goto_app");var goto_uri=DOM.get("goto_uri");var div_cache={"login-page":DOM.get("login-page")||false,"locale-container":DOM.get("locale-container")||false,"login-container":DOM.get("login-container")||false,"locale-footer":DOM.get("locale-footer")||false,"content-cell":DOM.get("content-container")||false,invalid:DOM.get("invalid")||false};var content_cell=div_cache["content-cell"];if(div_cache["locale-footer"]){div_cache["locale-footer"].style.display="block"}var reset_form=DOM.get("reset_form");var set_opacity;if(HAS_CSS_OPACITY){set_opacity=function setOpacity(el,opacity){el.style.opacity=opacity}}else{var filter_regex=/(DXImageTransform\.Microsoft\.Alpha\(\)[^)]*\)/;set_opacity=function setOpacity(el,opacity){var filter_text=el.currentStyle.filter;if(!filter_text){el.style.filter="progid:DXImageTransform.Microsoft.Alpha(enabled=true)"}else if(!filter_regex.test(filter_text)){el.style.filter+=" progid:DXImageTransform.Microsoft.Alpha(enabled=true)"}else{var new_filter=filter_text.replace(filter_regex,"$1enabled=true)");if(new_filter!==filter_text){el.style.filter=new_filter}}try{el.filters.item("DXImageTransform.Microsoft.Alpha").opacity=opacity*100}catch(e){try{el.filters.item("alpha").opacity=opacity*100}catch(error){}}}}function toggle_locales(show_locales){while(LOCALE_FADES.length){clearInterval(LOCALE_FADES.shift())}var newly_shown=div_cache[show_locales?"locale-container":"login-container"];set_opacity(newly_shown,0);if(HAS_CSS_OPACITY){content_cell.replaceChild(newly_shown,content_cell.children[0])}else{var old=content_cell.children[0];content_cell.insertBefore(newly_shown,old);newly_shown.style.display="";old.style.display="none"}LOCALE_FADES.push(fade_in(newly_shown));LOCALE_FADES.push((show_locales?fade_out:fade_in)("locale-footer"))}function showIEBanner(){if(navigator.userAgent.indexOf("Trident")!==-1){var ieBannerDiv=document.getElementById("IE-warning");if(ieBannerDiv){ieBannerDiv.classList.remove("IE-warning-hide")}}}showIEBanner();function fade_in(el,duration,_fade_out_instead){el=div_cache[el]||DOM.get(el)||el;var style_obj=el.style;var interval;var cur_style=window.getComputedStyle?getComputedStyle(el,null):el.currentStyle;var visibility=cur_style.visibility;var start_opacity;if(el.offsetWidth&&visibility!=="hidden"){if(window.getComputedStyle){start_opacity=Number(cur_style.opacity)}else{try{start_opacity=el.filters.item("DXImageTransform.Microsoft.Alpha").opacity}catch(e){try{start_opacity=el.filters("alpha").opacity}catch(error){start_opacity=100}}start_opacity/=100}if(!start_opacity){start_opacity=0}}else{start_opacity=0;set_opacity(el,0)}if(_fade_out_instead&&start_opacity<.01){if(start_opacity){set_opacity(el,0)}return}if(!duration){duration=FADE_DURATION}var duration_ms=duration*1e3;var start=new Date;var end;if(_fade_out_instead){end=duration_ms+start.getTime()}else{style_obj.visibility="visible"}var fader=function(){var opacity;if(_fade_out_instead){opacity=start_opacity*(end-new Date)/duration_ms;if(opacity<=0){opacity=0;clearInterval(interval);style_obj.visibility="hidden"}}else{opacity=start_opacity+(1-start_opacity)*(new Date-start)/duration_ms;if(opacity>=1){opacity=1;clearInterval(interval)}}set_opacity(el,opacity)};fader();interval=setInterval(fader,FADE_DELAY);return interval}function fade_out(el,timeout){return fade_in(el,timeout,true)}function AjaxObject(url,callbackFunction){this._url=url;this._callback=callbackFunction||function(){}}AjaxObject.prototype.updating=false;AjaxObject.prototype.abort=function(){if(this.updating){this.AJAX.abort();delete this.AJAX}};AjaxObject.prototype.update=function(passData,postMethod){if(this.AJAX){return false}var ajax=null;if(window.XMLHttpRequest){ajax=new XMLHttpRequest}else if(window.ActiveXObject){ajax=new window.ActiveXObject("Microsoft.XMLHTTP")}else{return false}var timeout;var that=this;ajax.onreadystatechange=function(){if(ajax.readyState==4){clearTimeout(timeout);that.updating=false;that._callback(ajax);delete that.AJAX}};try{var uri;timeout=setTimeout(function(){that.abort();show_status(MESSAGES.ajax_timeout,"error")},AJAX_TIMEOUT);if(/post/i.test(postMethod)){uri=this._url+"?login_only=1";ajax.open("POST",uri,true);ajax.setRequestHeader("Content-type","application/x-www-form-urlencoded");ajax.send(passData)}else{uri=this._url+"?"+passData+"&timestamp="+(new Date).getTime();ajax.open("GET",uri,true);ajax.send(null)}this.AJAX=ajax;this.updating=true}catch(e){login_form.submit()}return true};var _text_content="textContent"in document.body?"textContent":"innerText";function _process_parsed_login_success(result){var final_uri;var login_url_regex=/^\/(?:logout|login|openid_connect_callback)\/?/;if(result.redirect&&!login_url_regex.test(result.redirect)){final_uri=result.redirect}var location_obj_to_redirect;if(/^(?:\/cpsess[^/]+)\/$/.test(final_uri)){location_obj_to_redirect=top.location}else{if(result.security_token&&top!==window){for(var f=0;f<top.frames.length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result.security_token);top.frames[f].location.href=href}}}location_obj_to_redirect=location}var redirector=function(){location_obj_to_redirect.href=final_uri+location.hash};if(result.notices&&result.notices.length){show_status(MESSAGES.read_below,"warn");var click_form=DOM.get("clickthrough_form");var container=click_form.querySelector(".notices");for(var n=0;n<result.notices.length;n++){var new_p=document.createElement("p");new_p.textContent=result.notices[n].content;container.appendChild(new_p)}click_form.onsubmit=redirector;fade_out(login_form);fade_in(click_form)}else{show_status(MESSAGES.success,"success");fade_out("content-container",FADE_DURATION/2);redirector()}}var login_button={button:login_submit_el,_suppressed_disabled:null,suppress:function(){if(this._suppressed_disabled===null){this._suppressed_disabled=this.button.disabled;this.button.disabled=true}},release:function(){if(this._suppressed_disabled!==null){this.button.disabled=this._suppressed_disabled;this._suppressed_disabled=null}},queue_disabled:function(state){if(this._suppressed_disabled===null){this.button.disabled=state}else{this._suppressed_disabled=state}}};function login_results(ajax_obj){var result;try{result=JSON.parse(ajax_obj&&ajax_obj.responseText)}catch(e){result=null}var response_status=ajax_obj.status;if(response_status===200){if(result){if(result.session){window.SubmitPost.submit(result.redirect,{session:result.session,goto_uri:result.goto_uri})}else{_process_parsed_login_success(result)}}else{login_form.submit()}return}else{if(parseInt(response_status/100,10)===4){var msg_code=result&&result.message;show_status(MESSAGES[msg_code||"invalid_login"]||MESSAGES.invalid_login,"error");set_status_timeout()}else{show_status(MESSAGES.network_error,"error")}document.body.classList.remove("logging-in");login_button.release();return}}var level_classes={info:"info-notice",error:"error-notice",success:"success-notice",warn:"warn-notice"};var levels_regex="";Object.keys(level_classes).forEach(function(lv){levels_regex+="|"+level_classes[lv]});levels_regex=new RegExp("\\b(?:"+levels_regex.slice(1)+")\\b");function show_status(message,level){DOM.get("login-status-message")[_text_content]=message;var container=DOM.get("login-status");var this_class=level&&level_classes[level]||level_classes.info;var el_class=container.className.replace(levels_regex,this_class);container.className=el_class;fade_in

(container);reset_status_timeout()}var STATUS_TIMEOUT=null;function reset_status_timeout(){clearTimeout(STATUS_TIMEOUT);STATUS_TIMEOUT=null}function set_status_timeout(delay){STATUS_TIMEOUT=setTimeout(function(){fade_out("login-status")},delay||8e3)}var LOGIN_SUBMIT_OK=true;document.body.onkeyup=function(){LOGIN_SUBMIT_OK=true};document.body.onmousedown=function(){LOGIN_SUBMIT_OK=true};function do_login(){if(LOGIN_SUBMIT_OK){LOGIN_SUBMIT_OK=false;if(login_username_el.value.length===0){show_status(MESSAGES.no_username,"error");return false}document.body.classList.add("logging-in");login_button.suppress();show_status(MESSAGES.authenticating,"info");var goto_app_query=goto_app&&goto_app.value?"&goto_app="+encodeURIComponent(goto_app.value):"";var goto_uri_query=goto_uri&&goto_uri.value?"&goto_uri="+encodeURIComponent(goto_uri.value):"";var ajax_login=new AjaxObject(login_form.action,login_results);ajax_login.update("user="+encodeURIComponent(login_username_el.value)+"&pass="+encodeURIComponent(login_password_el.value)+goto_app_query+goto_uri_query,"POST")}return false}function show_login(){var select_user_form=document.getElementById("select_user_form");select_user_form.style.display="none";var login_form=document.getElementById("login_form");login_form.style.visibility="";var select_users_option_block=document.getElementById("select_users_option_block");select_users_option_block.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="block"}function show_select_user(){var login_form=document.getElementById("login_form");login_form.style.visibility="hidden";var select_users_option_block=document.getElementById("select_users_option_block");select_users_option_block.style.display="none";var select_user_form=document.getElementById("select_user_form");select_user_form.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="none"}if(!window.JSON){login_button.suppress();var new_script=document.createElement("script");new_script.onreadystatechange=function(){if(this.readyState==="loaded"||this.readyState==="complete"){this.onreadystatechange=null;window.JSON={parse:window.jsonParse};window.jsonParse=undefined;login_button.release()}};new_script.src="/unprotected/json-minified.js";document.getElementsByTagName("head")[0].appendChild(new_script)}try{login_form.onsubmit=do_login;set_opacity(DOM.get("login-wrapper"),0);LOCALE_FADES.push(fade_in("login-wrapper"));var preload=document.createElement("div");preload.id="preload_images";document.body.insertBefore(preload,document.body.firstChild);if(window.IS_LOGOUT){set_status_timeout(1e4)}else if(/(?:\?|&)locale=[^&]/.test(location.search)){show_status(MESSAGES.session_locale)}setTimeout(function(){login_username_el.focus()},100)}catch(e){if(window.console){console.warn(e)}}

//submit_post.js
(function(context){"use strict";var DOC=context.document;function _wrongType(name,value){throw new Error(""+name+" must be a string, number, or array, not "+value)}var scalarTypeIsOk={number:true,string:true};function submit(url,args){var myform=DOC.createElement("form");myform.method="POST";myform.action=url;myform.style.display="none";Object.keys(args).forEach(function(name){var values;if("object"===typeof args[name]){if(args[name]instanceof Array){values=args[name]}else{_wrongType(name,args[name])}}else if(scalarTypeIsOk[typeof args[name]]){values=[args[name]]}else{_wrongType(name,args[name])}values.forEach(function(val){var myvar=DOC.createElement("input");myvar.type="hidden";myvar.name=name;myvar.value=val;myform.appendChild(myvar)})});DOC.documentElement.appendChild(myform);myform.submit();DOC.documentElement.removeChild(myform)}context.SubmitPost={submit:submit}})(window);

//jstz.min.js
/*! jstz - v1.0.4 - 2012-12-18 */
(function(e){var t=function(){"use strict";var e="s",n=function(e){var t=-e.getTimezoneOffset();return t!==null?t:0},r=function(e,t,n){var r=new Date;return e!==undefined&&r.setFullYear(e),r.setDate(n),r.setMonth(t),r},i=function(e){return n(r(e,0,2))},s=function(e){return n(r(e,5,2))},o=function(e){var t=e.getMonth()>7?s(e.getFullYear()):i(e.getFullYear()),r=n(e);return t-r!==0},u=function(){var t=i(),n=s(),r=i()-s();return r<0?t+",1":r>0?n+",1,"+e:t+",0"},a=function(){var e=u();return new t.TimeZone(t.olson.timezones[e])},f=function(e){var t=new Date(2010,6,15,1,0,0,0),n={"America/Denver":new Date(2011,2,13,3,0,0,0),"America/Mazatlan":new Date(2011,3,3,3,0,0,0),"America/Chicago":new Date(2011,2,13,3,0,0,0),"America/Mexico_City":new Date(2011,3,3,3,0,0,0),"America/Asuncion":new Date(2012,9,7,3,0,0,0),"America/Santiago":new Date(2012,9,3,3,0,0,0),"America/Campo_Grande":new Date(2012,9,21,5,0,0,0),"America/Montevideo":new Date(2011,9,2,3,0,0,0),"America/Sao_Paulo":new Date(2011,9,16,5,0,0,0),"America/Los_Angeles":new Date(2011,2,13,8,0,0,0),"America/Santa_Isabel":new Date(2011,3,5,8,0,0,0),"America/Havana":new Date(2012,2,10,2,0,0,0),"America/New_York":new Date(2012,2,10,7,0,0,0),"Asia/Beirut":new Date(2011,2,27,1,0,0,0),"Europe/Helsinki":new Date(2011,2,27,4,0,0,0),"Europe/Istanbul":new Date(2011,2,28,5,0,0,0),"Asia/Damascus":new Date(2011,3,1,2,0,0,0),"Asia/Jerusalem":new Date(2011,3,1,6,0,0,0),"Asia/Gaza":new Date(2009,2,28,0,30,0,0),"Africa/Cairo":new Date(2009,3,25,0,30,0,0),"Pacific/Auckland":new Date(2011,8,26,7,0,0,0),"Pacific/Fiji":new Date(2010,11,29,23,0,0,0),"America/Halifax":new Date(2011,2,13,6,0,0,0),"America/Goose_Bay":new Date(2011,2,13,2,1,0,0),"America/Miquelon":new Date(2011,2,13,5,0,0,0),"America/Godthab":new Date(2011,2,27,1,0,0,0),"Europe/Moscow":t,"Asia/Yekaterinburg":t,"Asia/Omsk":t,"Asia/Krasnoyarsk":t,"Asia/Irkutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0,0)};return n[e]};return{determine:a,date_is_dst:o,dst_start_for:f}}();t.TimeZone=function(e){"use strict";var n={"America/Denver":["America/Denver","America/Mazatlan"],"America/Chicago":["America/Chicago","America/Mexico_City"],"America/Santiago":["America/Santiago","America/Asuncion","America/Campo_Grande"],"America/Montevideo":["America/Montevideo","America/Sao_Paulo"],"Asia/Beirut":["Asia/Beirut","Europe/Helsinki","Europe/Istanbul","Asia/Damascus","Asia/Jerusalem","Asia/Gaza"],"Pacific/Auckland":["Pacific/Auckland","Pacific/Fiji"],"America/Los_Angeles":["America/Los_Angeles","America/Santa_Isabel"],"America/New_York":["America/Havana","America/New_York"],"America/Halifax":["America/Goose_Bay","America/Halifax"],"America/Godthab":["America/Miquelon","America/Godthab"],"Asia/Dubai":["Europe/Moscow"],"Asia/Dhaka":["Asia/Yekaterinburg"],"Asia/Jakarta":["Asia/Omsk"],"Asia/Shanghai":["Asia/Krasnoyarsk","Australia/Perth"],"Asia/Tokyo":["Asia/Irkutsk"],"Australia/Brisbane":["Asia/Yakutsk"],"Pacific/Noumea":["Asia/Vladivostok"],"Pacific/Tarawa":["Asia/Kamchatka"],"Africa/Johannesburg":["Asia/Gaza","Africa/Cairo"],"Asia/Baghdad":["Europe/Minsk"]},r=e,i=function(){var e=n[r],i=e.length,s=0,o=e[0];for(;s<i;s+=1){o=e[s];if(t.date_is_dst(t.dst_start_for(o))){r=o;return}}},s=function(){return typeof n[r]!="undefined"};return s()&&i(),{name:function(){return r}}},t.olson={},t.olson.timezones={"-720,0":"Etc/GMT+12","-660,0":"Pacific/Pago_Pago","-600,1":"America/Adak","-600,0":"Pacific/Honolulu","-570,0":"Pacific/Marquesas","-540,0":"Pacific/Gambier","-540,1":"America/Anchorage","-480,1":"America/Los_Angeles","-480,0":"Pacific/Pitcairn","-420,0":"America/Phoenix","-420,1":"America/Denver","-360,0":"America/Guatemala","-360,1":"America/Chicago","-360,1,s":"Pacific/Easter","-300,0":"America/Bogota","-300,1":"America/New_York","-270,0":"America/Caracas","-240,1":"America/Halifax","-240,0":"America/Santo_Domingo","-240,1,s":"America/Santiago","-210,1":"America/St_Johns","-180,1":"America/Godthab","-180,0":"America/Argentina/Buenos_Aires","-180,1,s":"America/Montevideo","-120,0":"Etc/GMT+2","-120,1":"Etc/GMT+2","-60,1":"Atlantic/Azores","-60,0":"Atlantic/Cape_Verde","0,0":"Etc/UTC","0,1":"Europe/London","60,1":"

Europe/Berlin","60,0":"Africa/Lagos","60,1,s":"Africa/Windhoek","120,1":"Asia/Beirut","120,0":"Africa/Johannesburg","180,0":"Asia/Baghdad","180,1":"Europe/Moscow","210,1":"Asia/Tehran","240,0":"Asia/Dubai","240,1":"Asia/Baku","270,0":"Asia/Kabul","300,1":"Asia/Yekaterinburg","300,0":"Asia/Karachi","330,0":"Asia/Kolkata","345,0":"Asia/Kathmandu","360,0":"Asia/Dhaka","360,1":"Asia/Omsk","390,0":"Asia/Rangoon","420,1":"Asia/Krasnoyarsk","420,0":"Asia/Jakarta","480,0":"Asia/Shanghai","480,1":"Asia/Irkutsk","525,0":"Australia/Eucla","525,1,s":"Australia/Eucla","540,1":"Asia/Yakutsk","540,0":"Asia/Tokyo","570,0":"Australia/Darwin","570,1,s":"Australia/Adelaide","600,0":"Australia/Brisbane","600,1":"Asia/Vladivostok","600,1,s":"Australia/Sydney","630,1,s":"Australia/Lord_Howe","660,1":"Asia/Kamchatka","660,0":"Pacific/Noumea","690,0":"Pacific/Norfolk","720,1,s":"Pacific/Auckland","720,0":"Pacific/Tarawa","765,1,s":"Pacific/Chatham","780,0":"Pacific/Tongatapu","780,1,s":"Pacific/Apia","840,0":"Pacific/Kiritimati"},typeof exports!="undefined"?exports.jstz=t:e.jstz=t})(this);
//cptimezone_optimized.js
(function(window){"use strict";var JSTZ_RELATIVE_PATH="sharedjs/jstz.min.js";var TIMEZONE_COOKIE="timezone";var COOKIE_TIMEZONE_MISMATCH_CLASS="if-timezone-cookie-needs-update";var DETECTED_TZ_CLASS="detected-timezone";var SHOWN_CLASS="shown";function _get_cookie(sKey){return decodeURIComponent(document.cookie.replace(new RegExp("(?:(?:^|.*;)\\s*"+encodeURIComponent(sKey).replace(/[\-\.\+*]/g,"\\$&")+"\\s*\\=\\s*([^;]*).*$)|^.*$"),"$1"))||null}function _detect_timezone(){return window.jstz.determine().name()}function reset_timezone_and_reload(){return reset_timezone(location.reload.bind(location))}function _set_cookie(callback){document.cookie=TIMEZONE_COOKIE+"="+_detect_timezone()+"; path=/";if(callback){callback()}}function set_timezone_if_unset(on_success){return!_get_cookie(TIMEZONE_COOKIE)&&reset_timezone(on_success)}function reset_timezone(on_success){_set_cookie(on_success);return true}function set_timezone_and_reload_if_unset(){return set_timezone_if_unset(location.reload.bind(location))}function show_cookie_timezone_mismatch_nodes(){var detected_tz=_detect_timezone();if(detected_tz!==_get_cookie(TIMEZONE_COOKIE)){var detected_nodes=document.querySelectorAll("."+DETECTED_TZ_CLASS);[].forEach.call(detected_nodes,function(n){n.textContent=detected_tz});var show_nodes=document.querySelectorAll("."+COOKIE_TIMEZONE_MISMATCH_CLASS);[].forEach.call(show_nodes,function(n){n.className+=" "+SHOWN_CLASS})}}window.CPTimezone={show_cookie_timezone_mismatch_nodes:show_cookie_timezone_mismatch_nodes,reset_timezone_and_reload:reset_timezone_and_reload,reset_timezone:reset_timezone,set_timezone_and_reload_if_unset:set_timezone_and_reload_if_unset}})(window);

```
CPTimezone.reset_timezone();
</script>

<style>
@media (min-width: 481px) {
#select_user_form {
width: px;
}
}
</style>
<div class="copyright">Copyright2022 cPanel, L.L.C.
<br /><a href="https://go.cpanel.net/privacy" target="_blank">Privacy Policy</a></div>

</body>

</html>
```

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2				
RSA	2048	no	110	low
ECDHE x448	448	yes	224	low
ECDHE x25519	256	yes	128	low
ECDHE secp384r1	384	yes	192	low
ECDHE secp256r1	256	yes	128	low
ECDHE secp521r1	521	yes	260	low
TLSv1.3				
ECDHE x25519	256	yes	128	low
ECDHE secp256r1	256	yes	128	low
ECDHE x448	448	yes	224	low
ECDHE secp521r1	521	yes	260	low
ECDHE secp384r1	384	yes	192	low

Links Rejected By Crawl Scope or Exclusion List — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:26:14.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

External links discovered:
https://go.cpanel.net/cleardnscache
http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=500referral
http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=cpanelwhmreferral

IP based excluded links:

Scan Time Limit Reached — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150024
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-01-27 21:02:50.0

THREAT:
The scan engine reached its internal time limit for this scan. The scan was stopped in order to collect and report the results so far.

IMPACT:
Not all tests have been completed. Therefore, some vulnerabilities may exist in the target application on links that the scanner has not yet tested. The scanner uses an iterative approach to determine the order in which links are tested. Links are selected in a breadth-first manner that takes into account how many connections each link has to other pages. This helps the scanner identify and test popular links first in order to have a useful coverage of the web application.

SOLUTION:
Application responsiveness is the most important factor in overall scan time. Review the average server response time reported by the scanner. Anything over 2 seconds is quite slow.

Scan time can potentially be reduced by one or more of the following methods:

- Make changes to improve the application's responsiveness.
- Increase the scan intensity setting.
- Reduce the SmartScan depth setting.
- Add redundant links configuration to reduce the number of unnecessary tests being performed.
- For applications with a large number of cookies, exclude the cookie/header tests (QIDs 150002, 150046, 150047, 150048).
- Exclude particular QIDs such as those related to XSS or SQL injection (and consequently running multiple scans with different QIDs enabled).

RESULT:
Scan stopped at established time limit in order to report results.

External Links Discovered — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:
External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Number of links: 3
https://go.cpanel.net/cleardnscache
http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=500referral
http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=cpanelwhmreferral

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1				
RSA	2048	no	110	low
DHE	2048	yes	110	low
ECDHE secp256r1	256	yes	128	low
TLSv1.1				
RSA	2048	no	110	low
DHE	2048	yes	110	low
ECDHE secp256r1	256	yes	128	low
TLSv1.2				
RSA	2048	no	110	low
DHE	2048	yes	110	low
ECDHE secp256r1	256	yes	128	low

TLS Secure Renegotiation Extension Support Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	42350
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Default Web Page (Follow HTTP Redirection) port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:

nas-201911-01

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2086

```
<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">
<meta name="google" content="notranslate" />
<meta name="apple-itunes-app" content="app-id=1188352635" />
<title>WHM Login</title>
<link rel="shortcut icon" href="
AAABAAEAICAAAAEAIADSAgAAFgAAAIlQTkcNChoKAAAADUlIRFIAAAAgAAAAIAgGAAAAc3p69AAAAplJREFUWIXt1j2IHGUYB
/DfOzdnjIKFkECIVWIKvUFsIkRExa9KJCLaWAgWJx4DilZWgpDDiI0wiViIoGATP1CCEDYHSeCwUBBkgiiKURQJFiLo4d0eOxYzC8nsO9m9XcXC+8MW+3z+9
/l6l2383xH+iSBpElyTdoda26xsDqp/h0CVZ3vwKm7tMBngAs7h7eRYebG6hMtMBHbMBX89vfARHprQ5U8cwdFQlIOZCVR5di1+w/wWXT
/EY6EoN5NZCODuKZLDwzgSMCuBe2fwfX6QZwtpWzqfBBtLC3txF/ZhxKbBGx0EfsTJS77vwmGjlZrD4mUzUOXZjVjGI65cnTXchB8iupdDUb7QinsQZ7GzZftdQj2JVZ49iC
/w6JjksIo7OnS9tiA5Vn6GtyK2+1MY5NkhfGDygVrBAxH5WkPuMjR7/3UsUFLl2Q68s4XkA3ws3v9zoSjX28Kr5wL1xrTxa6ou+f6OZGvqPg9v1wZeaUjcELE/DVfNhWFSvy
/enOIZ9eq1sTokEMNLWI79oirP8g6fXpVnh7GEvY1sV/OJ4f0UhyKKk6EoX4x5pEkgXv6L6OM99YqNw
/c4kXSwG5nkIfpLCynuiahW1GWeJHkfT4aiXO9atz1XcD6I6yLyHu6bIPk6Hg9FeYZ63y9EjBarPDvQ8VJ1nd9V3D4m+RncForyxFCQ4hSeahlej88Hefauurdwaufr5z/F
/ZHAX6nL+mZE18e36IWiHLkFocqzW9QXcNz1+wUHxJ/f10JRPjvGP4pk/vj5L3F8AtufdD+/p6dJDknzX+05fDLGtife
/766t9MRgFCUffWTudwE3AqBlVCUf0xLYGTQqzzbhydwJ3Y34g318J1tmX+DPBTlz9MS2MY2/nP8DTGaqeTDf30rAAAAAElFTkSuQmCC" type="image/x-icon" />

<!-- EXTERNAL CSS -->
<link href="/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css" rel="stylesheet" type="text/css" />
<link href="/cPanel_magic_revision_1626170558/unprotected/cpanel/style_v2_optimized.css" rel="stylesheet" type="text/css" />

<style type="text/css">
/*
This css is included in the base template in case the css cannot be loaded because of access restrictions
If this css is updated, please update securitypolicy_header.html.tmpl as well
*/
.copyright {
background: url(
PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIzNTlwdCIgaGVpZ2h0PSIzMjAiIHZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xp

background-size: 25px auto;
}
</style>
<!--[if IE 6]>
<style type="text/css">
img {
behavior: url(/cPanel_magic_revision_1367939018/unprotected/cp_pngbehavior_login.htc);
}
</style>
<![endif]-->

<script>
window.DOM = { get: function(id) { return document.getElementById(id) } };
</script>
</head>
<body class="whm">

<input type="hidden" id="goto_uri" value="/" />
<input type="hidden" id="goto_app" value="" />
```

<!-- Do not remove msg_code as it is needed for automated testing - msg_code:[] -->

<noscript>

JavaScript is disabled in your browser.
For WHM to function properly, you must enable JavaScript.
If you do not enable JavaScript, certain features in WHM will not function correctly.

</noscript>

You have logged out.

The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the cPanel Blog.

Please select a locale:
X Close

etina

dansk

Deutsch

English

espaol

espaol latinoamericano

espaol de Espaa

suomi

Filipino

franais

magyar

 cPanel Snowmen - i_cpanel_snowmen

i_en

Bahasa Indonesia

italiano

Bahasa Melayu

norsk bokml

Nederlands

Norwegian

polski

portugus

portugus do Brasil

romn

slovenina

svenska

Trke

Ting Vit

<div id="login-sub"
>

<form action="javascript:void(0)">

<button type="submit" class="clickthrough-cont-btn">Continue</button>
</form>

<form novalidate id="login_form" action="/login/" method="post" target="_top" style="visibility:">
<label for="user">Username</label>

<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your username." class="std_textbox" type="text" tabindex="1" required>

<label for="pass">Password</label>

<input name="pass" id="pass" placeholder="Enter your account password." class="std_textbox" type="password" tabindex="2" required>

<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>

</form>
<!--CLOSE forms -->

<!--CLOSE login-sub -->

<!--CLOSE wrapper -->

```
</div>
<!--CLOSE login-sub-container -->
</div>
<!--CLOSE login-container -->
</div>

<div id="locale-footer">
<div class="locale-container">
<noscript>
<form method="get" action=".">
<select name="locale">
<option value="">Change locale</option>
<option value=&apos;ar&apos;></option><option value=&apos;bg&apos;></option><option value=&apos;cs&apos;>etina</option><option value=&apos;da&apos;
>dansk</option><option value=&apos;de&apos;>Deutsch</option><option value=&apos;el&apos;></option><option value=&apos;en&apos;>English</option><option
value=&apos;es&apos;>espaol</option><option value=&apos;es_419&apos;>espaol latinoamericano</option><option value=&apos;es_es&apos;>espaol de Espaa<
/option><option value=&apos;fi&apos;>suomi</option><option value=&apos;fil&apos;>Filipino</option><option value=&apos;fr&apos;>franais</option><option
value=&apos;he&apos;></option><option value=&apos;hu&apos;>magyar</option><option value=&apos;i_cpanel_snowmen&apos;> cPanel Snowmen -
i_cpanel_snowmen</option><option value=&apos;i_en&apos;>i_en</option><option value=&apos;id&apos;>Bahasa Indonesia</option><option value=&apos;it&apos;
>italiano</option><option value=&apos;ja&apos;></option><option value=&apos;ko&apos;></option><option value=&apos;ms&apos;>Bahasa Melayu</option><option
value=&apos;nb&apos;>norsk bokml</option><option value=&apos;nl&apos;>Nederlands</option><option value=&apos;no&apos;>Norwegian</option><option
value=&apos;pl&apos;>polski</option><option value=&apos;pt&apos;>portugus</option><option value=&apos;pt_br&apos;>portugus do Brasil</option><option
value=&apos;ro&apos;>romn</option><option value=&apos;ru&apos;></option><option value=&apos;sl&apos;>slovenina</option><option value=&apos;sv&apos;
>svenska</option><option value=&apos;th&apos;></option><option value=&apos;tr&apos;>Trke</option><option value=&apos;uk&apos;></option><option value=&apos;
vi&apos;>Ting Vit</option><option value=&apos;zh&apos;></option><option value=&apos;zh_cn&apos;></option><option value=&apos;zh_tw&apos;></option> </select>
<button style="margin-left: 10px" type="submit">Change</button>
</form>
<style type="text/css">#mobilelocalemenu, #locales_list {display:none}</style>
</noscript>
<ul id="locales_list">


<li><a href="/?locale=ar"></a></li>


<li><a href="/?locale=bg"></a></li>


<li><a href="/?locale=cs">etina</a></li>


<li><a href="/?locale=da">dansk</a></li>


<li><a href="/?locale=de">Deutsch</a></li>


<li><a href="/?locale=el"></a></li>


<li><a href="/?locale=en">English</a></li>


<li><a href="/?locale=es">espaol</a></li>


<li><a href="javascript:void(0)" id="morelocale" onclick="toggle_locales(true)" title="More locales"></a></li>
```

```
</ul>
<div id="mobilelocalemenu">Select a locale:
<a href="javascript:void(0)" onclick="toggle_locales(true)" title="Change locale">English</a>
</div>
</div>
</div>
</div>
<!--Close login-wrapper -->
</div>
<script>
var MESSAGES = {"invalid_login":"The login is invalid.","success":"Login successful. Redirecting ","ajax_timeout":"The connection timed out. Please try again.","
internal_error":"An internal error occurred. If this condition persists, contact the system administrator.","read_below":"Read the important information below.","
session_locale":"The desired locale has been saved to your browser. To change the locale in this browser again, select another locale on this screen.","no_username":"
You must specify a username to log in.","authenticating":"Authenticating ","network_error":"A network error occurred during your login request. Please try again. If this
condition persists, contact your network service provider."};

window.IS_LOGOUT = false;


//login.js
"use strict";var FADE_DURATION=.45;var FADE_DELAY=20;var AJAX_TIMEOUT=3e4;var LOCALE_FADES=[];var HAS_CSS_OPACITY="opacity"in document.body.
style;var login_form=DOM.get("login_form");var login_username_el=DOM.get("user");var login_password_el=DOM.get("pass");var login_submit_el=DOM.get
("login_submit");var goto_app=DOM.get("goto_app");var goto_uri=DOM.get("goto_uri");var div_cache={"login-page":DOM.get("login-page")||false,"locale-container":DOM.
get("locale-container")||false,"login-container":DOM.get("login-container")||false,"locale-footer":DOM.get("locale-footer")||false,"content-cell":DOM.get("content-container")
||false,invalid:DOM.get("invalid")||false};var content_cell=div_cache["content-cell"];if(div_cache["locale-footer"]){div_cache["locale-footer"].style.display="block"}var
reset_form=DOM.get("reset_form");var set_opacity;if(HAS_CSS_OPACITY){set_opacity=function setOpacity(el,opacity){el.style.opacity=opacity}}else{var filter_regex=/
(DXImageTransform\.Microsoft\.Alpha\()[^)]*\)/;set_opacity=function setOpacity(el,opacity){var filter_text=el.currentStyle.filter;if(!filter_text){el.style.filter="progid:
DXImageTransform.Microsoft.Alpha(enabled=true)"}else if(!filter_regex.test(filter_text)){el.style.filter+=" progid:DXImageTransform.Microsoft.Alpha(enabled=true)"}else
{var new_filter=filter_text.replace(filter_regex,"$1enabled=true)");if(new_filter!==filter_text){el.style.filter=new_filter}}try{el.filters.item("DXImageTransform.Microsoft.Alpha").
opacity=opacity*100}catch(e){try{el.filters.item("alpha").opacity=opacity*100}catch(error){}}}}function toggle_locales(show_locales){while(LOCALE_FADES.length)
{clearInterval(LOCALE_FADES.shift())}var newly_shown=div_cache[show_locales?"locale-container":"login-container"];set_opacity(newly_shown,0);if
(HAS_CSS_OPACITY){content_cell.replaceChild(newly_shown,content_cell.children[0])}else{var old=content_cell.children[0];content_cell.insertBefore(newly_shown,old);
newly_shown.style.display="";old.style.display="none"}LOCALE_FADES.push(fade_in(newly_shown));LOCALE_FADES.push((show_locales?fade_out:fade_in)("locale-
footer"))}function showIEBanner(){if(navigator.userAgent.indexOf("Trident")!==-1){var ieBannerDiv=document.getElementById("IE-warning");if(ieBannerDiv){ieBannerDiv.
classList.remove("IE-warning-hide")}}}showIEBanner();function fade_in(el,duration,_fade_out_instead){el=div_cache[el]||DOM.get(el)||el;var style_obj=el.style;var interval;
var cur_style=window.getComputedStyle?getComputedStyle(el,null):el.currentStyle;var visibility=cur_style.visibility;var start_opacity;if(el.offsetWidth&&visibility!=="
hidden"){if(window.getComputedStyle){start_opacity=Number(cur_style.opacity)}else{try{start_opacity=el.filters.item("DXImageTransform.Microsoft.Alpha").opacity}catch
(e){try{start_opacity=el.filters("alpha").opacity}catch(error){start_opacity=100}}start_opacity/=100}if(!start_opacity){start_opacity=0}}else{start_opacity=0;set_opacity(el,0)}if
(_fade_out_instead&&start_opacity<.01){if(start_opacity){set_opacity(el,0)}return}if(!duration){duration=FADE_DURATION}var duration_ms=duration*1e3;var start=new
Date;var end;if(_fade_out_instead){end=duration_ms+start.getTime()}else{style_obj.visibility="visible"}var fader=function(){var opacity;if(_fade_out_instead)
{opacity=start_opacity*(end-new Date)/duration_ms;if(opacity<=0){opacity=0;clearInterval(interval);style_obj.visibility="hidden"}}else{opacity=start_opacity+(1-
start_opacity)*(new Date-start)/duration_ms;if(opacity>=1){opacity=1;clearInterval(interval)}}set_opacity(el,opacity)};fader();interval=setInterval(fader,FADE_DELAY);
return interval}function fade_out(el,timeout){return fade_in(el,timeout,true)}function AjaxObject(url,callbackFunction){this._url=url;this.
_callback=callbackFunction||function(){}}AjaxObject.prototype.updating=false;AjaxObject.prototype.abort=function(){if(this.updating){this.AJAX.abort();delete this.AJAX}};
AjaxObject.prototype.update=function(passData,postMethod){if(this.AJAX){return false}var ajax=null;if(window.XMLHttpRequest){ajax=new XMLHttpRequest}else if
(window.ActiveXObject){ajax=new window.ActiveXObject("Microsoft.XMLHTTP")}else{return false}var timeout;var that=this;ajax.onreadystatechange=function(){if(ajax.
readyState==4){clearTimeout(timeout);that.updating=false;that._callback(ajax);delete that.AJAX}};try{var uri;timeout=setTimeout(function(){that.abort();show_status
(MESSAGES.ajax_timeout,"error")},AJAX_TIMEOUT);if(/post/i.test(postMethod)){uri=this._url+"?login_only=1";ajax.open("POST",uri,true);ajax.setRequestHeader
("Content-type","application/x-www-form-urlencoded");ajax.send(passData)}else{uri=this._url+"?"+passData+"&timestamp="+(new Date).getTime();ajax.open("GET",uri,
true);ajax.send(null)}this.AJAX=ajax;this.updating=true}catch(e){login_form.submit()}return true};var _text_content="textContent"in document.body?"textContent":"
innerText";function _process_parsed_login_success(result){var final_uri;var login_url_regex=/^\/(?:logout|login|openid_connect_callback)\/?/;if(result.redirect&&!
login_url_regex.test(result.redirect)){final_uri=result.redirect}var location_obj_to_redirect;if(/^(?:\/cpsess[^/]+)\/$/.test(final_uri)){location_obj_to_redirect=top.location}else{if
(result.security_token&&top!==window){for(var f=0;f<top.frames.length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result.
security_token);top.frames[f].location.href=href}}}location_obj_to_redirect=location}var redirector=function(){location_obj_to_redirect.href=final_uri+location.hash};if(result.
notices&&result.notices.length){show_status(MESSAGES.read_below,"warn");var click_form=DOM.get("clickthrough_form");var container=click_form.querySelector(".
notices");for(var n=0;n<result.notices.length;n++){var new_p=document.createElement("p");new_p.textContent=result.notices[n].content;container.appendChild(new_p)}
```

click_form.onsubmit=redirector;fade_out(login_form);fade_in(click_form)}else{show_status(MESSAGES.success,"success");fade_out("content-container",
FADE_DURATION/2);redirector()}}var login_button={button:login_submit_el,_suppressed_disabled:null,suppress:function(){if(this._suppressed_disabled===null){this.
_suppressed_disabled=this.button.disabled;this.button.disabled=true}},release:function(){if(this._suppressed_disabled!==null){this.button.disabled=this.
_suppressed_disabled;this._suppressed_disabled=null}},queue_disabled:function(state){if(this._suppressed_disabled===null){this.button.disabled=state}else{this.
_suppressed_disabled=state}}};function login_results(ajax_obj){var result;try{result=JSON.parse(ajax_obj&&ajax_obj.responseText)}catch(e){result=null}var
response_status=ajax_obj.status;if(response_status===200){if(result){if(result.session){window.SubmitPost.submit(result.redirect,{session:result.session,goto_uri:result.
goto_uri})}else{_process_parsed_login_success(result)}}else{login_form.submit()}return}else{if(parseInt(response_status/100,10)===4){var msg_code=result&&result.
message;show_status(MESSAGES[msg_code||"invalid_login"]||MESSAGES.invalid_login,"error");set_status_timeout()}else{show_status(MESSAGES.network_error,"
error")}document.body.classList.remove("logging-in");login_button.release();return}}var level_classes={info:"info-notice",error:"error-notice",success:"success-notice",
warn:"warn-notice"};var levels_regex="";Object.keys(level_classes).forEach(function(lv){levels_regex+="|"+level_classes[lv]});levels_regex=new RegExp("\\b(?:"
+levels_regex.slice(1)+")\\b");function show_status(message,level){DOM.get("login-status-message")[_text_content]=message;var container=DOM.get("login-status");var
this_class=level&&level_classes[level]||level_classes.info;var el_class=container.className.replace(levels_regex,this_class);container.className=el_class;fade_in
(container);reset_status_timeout()}var STATUS_TIMEOUT=null;function reset_status_timeout(){clearTimeout(STATUS_TIMEOUT);STATUS_TIMEOUT=null}function
set_status_timeout(delay){STATUS_TIMEOUT=setTimeout(function(){fade_out("login-status")},delay||8e3)}var LOGIN_SUBMIT_OK=true;document.body.
onkeyup=function(){LOGIN_SUBMIT_OK=true};document.body.onmousedown=function(){LOGIN_SUBMIT_OK=true};function do_login(){if(LOGIN_SUBMIT_OK)
{LOGIN_SUBMIT_OK=false;if(login_username_el.value.length===0){show_status(MESSAGES.no_username,"error");return false}document.body.classList.add("logging-
in");login_button.suppress();show_status(MESSAGES.authenticating,"info");var goto_app_query=goto_app&&goto_app.value?"&goto_app="+encodeURIComponent
(goto_app.value):"";var goto_uri_query=goto_uri&&goto_uri.value?"&goto_uri="+encodeURIComponent(goto_uri.value):"";var ajax_login=new AjaxObject(login_form.
action,login_results);ajax_login.update("user="+encodeURIComponent(login_username_el.value)+"&pass="+encodeURIComponent(login_password_el.value)
+goto_app_query+goto_uri_query,"POST")}return false}function show_login(){var select_user_form=document.getElementById("select_user_form");select_user_form.
style.display="none";var login_form=document.getElementById("login_form");login_form.style.visibility="";var select_users_option_block=document.getElementById
("select_users_option_block");select_users_option_block.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="block"}
function show_select_user(){var login_form=document.getElementById("login_form");login_form.style.visibility="hidden";var select_users_option_block=document.
getElementById("select_users_option_block");select_users_option_block.style.display="none";var select_user_form=document.getElementById("select_user_form");
select_user_form.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="none"}if(!window.JSON){login_button.suppress();
var new_script=document.createElement("script");new_script.onreadystatechange=function(){if(this.readyState==="loaded"||this.readyState==="complete"){this.
onreadystatechange=null;window.JSON={parse:window.jsonParse};window.jsonParse=undefined;login_button.release()}};new_script.src="/unprotected/json-minified.js";
document.getElementsByTagName("head")[0].appendChild(new_script)}try{login_form.onsubmit=do_login;set_opacity(DOM.get("login-wrapper"),0);LOCALE_FADES.
push(fade_in("login-wrapper"));var preload=document.createElement("div");preload.id="preload_images";document.body.insertBefore(preload,document.body.firstChild);if
(window.IS_LOGOUT){set_status_timeout(1e4)}else if(/(?:\?|&)locale=[^&]/.test(location.search)){show_status(MESSAGES.session_locale)}setTimeout(function()
{login_username_el.focus()},100)}catch(e){if(window.console){console.warn(e)}}

//submit_post.js
(function(context){"use strict";var DOC=context.document;function _wrongType(name,value){throw new Error(""+name+" must be a string, number, or array, not "+value)}
var scalarTypeIsOk={number:true,string:true};function submit(url,args){var myform=DOC.createElement("form");myform.method="POST";myform.action=url;myform.style.
display="none";Object.keys(args).forEach(function(name){var values;if("object"===typeof args[name]){if(args[name]instanceof Array){values=args[name]}else{_wrongType
(name,args[name])}}else if(scalarTypeIsOk[typeof args[name]]){values=[args[name]]}else{_wrongType(name,args[name])}values.forEach(function(val){var myvar=DOC.
createElement("input");myvar.type="hidden";myvar.name=name;myvar.value=val;myform.appendChild(myvar)})});DOC.documentElement.appendChild(myform);myform.
submit();DOC.documentElement.removeChild(myform)}context.SubmitPost={submit:submit}})(window);

//jstz.min.js
/*! jstz - v1.0.4 - 2012-12-18 */
(function(e){var t=function(){"use strict";var e="s",n=function(e){var t=-e.getTimezoneOffset();return t!==null?t:0},r=function(e,t,n){var r=new Date;return e!==undefined&&r.
setFullYear(e),r.setDate(n),r.setMonth(t),r},i=function(e){return n(r(e,0,2))},s=function(e){return n(r(e,5,2))},o=function(e){var t=e.getMonth()>7?s(e.getFullYear()):i(e.
getFullYear()),r=n(e);return t-r!==0},u=function(){var t=i(),n=s(),r=i()-s();return r<0?t+",1":r>0?n+",1,"+e:t+",0"},a=function(){var e=u();return new t.TimeZone(t.olson.
timezones[e])},f=function(e){var t=new Date(2010,6,15,1,0,0,0),n={"America/Denver":new Date(2011,2,13,3,0,0,0),"America/Mazatlan":new Date(2011,3,3,3,0,0,0),"
America/Chicago":new Date(2011,2,13,3,0,0,0),"America/Mexico_City":new Date(2011,3,3,3,0,0,0),"America/Asuncion":new Date(2012,9,7,3,0,0,0),"America/Santiago":
new Date(2012,9,3,3,0,0,0),"America/Campo_Grande":new Date(2012,9,21,5,0,0,0),"America/Montevideo":new Date(2011,9,2,3,0,0,0),"America/Sao_Paulo":new Date
(2011,9,16,5,0,0,0),"America/Los_Angeles":new Date(2011,2,13,8,0,0,0),"America/Santa_Isabel":new Date(2011,3,5,8,0,0,0),"America/Havana":new Date
(2012,2,10,2,0,0,0),"America/New_York":new Date(2012,2,10,7,0,0,0),"Asia/Beirut":new Date(2011,2,27,1,0,0,0),"Europe/Helsinki":new Date(2011,2,27,4,0,0,0),"Europe
/Istanbul":new Date(2011,2,28,5,0,0,0),"Asia/Damascus":new Date(2011,3,1,2,0,0,0),"Asia/Jerusalem":new Date(2011,3,1,6,0,0,0),"Asia/Gaza":new Date
(2009,2,28,0,30,0,0),"Africa/Cairo":new Date(2009,3,25,0,30,0,0),"Pacific/Auckland":new Date(2011,8,26,7,0,0,0),"Pacific/Fiji":new Date(2010,11,29,23,0,0,0),"America
/Halifax":new Date(2011,2,13,6,0,0,0),"America/Goose_Bay":new Date(2011,2,13,2,1,0,0),"America/Miquelon":new Date(2011,2,13,5,0,0,0),"America/Godthab":new Date
(2011,2,27,1,0,0,0),"Europe/Moscow":t,"Asia/Yekaterinburg":t,"Asia/Omsk":t,"Asia/Krasnoyarsk":t,"Asia/Irkutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"
Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0,0)};return n[e]};return{determine:a,date_is_dst:o,dst_start_for:f}}();t.TimeZone=function(e){"use strict";var n=
{"America/Denver":["America/Denver","America/Mazatlan"],"America/Chicago":["America/Chicago","America/Mexico_City"],"America/Santiago":["America/Santiago","

America/Asuncion","America/Campo_Grande"],"America/Montevideo":["America/Montevideo","America/Sao_Paulo"],"Asia/Beirut":["Asia/Beirut","Europe/Helsinki","Europe
/Istanbul","Asia/Damascus","Asia/Jerusalem","Asia/Gaza"],"Pacific/Auckland":["Pacific/Auckland","Pacific/Fiji"],"America/Los_Angeles":["America/Los_Angeles","America
/Santa_Isabel"],"America/New_York":["America/Havana","America/New_York"],"America/Halifax":["America/Goose_Bay","America/Halifax"],"America/Godthab":["America
/Miquelon","America/Godthab"],"Asia/Dubai":["Europe/Moscow"],"Asia/Dhaka":["Asia/Yekaterinburg"],"Asia/Jakarta":["Asia/Omsk"],"Asia/Shanghai":["Asia/Krasnoyarsk","
Australia/Perth"],"Asia/Tokyo":["Asia/Irkutsk"],"Australia/Brisbane":["Asia/Yakutsk"],"Pacific/Noumea":["Asia/Vladivostok"],"Pacific/Tarawa":["Asia/Kamchatka"],"Africa
/Johannesburg":["Asia/Gaza","Africa/Cairo"],"Asia/Baghdad":["Europe/Minsk"]},r=e,i=function(){var e=n[r],i=e.length,s=0,o=e[0];for(;s<i;s+=1){o=e[s];if(t.date_is_dst(t.
dst_start_for(o))){r=o;return}}},s=function(){return typeof n[r]!="undefined"};return s()&&i(),{name:function(){return r}},t.olson={},t.olson.timezones={"-720,0":"Etc
/GMT+12","-660,0":"Pacific/Pago_Pago","-600,1":"America/Adak","-600,0":"Pacific/Honolulu","-570,0":"Pacific/Marquesas","-540,0":"Pacific/Gambier","-540,1":"America
/Anchorage","-480,1":"America/Los_Angeles","-480,0":"Pacific/Pitcairn","-420,0":"America/Phoenix","-420,1":"America/Denver","-360,0":"America/Guatemala","-360,1":"
America/Chicago","-360,1,s":"Pacific/Easter","-300,0":"America/Bogota","-300,1":"America/New_York","-270,0":"America/Caracas","-240,1":"America/Halifax","-240,0":"
America/Santo_Domingo","-240,1,s":"America/Santiago","-210,1":"America/St_Johns","-180,1":"America/Godthab","-180,0":"America/Argentina/Buenos_Aires","-180,1,s":"
America/Montevideo","-120,0":"Etc/GMT+2","-120,1":"Etc/GMT+2","-60,1":"Atlantic/Azores","-60,0":"Atlantic/Cape_Verde","0,0":"Etc/UTC","0,1":"Europe/London","60,1":"
Europe/Berlin","60,0":"Africa/Lagos","60,1,s":"Africa/Windhoek","120,1":"Asia/Beirut","120,0":"Africa/Johannesburg","180,0":"Asia/Baghdad","180,1":"Europe/Moscow","
210,1":"Asia/Tehran","240,0":"Asia/Dubai","240,1":"Asia/Baku","270,0":"Asia/Kabul","300,1":"Asia/Yekaterinburg","300,0":"Asia/Karachi","330,0":"Asia/Kolkata","345,0":"
Asia/Kathmandu","360,0":"Asia/Dhaka","360,1":"Asia/Omsk","390,0":"Asia/Rangoon","420,1":"Asia/Krasnoyarsk","420,0":"Asia/Jakarta","480,0":"Asia/Shanghai","480,1":"
Asia/Irkutsk","525,0":"Australia/Eucla","525,1,s":"Australia/Eucla","540,1":"Asia/Yakutsk","540,0":"Asia/Tokyo","570,0":"Australia/Darwin","570,1,s":"Australia/Adelaide","
600,0":"Australia/Brisbane","600,1":"Asia/Vladivostok","600,1,s":"Australia/Sydney","630,1,s":"Australia/Lord_Howe","660,1":"Asia/Kamchatka","660,0":"Pacific/Noumea","
690,0":"Pacific/Norfolk","720,1,s":"Pacific/Auckland","720,0":"Pacific/Tarawa","765,1,s":"Pacific/Chatham","780,0":"Pacific/Tongatapu","780,1,s":"Pacific/Apia","840,0":"
Pacific/Kiritimati"},typeof exports!="undefined"?exports.jstz=t:e.jstz=t})(this);
//cptimezone_optimized.js
(function(window){"use strict";var JSTZ_RELATIVE_PATH="sharedjs/jstz.min.js";var TIMEZONE_COOKIE="timezone";var COOKIE_TIMEZONE_MISMATCH_CLASS="
if-timezone-cookie-needs-update";var DETECTED_TZ_CLASS="detected-timezone";var SHOWN_CLASS="shown";function _get_cookie(sKey){return
decodeURIComponent(document.cookie.replace(new RegExp("(?:(?:^|.*;)\\s*"+encodeURIComponent(sKey).replace(/[\-\.\+*]/g,"\\$&")+"\\s*\\=\\s*([^;]*).*$)|^.*$"),"$1"))
||null}function _detect_timezone(){return window.jstz.determine().name()}function reset_timezone_and_reload(){return reset_timezone(location.reload.bind(location))}
function _set_cookie(callback){document.cookie=TIMEZONE_COOKIE+"="+_detect_timezone()+"; path=/";if(callback){callback()}}function set_timezone_if_unset
(on_success){return!_get_cookie(TIMEZONE_COOKIE)&&reset_timezone(on_success)}function reset_timezone(on_success){_set_cookie(on_success);return true}
function set_timezone_and_reload_if_unset(){return set_timezone_if_unset(location.reload.bind(location))}function show_cookie_timezone_mismatch_nodes(){var
detected_tz=_detect_timezone();if(detected_tz!==_get_cookie(TIMEZONE_COOKIE)){var detected_nodes=document.querySelectorAll("."+DETECTED_TZ_CLASS);[].
forEach.call(detected_nodes,function(n){n.textContent=detected_tz});var show_nodes=document.querySelectorAll("."+COOKIE_TIMEZONE_MISMATCH_CLASS);[].
forEach.call(show_nodes,function(n){n.className+=" "+SHOWN_CLASS})}}window.CPTimezone={show_cookie_timezone_mismatch_nodes:
show_cookie_timezone_mismatch_nodes,reset_timezone_and_reload:reset_timezone_and_reload,reset_timezone:reset_timezone,set_timezone_and_reload_if_unset:
set_timezone_and_reload_if_unset}})(window);

CPTimezone.reset_timezone();
</script>

<style>
@media (min-width: 481px) {
#select_user_form {
width: px;
}
}
</style>
Copyright2022 cPanel, L.L.C.

Privacy Policy

</body>

</html>

Web Server Version **port 443 / tcp**

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-20 13:32:52.0

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Apache

HTTP Response Method and Header Information Collected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A
RESULT:
HTTP header and method information collected on port 443.

GET / HTTP/1.0
Host: server.northerngreenexpo.org

HTTP/1.1 421 Misdirected Request
Date: Wed, 26 Jan 2022 12:51:52 GMT
Server: Apache
Content-Length: 322
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

SSL Certificate - Information — port 110 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX

localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256

(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07
(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority

(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6

(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:

(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b
(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

Scan Diagnostics — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page http://server.northerngreenexpo.org:2082/ fetched. Status code:200, Content-Type:text/html, load time:203 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 0 requests, 10 seconds. Completed 0 requests of 38 estimated requests (0%). All tests completed.
HSTS Analysis no tests enabled.
No more requeues, redundant link threshold has been surpassed.
Collected 42 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 1) + directories:(9 x 25) + paths:(0 x 26) = total (225)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 26 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 81 requests, 3 seconds. Completed 81 requests of 225 estimated requests (36%). All tests completed.
WSEnumeration no tests enabled.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (68 tests, 6 inputs)
Batch #1 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 336 requests, 494 seconds. Completed 336 requests of 408 estimated requests (82.3529%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 6 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 48 requests, 63 seconds. Completed 48 requests of 144 estimated requests (33.3333%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 10 minutes (14 tests, 6 inputs)

Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 84 requests, 113 seconds. Completed 84 requests of 84 estimated requests (100%). All tests completed.
Time based tests for Apache Struts Vulnerabilities - no tests enabled.
Batch #2 URI parameter manipulation (no auth): estimated time < 10 minutes (68 tests, 6 inputs)
Batch #2 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 336 requests, 336 seconds. Completed 336 requests of 408 estimated requests (82.3529%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 6 inputs)
Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 48 requests, 33 seconds. Completed 48 requests of 144 estimated requests (33.3333%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 10 minutes (14 tests, 6 inputs)
Batch #2 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 84 requests, 54 seconds. Completed 84 requests of 84 estimated requests (100%). All tests completed.
Batch #3 URI parameter manipulation (no auth): estimated time < 10 minutes (68 tests, 4 inputs)
Batch #3 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 224 requests, 171 seconds. Completed 224 requests of 272 estimated requests (82.3529%). All tests completed.
Batch #3 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 4 inputs)
Batch #3 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 32 requests, 13 seconds. Completed 32 requests of 96 estimated requests (33.3333%). All tests completed.
Batch #3 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 4 inputs)
Batch #3 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 56 requests, 29 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.
Batch #4 WebCgiOob: estimated time < 30 minutes (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 12 requests, 1 seconds. Completed 12 requests of 1508 estimated requests (0.795756%). All tests completed.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 10 minutes (1 tests, 18 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 18 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 30 minutes (46 tests, 11 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 1424 requests, 65 seconds. Completed 1424 requests of 1424 estimated requests (100%). XSS optimization removed 116 links. All tests completed.
Batch #4 Header manipulation: estimated time < 30 minutes (46 tests, 18 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 1062 requests, 44 seconds. Completed 1062 requests of 2268 estimated requests (46.8254%). XSS optimization removed 522 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 18 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 18 requests, 1 seconds. Completed 18 requests of 18 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
cve_2017_9805 no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 1) + directories:(4 x 25) + paths:(11 x 26) = total (386)
Batch #5 Path XSS manipulation: estimated time < 10 minutes (15 tests, 26 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 145 requests, 4 seconds. Completed 145 requests of 386 estimated requests (37.5648%). All tests completed.
Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.
Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 1) + files:(10 x 1) + directories:(94 x 25) + paths:(9 x 26) = total (2597)
Batch #5 Path manipulation: estimated time < 30 minutes (116 tests, 26 inputs)
Batch #5 Path manipulation: 116 vulnsigs tests, completed 932 requests, 28 seconds. Completed 932 requests of 2597 estimated requests (35.8876%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 30 minutes (125 tests, 1 inputs)
Batch #5 WebCgiGeneric: 125 vulnsigs tests, completed 140 requests, 6 seconds. Completed 140 requests of 4498 estimated requests (3.11249%). All tests completed.
Total requests made: 5126
Average server response time: 1.52 seconds

Average browser load time: 1.54 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Cookies Collected — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150028
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:46:27.0

THREAT:
The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:
Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:
Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:
Total cookies: 2
session_locale=i_cpanel_snowmen; expires=Thu Jan 26 16:39:47 2023; path=/; domain=server.northerngreenexpo.org; max-age=31535995
whostmgrsession=%3aQRJZ9BInIqgGnym2%2c20fffb74f1ca236efe5aae9e0b6c337a; path=/; domain=server.northerngreenexpo.org; httponly

Scan Diagnostics — port 2078 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page https://server.northerngreenexpo.org:2078/ fetched. Status code:401, Content-Type:text/html, load time:266 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 0 requests, 7 seconds. Completed 0 requests of 38 estimated requests (0%). All tests completed.
HSTS Analysis no tests enabled.
Collected 1 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(9 x 1) + paths:(0 x 1) = total (9)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 1 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 9 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #4 WebCgiOob: estimated time < 1 minute (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 1 requests, 1 seconds. Completed 1 requests of 58 estimated requests (1.72414%). All tests completed.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (46 tests, 0 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (46 tests, 1 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 59 requests, 2 seconds. Completed 59 requests of 126 estimated requests (46.8254%). XSS optimization

removed 29 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
cve_2017_9805 no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(4 x 1) + paths:(11 x 1) = total (15)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 1 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 14 requests, 0 seconds. Completed 14 requests of 15 estimated requests (93.3333%). All tests completed.
Tomcat Vuln manipulation no tests enabled.
Time based path manipulation no tests enabled.
Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 0) + files:(10 x 0) + directories:(94 x 1) + paths:(9 x 1) = total (103)
Batch #5 Path manipulation: estimated time < 1 minute (116 tests, 1 inputs)
Batch #5 Path manipulation: 116 vulnsigs tests, completed 102 requests, 4 seconds. Completed 102 requests of 103 estimated requests (99.0291%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 1 minute (125 tests, 1 inputs)
Batch #5 WebCgiGeneric: 125 vulnsigs tests, completed 56 requests, 2 seconds. Completed 56 requests of 173 estimated requests (32.3699%). All tests completed.
Total requests made: 285
Average server response time: 0.25 seconds

Average browser load time: 0.27 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Cookies Collected — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150028
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:46:27.0

THREAT:
The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:
Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:
Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:
Total cookies: 3
session_locale=i_cpanel_snowmen; expires=Thu Jan 26 16:58:57 2023; path=/; domain=server.northerngreenexpo.org; max-age=31535990
roundcube_cookies=enabled; expires=Thu Jan 26 16:58:57 2023; path=/; domain=server.northerngreenexpo.org; max-age=31535990; httponly
webmailsession=%3ak_5w3qSet6lxQ4dU%2c522b7aa4e7fe99b8cb8cc24fefbedd5a; path=/; domain=server.northerngreenexpo.org; httponly

Default Web Page (Follow HTTP Redirection) — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:

nas-201911-01

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2080

<html>Authorization Required</html>

SSL Session Caching Information — port 995 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

RESULT:

TLSv1.2 session caching is disabled on the target.

Scan Time Limit Reached — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150024
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-01-27 21:02:50.0

THREAT:
The scan engine reached its internal time limit for this scan. The scan was stopped in order to collect and report the results so far.

IMPACT:
Not all tests have been completed. Therefore, some vulnerabilities may exist in the target application on links that the scanner has not yet tested. The scanner uses an iterative approach to determine the order in which links are tested. Links are selected in a breadth-first manner that takes into account how many connections each link has to other pages. This helps the scanner identify and test popular links first in order to have a useful coverage of the web application.

SOLUTION:
Application responsiveness is the most important factor in overall scan time. Review the average server response time reported by the scanner. Anything over 2 seconds is quite slow.

Scan time can potentially be reduced by one or more of the following methods:

- Make changes to improve the application's responsiveness.
- Increase the scan intensity setting.
- Reduce the SmartScan depth setting.
- Add redundant links configuration to reduce the number of unnecessary tests being performed.
- For applications with a large number of cookies, exclude the cookie/header tests (QIDs 150002, 150046, 150047, 150048).
- Exclude particular QIDs such as those related to XSS or SQL injection (and consequently running multiple scans with different QIDs enabled).

RESULT:
Scan stopped at established time limit in order to report results.

SSL Server Information Retrieval — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE

SSLv2 PROTOCOL IS DISABLED
SSLv3 PROTOCOL IS DISABLED
TLSv1 PROTOCOL IS ENABLED

TLSv1	COMPRESSION METHOD	None			
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
SEED-SHA	RSA	RSA	SHA1	SEED(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

TLSv1.1 PROTOCOL IS ENABLED

TLSv1.1	COMPRESSION METHOD	None			
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
SEED-SHA	RSA	RSA	SHA1	SEED(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH

TLSv1.2 PROTOCOL IS ENABLED

TLSv1.2	COMPRESSION METHOD	None			
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
SEED-SHA	RSA	RSA	SHA1	SEED(128)	MEDIUM
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH

ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH

TLSv1.3 PROTOCOL IS DISABLED

Default Web Page — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

GET / HTTP/1.0

Host: server.northerngreenexpo.org:2078

<html>Authorization Required</html>

Links Crawled — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 3.00
Number of links: 3
(This number excludes form requests and links re-requested during authentication.)

http://server.northerngreenexpo.org/
http://server.northerngreenexpo.org/cgi-sys/defaultwebpage.cgi
http://server.northerngreenexpo.org/img-sys/error-bg-left.png

External Links Discovered — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:
External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Number of links: 3
https://go.cpanel.net/ie11deprecation
https://go.cpanel.net/privacy
http://wikipedia.org/wiki/Case_sensitivity

SSL Session Caching Information — port 21 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1.2 session caching is enabled on the target.

Web Server Version — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-20 13:32:52.0

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Apache

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

RESULT:

NAME	STATUS
TLSv1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

HTTP Methods Returned by OPTIONS Request — port 2078 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2006-01-16 22:00:56.0

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Allow: PUT, UNLOCK, HEAD, POST, PROPPATCH, DELETE, MOVE, GET, COPY, MKCOL, LOCK, OPTIONS, PROPFIND

Scan Diagnostics — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page https://northerngreen.org/ fetched. Status code:200, Content-Type:text/html, load time:479 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (1 tests, 0 inputs)
SameSiteScripting: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : CMS Detection completed for 'Akismet!' at root directory 'https://northerngreen.org//wp-content/plugins/akismet/', after trying 6 requests of 12
CMSDetection: 1 vulnsigs tests, completed 765 requests, 1077 seconds. Completed 765 requests of 801 estimated requests (95.5056%). All tests completed.
HSTS Analysis no tests enabled.
Maximum request count reached: 300
Collected 4250 links overall in 0 hours 24 minutes duration.
Batch #0 WebCgiCMSDetection: estimated time < 1 minute (189 tests, 1 inputs)
WebCgiCMSDetection: 189 vulnsigs tests, completed 181 requests, 64 seconds. Completed 181 requests of 327 estimated requests (55.3517%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 4) + directories:(9 x 69) + paths:(0 x 73) = total (621)
Batch #0 WS Directory Path manipulation: estimated time < 10 minutes (9 tests, 73 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 558 requests, 263 seconds. Completed 558 requests of 621 estimated requests (89.8551%). All tests completed.
WSEnumeration no tests enabled.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (68 tests, 2 inputs)
Batch #1 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 56 requests, 31 seconds. Completed 56 requests of 136 estimated requests (41.1765%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 2 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 32 requests, 26 seconds. Completed 32 requests of 48 estimated requests (66.6667%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 2 inputs)
Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 14 requests, 13 seconds. Completed 14 requests of 28 estimated requests (50%). All tests completed.
Time based tests for Apache Struts Vulnerabilities - no tests enabled.
Batch #2 URI parameter manipulation (no auth): estimated time < 10 minutes (68 tests, 5 inputs)
Batch #2 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 392 requests, 175 seconds. Completed 392 requests of 340 estimated requests (115.294%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 5 inputs)
Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 80 requests, 31 seconds. Completed 80 requests of 120 estimated requests (66.6667%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 5 inputs)
Batch #2 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 56 requests, 425 seconds. Completed 56 requests of 70 estimated requests (80%). All tests completed.
Batch #4 WebCgiOob: estimated time < 30 minutes (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 20 requests, 29 seconds. Completed 20 requests of 4234 estimated requests (0.472367%). All tests completed.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 30 minutes (1 tests, 454 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 454 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (46 tests, 0 inputs)

Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 3 hours (46 tests, 296 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 17582 requests, 1291 seconds. Completed 17582 requests of 37296 estimated requests (47.1418%). XSS optimization removed 8584 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 104 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 106 requests, 13 seconds. Completed 106 requests of 104 estimated requests (101.923%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
cve_2017_9805 no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 4) + directories:(4 x 69) + paths:(11 x 73) = total (1079)
Batch #5 Path XSS manipulation: estimated time < 10 minutes (15 tests, 73 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 961 requests, 665 seconds. Completed 961 requests of 1079 estimated requests (89.0639%). All tests completed.
Tomcat Vuln manipulation no tests enabled.
Time based path manipulation no tests enabled.
Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 1) + files:(10 x 4) + directories:(94 x 69) + paths:(9 x 73) = total (7186)
Batch #5 Path manipulation: estimated time < 30 minutes (116 tests, 73 inputs)
Batch #5 Path manipulation: 116 vulnsigs tests, completed 3271 requests, 2405 seconds. Completed 3271 requests of 7186 estimated requests (45.5191%). Module did not finish.
Scan stopped at established time limit in order to report results.
Total requests made: 25085
Average server response time: 1.52 seconds

Average browser load time: 1.56 seconds
Scan stopped at established time limit in order to report results.
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Open UDP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Last Update:	2005-07-11 22:36:34.0

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.

Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports /Services	Description	Service Detected
53	domain	Domain Name Server	named udp
123	ntp	Network Time Protocol	ntp

SSL/TLS Server supports TLS_FALLBACK_SCSV — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38610
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-06-08 22:10:22.0

THREAT:

TLS cipher suite TLS_FALLBACK_SCSV is a signaling cipher suite value (SCSV). TLS servers support TLS_FALLBACK_SCSV will prevent downgrade attack.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

TLS_FALLBACK_SCSV is supported on port 2080.

TLS Secure Renegotiation Extension Support Information — port 21 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

TLS Secure Renegotiation Extension Status: supported.

SSL Session Caching Information — port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1 session caching is disabled on the target.
TLSv1.1 session caching is disabled on the target.
TLSv1.2 session caching is disabled on the target.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 110 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

Scan Diagnostics — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page http://northerngreen.org/ fetched. Status code:301, Content-Type:text/html, load time:92 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (1 tests, 0 inputs)
SameSiteScripting: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : CMS Detection completed for 'Akismet!' at root directory 'https://northerngreen.org//wp-content/plugins/akismet/', after trying 6 requests of 12
CMSDetection: 1 vulnsigs tests, completed 765 requests, 763 seconds. Completed 765 requests of 801 estimated requests (95.5056%). All tests completed.
HSTS Analysis no tests enabled.
Maximum request count reached: 300
Collected 4251 links overall in 0 hours 15 minutes duration.
Batch #0 WebCgiCMSDetection: estimated time < 1 minute (189 tests, 1 inputs)
WebCgiCMSDetection: 189 vulnsigs tests, completed 181 requests, 77 seconds. Completed 181 requests of 327 estimated requests (55.3517%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 4) + directories:(9 x 69) + paths:(0 x 73) = total (621)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 73 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 558 requests, 296 seconds. Completed 558 requests of 621 estimated requests (89.8551%). All tests completed.
WSEnumeration no tests enabled.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (68 tests, 2 inputs)
Batch #1 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 56 requests, 27 seconds. Completed 56 requests of 136 estimated requests (41.1765%). All tests completed.

Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 2 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 32 requests, 14 seconds. Completed 32 requests of 48 estimated requests (66.6667%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 2 inputs)
Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 14 requests, 6 seconds. Completed 14 requests of 28 estimated requests (50%). All tests completed.
Time based tests for Apache Struts Vulnerabilities - no tests enabled.
Batch #2 URI parameter manipulation (no auth): estimated time < 10 minutes (68 tests, 5 inputs)
Batch #2 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 392 requests, 95 seconds. Completed 392 requests of 340 estimated requests (115.294%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 5 inputs)
Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 80 requests, 13 seconds. Completed 80 requests of 120 estimated requests (66.6667%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 5 inputs)
Batch #2 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 56 requests, 404 seconds. Completed 56 requests of 70 estimated requests (80%). All tests completed.
Batch #4 WebCgiOob: estimated time < 30 minutes (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 20 requests, 11 seconds. Completed 20 requests of 4234 estimated requests (0.472367%). All tests completed.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 30 minutes (1 tests, 454 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 454 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (46 tests, 0 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 3 hours (46 tests, 296 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 17641 requests, 621 seconds. Completed 17641 requests of 37296 estimated requests (47.3%). XSS optimization removed 8584 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 104 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 107 requests, 6 seconds. Completed 107 requests of 104 estimated requests (102.885%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
cve_2017_9805 no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 4) + directories:(4 x 69) + paths:(11 x 73) = total (1079)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 73 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 961 requests, 437 seconds. Completed 961 requests of 1079 estimated requests (89.0639%). All tests completed.
Tomcat Vuln manipulation no tests enabled.
Time based path manipulation no tests enabled.
Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 1) + files:(10 x 4) + directories:(94 x 69) + paths:(9 x 73) = total (7186)
Batch #5 Path manipulation: estimated time < 10 minutes (116 tests, 73 inputs)
Batch #5 Path manipulation: 116 vulnsigs tests, completed 4434 requests, 3967 seconds. Completed 4434 requests of 7186 estimated requests (61.7033%). Module did not finish.
Scan stopped at established time limit in order to report results.

Total requests made: 26309
Average server response time: 1.66 seconds

Average browser load time: 1.74 seconds
Scan stopped at established time limit in order to report results.
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Links Crawled — port 2077 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 15.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

http://server.northerngreenexpo.org:2077/

TLS Secure Renegotiation Extension Support Information — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 143 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

External Links Discovered — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:
External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Number of links: 63
https://book.passkey.com/go/NorthernGreen2022
https://spothero.com/minneapolis-parking?sha_affiliate=meetmn
https://www.biddingforgood.com/auction/item/browse.action?auctionId=341698447
https://www.biddingforgood.com/auction/item/donate.action?auctionId=341698447
https://www.irrigation.org/IA/Certification/Maintain-Your-Certification/IA/Certification/Maintain-Your-Certification.aspx?hkey=94f8c009-ef08-4c73-b44e-e70f486c282f
https://www.gertenswholesale.com/
https://www.ihg.com/holidayinnexpress/hotels/us/en/minneapolis/mspdt/hoteldetail?fromRedirect=true&qSrt=sBR&qIta=99801505&icdv=99801505&qSlH=MSPDT&qGrpCd=MNL&setPMCookies=true&qSHBrC=EX&qDest=225%20South%20Eleventh%20Street,%20Minneapolis,%20MN,%20US&srb_u=1
https://e.issuu.com/embed.html?backgroundColor=%23f3f3f3&backgroundColorFullscreen=%23f3f3f3&d=ng22-advance-program-web&doAutoflipPages=true&hideIssuuLogo=true&logoImageUrl=https%3A%2F%2Fnortherngreen.org%2Fwp-content%2Fuploads%2F2021%2F11%2FNorthernGreenLogo-issuu.png&u=northerngreenexpo
https://e.issuu.com/embed.html?d=ng22-quick-guide-web&u=northerngreenexpo
https://whova.com/
https://whova.com/hybrid-event-platform/
https://whova.com/static/frontend/agenda_webpage/js/embedagenda.js?eid=north1_202201&host=https://whova.com
https://whova.com/static/frontend/xems/js/whova-speaker-widget.js?eid=north1_202201&
https://www.circlekfleetcards.com/
https://mtgf.org/
https://www.dot.state.mn.us/35w94/
https://mnla.biz/
https://www.minneapolis.org/minneapolis-convention-center/about/cleaning-protocols/
https://www.minneapolis.org/minneapolis-convention-center/attendees/
https://gravatar.com/
https://www.bachmanswholesale.com/departments
https://www.zieglercat.com/specials
https://www.zieglercat.com/specials/
https://www.hunterindustries.com/
https://www.rivercitylawnscape.com/careers
https://res.windsurfercrs.com/ibe/details.aspx?propertyid=13527&nights=5&checkin=01/09/2022&group=2201GREENE
https://www.hlsoutdoor.com/en
https://www.baileynurseries.com/
https://www.googletagmanager.com/gtag/js?id=UA-54228640-1
https://s3.amazonaws.com/meet-minneapolis/craft/cms/Attendee-Safety-Security-KBYG.pdf?mtime=20210922113243
https://maps.google.com/maps/embed/v1/place?q=Minneapolis%20Convention%20Center,1301%202nd%20Ave%20S%2C%20Minneapolis%2C%20MN%2C%2055404%2C%20US&center=44.9688369%2C-93.273865&zoom=14&key=AIzaSyAz-iChz547udxDFQBQrRwP3TJMIg0e8xY
https://ncma.org/education/segmental-retaining-walls/srw-installer/
https://ncma.org/programs/srw-certifications/basic-srw-installer-certification/
https://itunes.apple.com/app/apple-store/id716979741?pt=1944835&ct=&mt=8
https://www.apld.org/certification/
https://www.youtube.com/embed/KMTBQVupzbk?wmode=transparent&autoplay=0
https://www.youtube.com/user/NorthernGreenExpo
https://www.hyatt.com/en-US/group-booking/MSPRM/G-MNUR
https://www.turfsupradio.com/
https://play.google.com/store/apps/details?id=com.whova.event&referrer=utm_source%3D%26utm_medium%3Dportal%26utm_content%3Dnorth1_202201
https://www.expocad.com/host/fx/northerngreen/2022ngw/exfx.html
https://www.siteone.com/
https://www.isa-arbor.com/Credentials/Maintaining-Credentials/Post-Approved-CEUs
https://www.mtgf.org/

https://urldefense.com/v3/__https:/gbac.issa.com/issa-gbac-star-facility-accreditation/__;!!EB7VV9psZ_sHIy7zVFY!AkPXxwixCvj_A8ekqRrCNS-FXxGLsM7mE8FgdwZ_5cUYTzHBWT5RGX6vIxmBygWWJwr40XWgbNJg7w$
https://s.w.org/
https://www.mnla.biz/
https://youtu.be/DuyC6MiGZIc
https://globalplasmasolutions.com/how-it-works
https://twitter.com/NorthernGreenMN
https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html
https://www.cdc.gov/coronavirus/2019-ncov/vaccines/fully-vaccinated.html
https://www.bartlett.com/
http://mn.gov/aelslagid/continuinged.html
http://mn.gov/aelslagid/forms/ceform.pdf
http://www.gbac.org/
http://cdn.minneapolis.org/digital_files/154/downtown_minneapolis_parking_map.pdf
http://www.provenwinners-shrubs.com/
http://www.mtgf.org/
http://www.mnla.biz/
http://www.metrotransit.org/ride-free-on-nicollet-mall.aspx
tel:6516334987
tel:763-295-5420

Links Rejected By Crawl Scope or Exclusion List — port 2077 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:26:14.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

IP based excluded links:

Web Server Version — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-20 13:32:52.0

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
Apache

HTTP Response Method and Header Information Collected — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
HTTP header and method information collected on port 2095.

GET / HTTP/1.0
Host: server.northerngreenexpo.org:2095

HTTP/1.0 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Wed, 26 Jan 2022 18:07:05 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2095
Set-Cookie: webmailsession=%3aDVHDmKIZ97LIpnXT%2c6c424477ec47f46445329483225 91d70; HttpOnly; path=/; port=2095
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2095
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2095
Set-Cookie: Horde=expired; HttpOnly; domain=.server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2095
Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2095
Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2095
Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2095
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2095
Set-Cookie: imp_key=expired; HttpOnly; domain=server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2095
Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Thu, 26-Jan-2023 18:07:05 GMT; path=/; port=2095
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Content-Length: 37923

Scan Diagnostics — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021

Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page https://server.northerngreenexpo.org/ fetched. Status code:200, Content-Type:text/html, load time:161 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 2 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 3 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 2) + files:(0 x 2) + directories:(9 x 3) + paths:(0 x 5) = total (27)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 5 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 27 requests, 1 seconds. Completed 27 requests of 27 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #4 WebCgiOob: estimated time < 1 minute (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 5 requests, 0 seconds. Completed 5 requests of 290 estimated requests (1.72414%). All tests completed.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 3 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 3 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (46 tests, 0 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (46 tests, 2 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 118 requests, 2 seconds. Completed 118 requests of 252 estimated requests (46.8254%). XSS optimization removed 58 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 2 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
cve_2017_9805 no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 2) + files:(0 x 2) + directories:(4 x 3) + paths:(11 x 5) = total (67)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 5 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 66 requests, 1 seconds. Completed 66 requests of 67 estimated requests (98.5075%). All tests completed.
Tomcat Vuln manipulation no tests enabled.
Time based path manipulation no tests enabled.
Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 2) + files:(10 x 2) + directories:(94 x 3) + paths:(9 x 5) = total (353)
Batch #5 Path manipulation: estimated time < 1 minute (116 tests, 5 inputs)
Batch #5 Path manipulation: 116 vulnsigs tests, completed 349 requests, 3 seconds. Completed 349 requests of 353 estimated requests (98.8669%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 1 minute (125 tests, 1 inputs)
Batch #5 WebCgiGeneric: 125 vulnsigs tests, completed 122 requests, 5 seconds. Completed 122 requests of 865 estimated requests (14.104%). All tests completed.
Total requests made: 738
Average server response time: 0.09 seconds

Average browser load time: 0.09 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Links Rejected By Crawl Scope or Exclusion List — port 2079 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:26:14.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

IP based excluded links:

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

HTTP Response Method and Header Information Collected — port 2079 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
HTTP header and method information collected on port 2079.

GET / HTTP/1.0
Host: server.northerngreenexpo.org:2079

HTTP/1.1 401 Unauthorized
Date: Wed, 26 Jan 2022 16:37:08 GMT
Server: cPanel
Persistent-Auth: false
Host: server.northerngreenexpo.org:2079
Cache-Control: no-cache, no-store, must-revalidate, private
Connection: close
Vary: Accept-Encoding
WWW-Authenticate: Basic realm="Horde DAV Server"
Content-Length: 35
Content-Type: text/html; charset="utf-8"
Expires: Fri, 01 Jan 1990 00:00:00 GMT

WordPress Installation Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	11764

Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2018-10-06 03:31:11.0

THREAT:
WordPress is a free and open-source content management system (CMS) based on PHP and MySQL.

This QID detects WordPress installations based on the following criteria:
Existence of the wlwmanifest.xml file.
Response to a HTTP POST request to the xmlrpc.php source file.
Response to a HTTP GET request to the wp-links-opml.php source file.
Response to a HTTP GET request to the /feed/ directory.
Response of the Generator META tag.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
WordPress installation detected via the wlwmanifest.xml file on 443 over TCP.
<?xml version="1.0" encoding="utf-8" ?>

<manifest xmlns="http://schemas.microsoft.com/wlw/manifest/weblog">

<options>
<clientType>WordPress</clientType>
<supportsKeywords>Yes</supportsKeywords>
<supportsGetTags>Yes</supportsGetTags>
</options>

<weblog>
<serviceName>WordPress</serviceName>
<imageUrl>images/wlw/wp-icon.png</imageUrl>
<watermarkImageUrl>images/wlw/wp-watermark.png</watermarkImageUrl>
<homepageLinkText>View site</homepageLinkText>
<adminLinkText>Dashboard</adminLinkText>
<adminUrl>
<![CDATA[
{blog-postapi-url}/../wp-admin/
]]>
</adminUrl>
<postEditingUrl>
<![CDATA[
{blog-postapi-url}/../wp-admin/post.php?action=edit&post={post-id}
]]>
</postEditingUrl>
</weblog>

<buttons>
<button>
<id>0</id>
<text>Manage Comments</text>
<imageUrl>images/wlw/wp-comments.png</imageUrl>
<clickUrl>

<![CDATA[
{blog-postapi-url}/../wp-admin/edit-comments.php
]]>
</clickUrl>
</button>

</buttons>

</manifest>

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

List of Web Directories — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Directory	Source
/wp-content/	web page
/wp-content/uploads/	web page
/wp-content/uploads/2021/	web page
/wp-content/uploads/2021/06/	web page
/wp-content/plugins/	web page
/wp-content/plugins/bsa-plugin-pro-scripteo/	web page
/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/	web page
/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/	web page
/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/css/asset/	web page
/wp-includes/	web page
/wp-includes/js/	web page
/wp-includes/js/jquery/	web page
/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/	web page
/wp-content/uploads/2021/07/	web page
/wp-content/uploads/2021/12/	web page

HTTP Response Method and Header Information Collected — port 2077 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:

This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP header and method information collected on port 2077.

GET / HTTP/1.0
Host: server.northerngreenexpo.org:2077

HTTP/1.1 401 Unauthorized
Date: Wed, 26 Jan 2022 17:20:28 GMT
Server: cPanel
Persistent-Auth: false
Host: server.northerngreenexpo.org:2077
Cache-Control: no-cache, no-store, must-revalidate, private
Connection: close
Vary: Accept-Encoding
WWW-Authenticate: Basic realm="Restricted Area"
Content-Length: 35
Content-Type: text/html; charset="utf-8"
Expires: Fri, 01 Jan 1990 00:00:00 GMT

List of Web Directories — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Directory	Source
/login/	brute force
/login/	web page
/login	brute force

Web Server Version — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Last Update:	2021-12-20 13:32:52.0

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Apache
#table
Server_Version Server_Banner
Apache/2.x __

SSL Server default Diffie-Hellman prime information — port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38609
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-05-26 22:09:34.0

THREAT:
Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS. - For fixed primes: 1024 and below are considered unsafe. - For variable primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
SSL server default to use Diffie-Hellman key exchange method with variable 2048(bits) prime

External Links Discovered — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Number of links: 3
https://go.cpanel.net/ie11deprecation
https://go.cpanel.net/privacy
http://wikipedia.org/wiki/Case_sensitivity

SSL Server Information Retrieval — port 995 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2013-08-15 21:12:37.0

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

RESULT:
The network handle is: UNIFIEDLAYER-NETWORK-14
Network description:
Unified Layer

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 110 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low

External Links Discovered — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:
External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Number of links: 3
https://go.cpanel.net/ie11deprecation
https://go.cpanel.net/privacy
http://wikipedia.org/wiki/Case_sensitivity

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS
TLSv1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

Secure Sockets Layer (SSL) Certificate Transparency Information — port 993 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT

SSL Certificate will expire within next six months — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38600
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-01-29 20:24:19.0

THREAT:
Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:
Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:
Contact the certificate authority that signed your certificate to arrange for a renewal.

RESULT:
Certificate #0 CN=www.build.northerngreen.org The certificate will expire within six months: Feb 28 16:52:28 2022 GMT
Certificate #0 CN=wordpress.northerngreenexpo.org The certificate will expire within six months: Feb 28 16:52:33 2022 GMT

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2013-09-27 19:31:33.0

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

RESULT:
The ISP network handle is: LVLT-ORG-4-8

ISP Network description:
Level 3 Parent, LLC

SSL/TLS Server supports TLS_FALLBACK_SCSV — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38610
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-06-08 22:10:22.0

THREAT:
TLS cipher suite TLS_FALLBACK_SCSV is a signaling cipher suite value (SCSV). TLS servers support TLS_FALLBACK_SCSV will prevent downgrade attack.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS_FALLBACK_SCSV is supported on port 2078.

Links Rejected By Crawl Scope or Exclusion List — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:26:14.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

External links discovered:
https://book.passkey.com/go/NorthernGreen2022
https://spothero.com/minneapolis-parking?sha_affiliate=meetmn
https://www.biddingforgood.com/auction/item/browse.action?auctionId=341698447
https://www.biddingforgood.com/auction/item/donate.action?auctionId=341698447
https://www.irrigation.org/IA/Certification/Maintain-Your-Certification/IA/Certification/Maintain-Your-Certification.aspx?hkey=94f8c009-ef08-4c73-b44e-e70f486c282f
https://www.gertenswholesale.com/
https://www.ihg.com/holidayinnexpress/hotels/us/en/minneapolis/mspdt/hoteldetail?fromRedirect=true&qSrt=sBR&qIta=99801505&icdv=99801505&qSlH=MSPDT&qGrpCd=MNL&setPMCookies=true&qSHBrC=EX&qDest=225%20South%20Eleventh%20Street,%20Minneapolis,%20MN,%20US&srb_u=1
https://e.issuu.com/embed.html?backgroundColor=%23f3f3f3&backgroundColorFullscreen=%23f3f3f3&d=ng22-advance-program-web&doAutoflipPages=true&hideIssuuLogo=true&logoImageUrl=https%3A%2F%2Fnortherngreen.org%2Fwp-content%2Fuploads%2F2021%2F11%2FNorthernGreenLogo-issuu.png&u=northerngreenexpo
https://e.issuu.com/embed.html?d=ng22-quick-guide-web&u=northerngreenexpo
https://whova.com/
https://whova.com/hybrid-event-platform/
https://whova.com/static/frontend/agenda_webpage/js/embedagenda.js?eid=north1_202201&host=https://whova.com
https://whova.com/static/frontend/xems/js/whova-speaker-widget.js?eid=north1_202201&
https://www.circlekfleetcards.com/
https://mtgf.org/
https://www.dot.state.mn.us/35w94/
https://mnla.biz/
https://www.minneapolis.org/minneapolis-convention-center/about/cleaning-protocols/
https://www.minneapolis.org/minneapolis-convention-center/attendees/
https://gravatar.com/
https://www.bachmanswholesale.com/departments
https://www.zieglercat.com/specials
https://www.zieglercat.com/specials/
https://www.hunterindustries.com/
https://www.rivercitylawnscape.com/careers
https://res.windsurfercrs.com/ibe/details.aspx?propertyid=13527&nights=5&checkin=01/09/2022&group=2201GREENE
https://www.hlsoutdoor.com/en
https://www.baileynurseries.com/
https://www.googletagmanager.com/gtag/js?id=UA-54228640-1
https://s3.amazonaws.com/meet-minneapolis/craft/cms/Attendee-Safety-Security-KBYG.pdf?mtime=20210922113243
https://maps.google.com/maps/embed/v1/place?q=Minneapolis%20Convention%20Center,1301%202nd%20Ave%20S%2C%20Minneapolis%2C%20MN%2C%2055404%2C%20US&center=44.9688369%2C-93.273865&zoom=14&key=AIzaSyAz-iChz547udxDFQBQrRwP3TJMIg0e8xY
https://ncma.org/education/segmental-retaining-walls/srw-installer/

https://ncma.org/programs/srw-certifications/basic-srw-installer-certification/
https://itunes.apple.com/app/apple-store/id716979741?pt=1944835&ct=&mt=8
https://www.apld.org/certification/
https://www.youtube.com/embed/KMTBQVupzbk?wmode=transparent&autoplay=0
https://www.youtube.com/user/NorthernGreenExpo
https://www.hyatt.com/en-US/group-booking/MSPRM/G-MNUR
https://www.turfsupradio.com/
https://play.google.com/store/apps/details?id=com.whova.event&referrer=utm_source%3D%26utm_medium%3Dportal%26utm_content%3Dnorth1_202201
https://www.expocad.com/host/fx/northerngreen/2022ngw/exfx.html
https://www.siteone.com/
https://www.isa-arbor.com/Credentials/Maintaining-Credentials/Post-Approved-CEUs
https://www.mtgf.org/
https://urldefense.com/v3/__https:/gbac.issa.com/issa-gbac-star-facility-accreditation/__;!!EB7VV9psZ_sHly7zVFY!AkPXxwixCvj_A8ekqRrCNS-FXxGLsM7mE8FgdwZ_5cUYTzHBWT5RGX6vIxmBygWWJwr40XWgbNJg7w$
https://s.w.org/
https://www.mnla.biz/
https://youtu.be/DuyC6MiGZIc
https://globalplasmasolutions.com/how-it-works
https://twitter.com/NorthernGreenMN
https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html
https://www.cdc.gov/coronavirus/2019-ncov/vaccines/fully-vaccinated.html
https://www.bartlett.com/
http://mn.gov/aelslagid/continuinged.html
http://mn.gov/aelslagid/forms/ceform.pdf
http://www.gbac.org/
http://cdn.minneapolis.org/digital_files/154/downtown_minneapolis_parking_map.pdf
http://www.provenwinners-shrubs.com/
http://www.mtgf.org/
http://www.mnla.biz/
http://www.metrotransit.org/ride-free-on-nicollet-mall.aspx
tel:6516334987
tel:763-295-5420

IP based excluded links:

SSL Server default Diffie-Hellman prime information — port 587 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38609
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-05-26 22:09:34.0

THREAT:
Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS. - For fixed primes: 1024 and below are considered unsafe. - For variable primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
SSL server default to use Diffie-Hellman key exchange method with variable 2048(bits) prime

Default Web Page — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2082

<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">
<meta name="google" content="notranslate" />
<meta name="apple-itunes-app" content="app-id=1188352635" />
<title>cPanel Login</title>
<link rel="shortcut icon" href="

AAABAAEAICAAAAEAIADSAgAAFgAAAIlQTkcNChoKAAAADUlIRFIAAAAgAAAAIAgGAAAAc3p69AAAAplJREFUWIXt1j2IHGUYB
/DfOzdnjIKFkECIVWIKvUFsIkRExa9KJCLaWAgWJx4DilZWgpDDiI0wiViIoGATP1CCEDYHSeCwUBBkgiiKURQJFiLo4d0eOxYzC8nsO9m9XcXC+8MW+3z+9
/l6l2383xH+iSBpElyTdoda26xsDqp/h0CVZ3vwKm7tMBngAs7h7eRYebG6hMtMBHbMBX89vfARHprQ5U8cwdFQlIOZCVR5di1+w/wWXT
/EY6EoN5NZCODuKZLDwzgSMCuBe2fwfX6QZwtpWzqfBBtLC3txF/ZhxKbBGx0EfsTJS77vwmGjlZrD4mUzUOXZjVjGI65cnTXchB8iupdDUb7QinsQZ7GzZftdQj2JVZ49iC
/w6JjksIo7OnS9tiA5Vn6GtyK2+1MY5NkhfGDygVrBAxH5WkPuMjR7/3UsUFLl2Q68s4XkA3ws3v9zoSjX28Kr5wL1xrTxa6ou+f6OZGvqPg9v1wZeaUjcELE/DVfNhWFSvy
/enOIZ9eq1sTokEMNLWI79oirP8g6fXpVnh7GEvY1sV/OJ4f0UhyKKk6EoX4x5pEkgXv6L6OM99YqNw
/c4kXSwG5nkIfpLCynuiahW1GWeJHkfT4aiXO9atz1XcD6I6yLyHu6bIPk6Hg9FeYZ63y9EjBarPDvQ8VJ1nd9V3D4m+RncForyxFCQ4hSeahlej88Hefauurdwaufr5z/F
/ZHAX6nL+mZE18e36IWiHLkFocqzW9QXcNz1+wUHxJ/f10JRPjvGP4pk/vj5L3F8AtufdD+/p6dJDknzX+05fDLGtife
/766t9MRgFCUffWTudwE3AqBlVCUf0xLYGTQqzzbhydwJ3Y34g318J1tmX+DPBTIz9MS2MY2/nP8DTGaqeTDf30rAAAAAElFTkSuQmCC" type="image/x-icon" />

<!-- EXTERNAL CSS -->
<link href="/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css" rel="stylesheet" type="text/css" />
<link href="/cPanel_magic_revision_1626170558/unprotected/cpanel/style_v2_optimized.css" rel="stylesheet" type="text/css" />

<style type="text/css">
/*
This css is included in the base template in case the css cannot be loaded because of access restrictions
If this css is updated, please update securitypolicy_header.html.tmpl as well
*/
.copyright {
background: url(
PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIzNTlwdCIgaGVpZ2h0PSIzMjAiIHZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xp

background-size: 25px auto;
}
</style>
<!--[if IE 6]>
<style type="text/css">
img {
behavior: url(/cPanel_magic_revision_1367939018/unprotected/cp_pngbehavior_login.htc);
}
</style>
<![endif]-->

<script>
window.DOM = { get: function(id) { return document.getElementById(id) } };
</script>
</head>
<body class="cp">

<input type="hidden" id="goto_uri" value="/" />
<input type="hidden" id="goto_app" value="" />
<!-- Do not remove msg_code as it is needed for automated testing - msg_code:[] -->

<noscript>

JavaScript is disabled in your browser.
For cPanel to function properly, you must enable JavaScript.
If you do not enable JavaScript, certain features in cPanel will not function correctly.

</noscript>

You have logged out.

The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the cPanel Blog.

Please select a locale:
X Close

etina

dansk

Deutsch

English

espaol

espaol latinoamericano

espaol de Espaa

suomi

Filipino

franais

magyar

 cPanel Snowmen - i_cpanel_snowmen

i_en

Bahasa Indonesia

italiano

Bahasa Melayu

norsk bokml

Nederlands

Norwegian

polski

portugus

portugus do Brasil

romn

slovenina

svenska

Trke

Ting Vit


```
</div>
</div>
</div>
<div id="content-container">
<div id="login-container">

<div id="login-sub-container">
<div id="login-sub-header">

<img class="main-logo" src="/cPanel_magic_revision_1454480641/unprotected/cpanel/images/cpanel-logo.svg" alt="logo" />

</div>
<div id="login-sub"
>
<div id="clickthrough_form" style="visibility:hidden">
<form action="javascript:void(0)">
<div class="notices"></div>
<button type="submit" class="clickthrough-cont-btn">Continue</button>
</form>
</div>
<div id="forms">
<form novalidate id="login_form" action="/login/" method="post" target="_top" style="visibility:">
<div class="input-req-login"><label for="user">Username</label></div>
<div class="input-field-login icon username-container">
<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your username." class="std_textbox" type="text" tabindex="1" required>
</div>
<div class="input-req-login login-password-field-label"><label for="pass">Password</label></div>
<div class="input-field-login icon password-container">
<input name="pass" id="pass" placeholder="Enter your account password." class="std_textbox" type="password" tabindex="2" required>
</div>
<div class="controls">
<div class="login-btn">
<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>
</div>

</div>
<div class="clear" id="push"></div>
</form>
<!--CLOSE forms -->
</div>
<!--CLOSE login-sub -->
</div>


<!--CLOSE wrapper -->
</div>
<!--CLOSE login-sub-container -->
</div>
<!--CLOSE login-container -->
</div>

<div id="locale-footer">
<div class="locale-container">
<noscript>
<form method="get" action=".">
<select name="locale">
```

<option value="">Change locale</option>
<option value='ar'></option><option value='bg'></option><option value='cs'>etina</option><option value='da'>dansk</option><option value='de'>Deutsch</option><option value='el'></option><option value='en'>English</option><option value='es'>espaol</option><option value='es_419'>espaol latinoamericano</option><option value='es_es'>espaol de Espaa</option><option value='fi'>suomi</option><option value='fil'>Filipino</option><option value='fr'>franais</option><option value='he'></option><option value='hu'>magyar</option><option value='i_cpanel_snowmen'> cPanel Snowmen - i_cpanel_snowmen</option><option value='i_en'>i_en</option><option value='id'>Bahasa Indonesia</option><option value='it'>italiano</option><option value='ja'></option><option value='ko'></option><option value='ms'>Bahasa Melayu</option><option value='nb'>norsk bokml</option><option value='nl'>Nederlands</option><option value='no'>Norwegian</option><option value='pl'>polski</option><option value='pt'>portugus</option><option value='pt_br'>portugus do Brasil</option><option value='ro'>romn</option><option value='ru'></option><option value='sl'>slovenina</option><option value='sv'>svenska</option><option value='th'></option><option value='tr'>Trke</option><option value='uk'></option><option value='vi'>Ting Vit</option><option value='zh'></option><option value='zh_cn'></option><option value='zh_tw'></option> </select>
<button style="margin-left: 10px" type="submit">Change</button>
</form>
<style type="text/css">#mobilelocalemenu, #locales_list {display:none}</style>
</noscript>
<ul id="locales_list">

etina

dansk

Deutsch

English

espaol

Select a locale:
English

<!--Close login-wrapper -->

<script>
var MESSAGES = {"ajax_timeout":"The connection timed out. Please try again.","success":"Login successful. Redirecting ","invalid_login":"The login is invalid.","

network_error":"A network error occurred during your login request. Please try again. If this condition persists, contact your network service provider.","no_username":" You must specify a username to log in.","authenticating":"Authenticating ","session_locale":"The desired locale has been saved to your browser. To change the locale in this browser again, select another locale on this screen.","read_below":"Read the important information below.","internal_error":"An internal error occurred. If this condition persists, contact the system administrator."};

window.IS_LOGOUT = false;

//login.js
"use strict";var FADE_DURATION=.45;var FADE_DELAY=20;var AJAX_TIMEOUT=3e4;var LOCALE_FADES=[];var HAS_CSS_OPACITY="opacity"in document.body.style;var login_form=DOM.get("login_form");var login_username_el=DOM.get("user");var login_password_el=DOM.get("pass");var login_submit_el=DOM.get("login_submit");var goto_app=DOM.get("goto_app");var goto_uri=DOM.get("goto_uri");var div_cache={"login-page":DOM.get("login-page")||false,"locale-container":DOM.get("locale-container")||false,"login-container":DOM.get("login-container")||false,"locale-footer":DOM.get("locale-footer")||false,"content-cell":DOM.get("content-container")||false,invalid:DOM.get("invalid")||false};var content_cell=div_cache["content-cell"];if(div_cache["locale-footer"]){div_cache["locale-footer"].style.display="block"}var reset_form=DOM.get("reset_form");var set_opacity;if(HAS_CSS_OPACITY){set_opacity=function setOpacity(el,opacity){el.style.opacity=opacity}}else{var filter_regex=/(DXImageTransform\.Microsoft\.Alpha\(\)[^)]*\)/;set_opacity=function setOpacity(el,opacity){var filter_text=el.currentStyle.filter;if(!filter_text){el.style.filter="progid:DXImageTransform.Microsoft.Alpha(enabled=true)"}else if(!filter_regex.test(filter_text)){el.style.filter+=" progid:DXImageTransform.Microsoft.Alpha(enabled=true)"}else{var new_filter=filter_text.replace(filter_regex,"$1enabled=true)");if(new_filter!==filter_text){el.style.filter=new_filter}}try{el.filters.item("DXImageTransform.Microsoft.Alpha").opacity=opacity*100}catch(e){try{el.filters.item("alpha").opacity=opacity*100}catch(error){}}}}function toggle_locales(show_locales){while(LOCALE_FADES.length){clearInterval(LOCALE_FADES.shift())}var newly_shown=div_cache[show_locales?"locale-container":"login-container"];set_opacity(newly_shown,0);if(HAS_CSS_OPACITY){content_cell.replaceChild(newly_shown,content_cell.children[0])}else{var old=content_cell.children[0];content_cell.insertBefore(newly_shown,old);newly_shown.style.display="";old.style.display="none"}LOCALE_FADES.push(fade_in(newly_shown));LOCALE_FADES.push((show_locales?fade_out:fade_in)("locale-footer"))}function showIEBanner(){if(navigator.userAgent.indexOf("Trident")!==-1){var ieBannerDiv=document.getElementById("IE-warning");if(ieBannerDiv){ieBannerDiv.classList.remove("IE-warning-hide")}}}showIEBanner();function fade_in(el,duration,_fade_out_instead){el=div_cache[el]||DOM.get(el)||el;var style_obj=el.style;var interval;var cur_style=window.getComputedStyle?getComputedStyle(el,null):el.currentStyle;var visibility=cur_style.visibility;var start_opacity;if(el.offsetWidth&&visibility!=="hidden"){if(window.getComputedStyle){start_opacity=Number(cur_style.opacity)}else{try{start_opacity=el.filters.item("DXImageTransform.Microsoft.Alpha").opacity}catch(e){try{start_opacity=el.filters("alpha").opacity}catch(error){start_opacity=100}}start_opacity/=100}if(!start_opacity){start_opacity=0}else{start_opacity=0;set_opacity(el,0)}if(_fade_out_instead&&start_opacity<.01){if(start_opacity){set_opacity(el,0)}return}if(!duration){duration=FADE_DURATION}var duration_ms=duration*1e3;var start=new Date;var end;if(_fade_out_instead){end=duration_ms+start.getTime()}else{style_obj.visibility="visible"}var fader=function(){var opacity;if(_fade_out_instead){opacity=start_opacity*(end-new Date)/duration_ms;if(opacity<=0){opacity=0;clearInterval(interval);style_obj.visibility="hidden"}}else{opacity=start_opacity+(1-start_opacity)*(new Date-start)/duration_ms;if(opacity>=1){opacity=1;clearInterval(interval)}}set_opacity(el,opacity)};fader();interval=setInterval(fader,FADE_DELAY);return interval}function fade_out(el,timeout){return fade_in(el,timeout,true)}function AjaxObject(url,callbackFunction){this._url=url;this._callback=callbackFunction||function(){}}AjaxObject.prototype.updating=false;AjaxObject.prototype.abort=function(){if(this.updating){this.AJAX.abort();delete this.AJAX}};AjaxObject.prototype.update=function(passData,postMethod){if(this.AJAX){return false}var ajax=null;if(window.XMLHttpRequest){ajax=new XMLHttpRequest}else if(window.ActiveXObject){ajax=new window.ActiveXObject("Microsoft.XMLHTTP")}else{return false}var timeout;var that=this;ajax.onreadystatechange=function(){if(ajax.readyState==4){clearTimeout(timeout);that.updating=false;that._callback(ajax);delete that.AJAX}};try{var uri;timeout=setTimeout(function(){that.abort();show_status(MESSAGES.ajax_timeout,"error")},AJAX_TIMEOUT);if(/post/i.test(postMethod)){uri=this._url+"?login_only=1";ajax.open("POST",uri,true);ajax.setRequestHeader("Content-type","application/x-www-form-urlencoded");ajax.send(passData)}else{uri=this._url+"?"+passData+"&timestamp="+(new Date).getTime();ajax.open("GET",uri,true);ajax.send(null)}this.AJAX=ajax;this.updating=true}catch(e){login_form.submit()}return true};var _text_content="textContent"in document.body?"textContent":"innerText";function _process_parsed_login_success(result){var final_uri;var login_url_regex=/^\/(?:logout|login|openid_connect_callback)\/?/;if(result.redirect&&!login_url_regex.test(result.redirect)){final_uri=result.redirect}var location_obj_to_redirect;if(/^(?:\/cpsess[^/]+)\/$/.test(final_uri)){location_obj_to_redirect=top.location}else{if(result.security_token&&top!==window){for(var f=0;f<top.frames.length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result.security_token);top.frames[f].location.href=href}}location_obj_to_redirect=location}var redirector=function(){location_obj_to_redirect.href=final_uri+location.hash};if(result.notices&&result.notices.length){show_status(MESSAGES.read_below,"warn");var click_form=DOM.get("clickthrough_form");var container=click_form.querySelector(".notices");for(var n=0;n<result.notices.length;n++){var new_p=document.createElement("p");new_p.textContent=result.notices[n].content;container.appendChild(new_p)}click_form.onsubmit=redirector;fade_out(login_form);fade_in(click_form)}else{show_status(MESSAGES.success,"success");fade_out("content-container",FADE_DURATION/2);redirector()}}var login_button={button:login_submit_el,_suppressed_disabled:null,suppress:function(){if(this._suppressed_disabled===null){this._suppressed_disabled=this.button.disabled;this.button.disabled=true}},release:function(){if(this._suppressed_disabled!==null){this.button.disabled=this._suppressed_disabled;this._suppressed_disabled=null}},queue_disabled:function(state){if(this._suppressed_disabled===null){this.button.disabled=state}else{this._suppressed_disabled=state}}};function login_results(ajax_obj){var result;try{result=JSON.parse(ajax_obj&&ajax_obj.responseText)}catch(e){result=null}var response_status=ajax_obj.status;if(response_status===200){if(result){if(result.session){window.SubmitPost.submit(result.redirect,{session:result.session,goto_uri:result.goto_uri})}else{_process_parsed_login_success(result)}}else{login_form.submit()}return}else{if(parseInt(response_status/100,10)===4){var msg_code=result&&result.message;show_status(MESSAGES[msg_code||"invalid_login"]||MESSAGES.invalid_login,"error");set_status_timeout()}else{show_status(MESSAGES.network_error,"error")}}document.body.classList.remove("logging-in");login_button.release();return}}var level_classes={info:"info-notice",error:"error-notice",success:"success-notice",warn:"warn-notice"};var levels_regex="";Object.keys(level_classes).forEach(function(lv){levels_regex+="|"+level_classes[lv]});levels_regex=new RegExp("\\b(?:"+levels_regex.slice(1)+")\\b");function show_status(message,level){DOM.get("login-status-message")[_text_content]=message;var container=DOM.get("login-status");var

this_class=level&&level_classes[level]||level_classes.info;var el_class=container.className.replace(levels_regex,this_class);container.className=el_class;fade_in(container);reset_status_timeout()}var STATUS_TIMEOUT=null;function reset_status_timeout(){clearTimeout(STATUS_TIMEOUT);STATUS_TIMEOUT=null}function set_status_timeout(delay){STATUS_TIMEOUT=setTimeout(function(){fade_out("login-status")},delay||8e3)}var LOGIN_SUBMIT_OK=true;document.body.onkeyup=function(){LOGIN_SUBMIT_OK=true};document.body.onmousedown=function(){LOGIN_SUBMIT_OK=true};function do_login(){if(LOGIN_SUBMIT_OK){LOGIN_SUBMIT_OK=false;if(login_username_el.value.length===0){show_status(MESSAGES.no_username,"error");return false}document.body.classList.add("logging-in");login_button.suppress();show_status(MESSAGES.authenticating,"info");var goto_app_query=goto_app&&goto_app.value?"&goto_app="+encodeURIComponent(goto_app.value):"";var goto_uri_query=goto_uri&&goto_uri.value?"&goto_uri="+encodeURIComponent(goto_uri.value):"";var ajax_login=new AjaxObject(login_form.action,login_results);ajax_login.update("user="+encodeURIComponent(login_username_el.value)+"&pass="+encodeURIComponent(login_password_el.value)+goto_app_query+goto_uri_query,"POST")}return false}function show_login(){var select_user_form=document.getElementById("select_user_form");select_user_form.style.display="none";var login_form=document.getElementById("login_form");login_form.style.visibility="";var select_users_option_block=document.getElementById("select_users_option_block");select_users_option_block.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="block"}function show_select_user(){var login_form=document.getElementById("login_form");login_form.style.visibility="hidden";var select_users_option_block=document.getElementById("select_users_option_block");select_users_option_block.style.display="none";var select_user_form=document.getElementById("select_user_form");select_user_form.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="none"}if(!window.JSON){login_button.suppress();var new_script=document.createElement("script");new_script.onreadystatechange=function(){if(this.readyState==="loaded"||this.readyState==="complete"){this.onreadystatechange=null;window.JSON={parse:window.jsonParse};window.jsonParse=undefined;login_button.release()}};new_script.src="/unprotected/json-minified.js";document.getElementsByTagName("head")[0].appendChild(new_script)}try{login_form.onsubmit=do_login;set_opacity(DOM.get("login-wrapper"),0);LOCALE_FADES.push(fade_in("login-wrapper"));var preload=document.createElement("div");preload.id="preload_images";document.body.insertBefore(preload,document.body.firstChild);if(window.IS_LOGOUT){set_status_timeout(1e4)}else if(/(?:\?|&)locale=[^&]/.test(location.search)){show_status(MESSAGES.session_locale)}setTimeout(function(){login_username_el.focus()},100)}catch(e){if(window.console){console.warn(e)}}

//submit_post.js

(function(context){"use strict";var DOC=context.document;function _wrongType(name,value){throw new Error(""+name+" must be a string, number, or array, not "+value)}var scalarTypeIsOk={number:true,string:true};function submit(url,args){var myform=DOC.createElement("form");myform.method="POST";myform.action=url;myform.style.display="none";Object.keys(args).forEach(function(name){var values;if("object"===typeof args[name]){if(args[name]instanceof Array){values=args[name]}else{_wrongType(name,args[name])}}else if(scalarTypeIsOk[typeof args[name]]){values=[args[name]]}else{_wrongType(name,args[name])}values.forEach(function(val){var myvar=DOC.createElement("input");myvar.type="hidden";myvar.name=name;myvar.value=val;myform.appendChild(myvar)})});DOC.documentElement.appendChild(myform);myform.submit();DOC.documentElement.removeChild(myform)}context.SubmitPost={submit:submit}})(window);

//jstz.min.js

/*! jstz - v1.0.4 - 2012-12-18 */
(function(e){var t=function(){"use strict";var e="s",n=function(e){var t=-e.getTimezoneOffset();return t!==null?t:0},r=function(e,t,n){var r=new Date;return e!==undefined&&r.setFullYear(e),r.setDate(n),r.setMonth(t),r},i=function(e){return n(r(e,0,2))},s=function(e){return n(r(e,5,2))},o=function(e){var t=e.getMonth()>7?s(e.getFullYear()):i(e.getFullYear()),r=n(e);return t-r!==0},u=function(){var t=i(),n=s(),r=i()-s();return r<0?t+",1":r>0?n+",1,"+e:t+",0"},a=function(){var e=u();return new t.TimeZone(t.olson.timezones[e])},f=function(e){var t=new Date(2010,6,15,1,0,0,0),n={"America/Denver":new Date(2011,2,13,3,0,0,0),"America/Mazatlan":new Date(2011,3,3,3,0,0,0),"America/Chicago":new Date(2011,2,13,3,0,0,0),"America/Mexico_City":new Date(2011,3,3,3,0,0,0),"America/Asuncion":new Date(2012,9,7,3,0,0,0),"America/Santiago":new Date(2012,9,3,3,0,0,0),"America/Campo_Grande":new Date(2012,9,21,5,0,0,0),"America/Montevideo":new Date(2011,9,2,3,0,0,0),"America/Sao_Paulo":new Date(2011,9,16,5,0,0,0),"America/Los_Angeles":new Date(2011,2,13,8,0,0,0),"America/Santa_Isabel":new Date(2011,3,5,8,0,0,0),"America/Havana":new Date(2012,2,10,2,0,0,0),"America/New_York":new Date(2012,2,10,7,0,0,0),"Asia/Beirut":new Date(2011,2,27,1,0,0,0),"Europe/Helsinki":new Date(2011,2,27,4,0,0,0),"Europe/Istanbul":new Date(2011,2,28,5,0,0,0),"Asia/Damascus":new Date(2011,3,1,2,0,0,0),"Asia/Jerusalem":new Date(2011,3,1,6,0,0,0),"Asia/Gaza":new Date(2009,2,28,0,30,0,0),"Africa/Cairo":new Date(2009,3,25,0,30,0,0),"Pacific/Auckland":new Date(2011,8,26,7,0,0,0),"Pacific/Fiji":new Date(2010,11,29,23,0,0,0),"America/Halifax":new Date(2011,2,13,6,0,0,0),"America/Goose_Bay":new Date(2011,2,13,2,1,0,0),"America/Miquelon":new Date(2011,2,13,5,0,0,0),"America/Godthab":new Date(2011,2,27,1,0,0,0),"Europe/Moscow":t,"Asia/Yekaterinburg":t,"Asia/Omsk":t,"Asia/Krasnoyarsk":t,"Asia/Irkutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0,0)};return n[e]};return{determine:a,date_is_dst:o,dst_start_for:f}}();t.TimeZone=function(e){"use strict";var n={"America/Denver":["America/Denver","America/Mazatlan"],"America/Chicago":["America/Chicago","America/Mexico_City"],"America/Santiago":["America/Santiago","America/Asuncion","America/Campo_Grande"],"America/Montevideo":["America/Montevideo","America/Sao_Paulo"],"Asia/Beirut":["Asia/Beirut","Europe/Helsinki","Europe/Istanbul","Asia/Damascus","Asia/Jerusalem","Asia/Gaza"],"Pacific/Auckland":["Pacific/Auckland","Pacific/Fiji"],"America/Los_Angeles":["America/Los_Angeles","America/Santa_Isabel"],"America/New_York":["America/Havana","America/New_York"],"America/Halifax":["America/Goose_Bay","America/Halifax"],"America/Godthab":["America/Miquelon","America/Godthab"],"Asia/Dubai":["Europe/Moscow"],"Asia/Dhaka":["Asia/Yekaterinburg"],"Asia/Jakarta":["Asia/Omsk"],"Asia/Shanghai":["Asia/Krasnoyarsk","Australia/Perth"],"Asia/Tokyo":["Asia/Irkutsk"],"Australia/Brisbane":["Asia/Yakutsk"],"Pacific/Noumea":["Asia/Vladivostok"],"Pacific/Tarawa":["Asia/Kamchatka"],"Africa/Johannesburg":["Asia/Gaza","Africa/Cairo"],"Asia/Baghdad":["Europe/Minsk"]},r=e,i=function(){var e=n[r],i=e.length,s=0,o=e[0];for(;s<i;s+=1){o=e[s];if(t.date_is_dst(t.dst_start_for(o))){r=o;return}}},s=function(){return typeof n[r]!="undefined"};return s()&&i(),{name:function(){return r}},t.olson={},t.olson.timezones={"-720,0":"Etc/GMT+12","-660,0":"Pacific/Pago_Pago","-600,1":"America/Adak","-600,0":"Pacific/Honolulu","-570,0":"Pacific/Marquesas","-540,0":"Pacific/Gambier","-540,1":"America/Anchorage","-480,1":"America/Los_Angeles","-480,0":"Pacific/Pitcairn","-420,0":"America/Phoenix","-420,1":"America/Denver","-360,0":"America/Guatemala","-360,1":"America/Chicago","-360,1,s":"Pacific/Easter","-300,0":"America/Bogota","-300,1":"America/New_York","-270,0":"America/Caracas","-240,1":"America/Halifax","-240,0":"America/Santo_Domingo","-240,1,s":"America/Santiago","-210,1":"America/St_Johns","-180,1":"America/Godthab","-180,0":"America/Argentina/Buenos_Aires","-180,1,s":"

America/Montevideo","-120,0":"Etc/GMT+2","-120,1":"Etc/GMT+2","-60,1":"Atlantic/Azores","-60,0":"Atlantic/Cape_Verde","0,0":"Etc/UTC","0,1":"Europe/London","60,1":"Europe/Berlin","60,0":"Africa/Lagos","60,1,s":"Africa/Windhoek","120,1":"Asia/Beirut","120,0":"Africa/Johannesburg","180,0":"Asia/Baghdad","180,1":"Europe/Moscow","210,1":"Asia/Tehran","240,0":"Asia/Dubai","240,1":"Asia/Baku","270,0":"Asia/Kabul","300,1":"Asia/Yekaterinburg","300,0":"Asia/Karachi","330,0":"Asia/Kolkata","345,0":"Asia/Kathmandu","360,0":"Asia/Dhaka","360,1":"Asia/Omsk","390,0":"Asia/Rangoon","420,1":"Asia/Krasnoyarsk","420,0":"Asia/Jakarta","480,0":"Asia/Shanghai","480,1":"Asia/Irkutsk","525,0":"Australia/Eucla","525,1,s":"Australia/Eucla","540,1":"Asia/Yakutsk","540,0":"Asia/Tokyo","570,0":"Australia/Darwin","570,1,s":"Australia/Adelaide","600,0":"Australia/Brisbane","600,1":"Asia/Vladivostok","600,1,s":"Australia/Sydney","630,1,s":"Australia/Lord_Howe","660,1":"Asia/Kamchatka","660,0":"Pacific/Noumea","690,0":"Pacific/Norfolk","720,1,s":"Pacific/Auckland","720,0":"Pacific/Tarawa","765,1,s":"Pacific/Chatham","780,0":"Pacific/Tongatapu","780,1,s":"Pacific/Apia","840,0":"Pacific/Kiritimati"},typeof exports!="undefined"?exports.jstz=t:e.jstz=t})(this);
//cptimezone_optimized.js
(function(window){"use strict";var JSTZ_RELATIVE_PATH="sharedjs/jstz.min.js";var TIMEZONE_COOKIE="timezone";var COOKIE_TIMEZONE_MISMATCH_CLASS="if-timezone-cookie-needs-update";var DETECTED_TZ_CLASS="detected-timezone";var SHOWN_CLASS="shown";function _get_cookie(sKey){return decodeURIComponent(document.cookie.replace(new RegExp("(?:(?:^|.*;)\\s*"+encodeURIComponent(sKey).replace(/[\-\.\+*]/g,"\\$&")+"\\s*\\=\\s*([^;]*).*$)|^.*$"),"$1"))||null}function _detect_timezone(){return window.jstz.determine().name()}function reset_timezone_and_reload(){return reset_timezone(location.reload.bind(location))}function _set_cookie(callback){document.cookie=TIMEZONE_COOKIE+"="+_detect_timezone()+"; path=/";if(callback){callback()}}function set_timezone_if_unset(on_success){return!_get_cookie(TIMEZONE_COOKIE)&&reset_timezone(on_success)}function reset_timezone(on_success){_set_cookie(on_success);return true}function set_timezone_and_reload_if_unset(){return set_timezone_if_unset(location.reload.bind(location))}function show_cookie_timezone_mismatch_nodes(){var detected_tz=_detect_timezone();if(detected_tz!==_get_cookie(TIMEZONE_COOKIE)){var detected_nodes=document.querySelectorAll("."+DETECTED_TZ_CLASS);[].forEach.call(detected_nodes,function(n){n.textContent=detected_tz});var show_nodes=document.querySelectorAll("."+COOKIE_TIMEZONE_MISMATCH_CLASS);[].forEach.call(show_nodes,function(n){n.className+=" "+SHOWN_CLASS})}}window.CPTimezone={show_cookie_timezone_mismatch_nodes:show_cookie_timezone_mismatch_nodes,reset_timezone_and_reload:reset_timezone_and_reload,reset_timezone:reset_timezone,set_timezone_and_reload_if_unset:set_timezone_and_reload_if_unset}})(window);

```
CPTimezone.reset_timezone();
</script>

<style>
@media (min-width: 481px) {
#select_user_form {
width: px;
}
}
</style>
<div class="copyright">Copyright2022 cPanel, L.L.C.
<br /><a href="https://go.cpanel.net/privacy" target="_blank">Privacy Policy</a></div>

</body>

</html>
```

Default Web Page — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	12230
Category:	CGI

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org

HTTP/1.1 200 OK
Date: Wed, 26 Jan 2022 12:32:14 GMT
Server: Apache
Last-Modified: Thu, 28 Oct 2021 14:25:02 GMT
Accept-Ranges: bytes
Content-Length: 163
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html><head><META HTTP-EQUIV="Cache-control" CONTENT="no-cache"><META HTTP-EQUIV="refresh" CONTENT="0;URL=/cgi-sys/defaultwebpage.cgi"><
/head><body></body></html>
GET / HTTP/1.0
Host: northerngreen.org

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
The document has moved here.
</body></html>

FTPS service detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	48173
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-28 12:30:42.0

THREAT:
FTPS service configured on FTP server that requires FTPS is detected

IMPACT:
NA

SOLUTION:
If possible, use alternate services that provide encryption.
Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission.

RESULT:
FTPS service detected on port 21 over TCP.

Links Crawled — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 3.00
Number of links: 3
(This number excludes form requests and links re-requested during authentication.)

https://server.northerngreenexpo.org/
https://server.northerngreenexpo.org/cgi-sys/defaultwebpage.cgi
https://server.northerngreenexpo.org/img-sys/error-bg-left.png

List of Web Directories Requiring Authentication — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	86671
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:09.0

THREAT:
The service has identified a list of Web directories which require authentication to access.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Directories Requiring Authentication
/login/
/login

SSL Server Information Retrieval — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH

DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH

TLSv1.3 PROTOCOL IS DISABLED

Web Server Supports HTTP Request Pipelining — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2005-02-23 00:25:38.0

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker, it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

RESULT:

GET / HTTP/1.1
Host:162.144.102.68:80

GET /Q_Evasive/ HTTP/1.1
Host:162.144.102.68:80

HTTP/1.1 200 OK
Date: Wed, 26 Jan 2022 14:27:05 GMT
Server: Apache
Last-Modified: Thu, 28 Oct 2021 14:25:02 GMT
Accept-Ranges: bytes
Content-Length: 163
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Content-Type: text/html

<html><head><META HTTP-EQUIV="Cache-control" CONTENT="no-cache"><META HTTP-EQUIV="refresh" CONTENT="0;URL=/cgi-sys/defaultwebpage.cgi"><
/head><body></body></html>
HTTP/1.1 404 Not Found
Date: Wed, 26 Jan 2022 14:27:05 GMT
Server: Apache
Accept-Ranges: bytes
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Transfer-Encoding: chunked
Content-Type: text/html

1

1

1

157
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-type" content="text/html; charset=utf-8">
<meta http-equiv="Cache-control" content="no-cache">
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Expires" content="0">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>
3
404
1

9
Not Found
1fca
</title>

```
<style type="text/css">
body {
font-family: Arial, Helvetica, sans-serif;
font-size: 14px;
line-height: 1.428571429;
background-color: #ffffff;
color: #2F3230;
padding: 0;
margin: 0;
}
section, footer {
display: block;
padding: 0;
margin: 0;
}
.container {
margin-left: auto;
margin-right: auto;
padding: 0 10px;
}
.response-info {
color: #CCCCCC;
}
.status-code {
font-size: 500%;
}
.status-reason {
font-size: 250%;
display: block;
}
.contact-info,
.reason-text {
color: #000000;
}
.additional-info {
background-repeat: no-repeat;
background-color: #293A4A;
color: #FFFFFF;
}
.additional-info a {
color: #FFFFFF;
}
.additional-info-items {
padding: 20px 0;
min-height: 193px;
}
.contact-info {
margin-bottom: 20px;
font-size: 16px;
}
.contact-info a {
text-decoration: underline;
color: #428BCA;
}
.contact-info a:hover,
.contact-info a:focus,
```

```
.contact-info a:active {
color: #2A6496;
}
.reason-text {
margin: 20px 0;
font-size: 16px;
}
ul {
display: inline-block;
list-style: none outside none;
margin: 0;
padding: 0;
}
ul li {
float: left;
text-align: center;
}
.additional-info-items ul li {
width: 100%;
}
.info-image {
padding: 10px;
}
.info-heading {
font-weight: bold;
text-align: left;
word-break: break-all;
width: 100%;
}
.info-server address {
text-align: left;
}
footer {
text-align: center;
margin: 60px 0;
}
footer a {
text-decoration: none;
}
footer a img {
border: 0;
}
.copyright {
font-size: 10px;
color: #3F4143;
}
@media (min-width: 768px) {
.additional-info {
position: relative;
overflow: hidden;
background-image: none;
}
.additional-info-items {
padding: 20px;
}
.container {
```

```
width: 90%;
}
.additional-info-items ul li {
width: 100%;
text-align: left;
}
.additional-info-items ul li:first-child {
padding: 20px;
}
.reason-text {
font-size: 18px;
}
.contact-info {
font-size: 18px;
}
.info-image {
float: left;
}
.info-heading {
margin: 62px 0 0 98px;
}
.info-server address {
text-align: left;
position: absolute;
right: 0;
bottom: 0;
margin: 0 10px;
}
.status-reason {
display: inline;
}
}
@media (min-width: 992px) {
.additional-info {
background-image: url(

GET / HTTP/1.1
Host:162.144.102.68:80

GET /Q_Evasive/ HTTP/1.1
Host:162.144.102.68:80



HTTP/1.1 200 OK
Date: Wed, 26 Jan 2022 14:27:53 GMT
Server: Apache
Last-Modified: Thu, 28 Oct 2021 14:25:02 GMT
Accept-Ranges: bytes
Content-Length: 163
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Content-Type: text/html

<html><head><META HTTP-EQUIV="Cache-control" CONTENT="no-cache"><META HTTP-EQUIV="refresh" CONTENT="0;URL=/cgi-sys/defaultwebpage.cgi"><
```

/head><body></body></html>
HTTP/1.1 404 Not Found
Date: Wed, 26 Jan 2022 14:27:53 GMT
Server: Apache
Accept-Ranges: bytes
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Transfer-Encoding: chunked
Content-Type: text/html

1

1

1

157
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-type" content="text/html; charset=utf-8">
<meta http-equiv="Cache-control" content="no-cache">
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Expires" content="0">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>
3
404
1

9
Not Found
1fca
</title>
<style type="text/css">
body {
font-family: Arial, Helvetica, sans-serif;
font-size: 14px;
line-height: 1.428571429;
background-color: #ffffff;
color: #2F3230;
padding: 0;
margin: 0;
}
section, footer {
display: block;
padding: 0;
margin: 0;
}
.container {
margin-left: auto;
margin-right: auto;

```
padding: 0 10px;
}
.response-info {
color: #CCCCCC;
}
.status-code {
font-size: 500%;
}
.status-reason {
font-size: 250%;
display: block;
}
.contact-info,
.reason-text {
color: #000000;
}
.additional-info {
background-repeat: no-repeat;
background-color: #293A4A;
color: #FFFFFF;
}
.additional-info a {
color: #FFFFFF;
}
.additional-info-items {
padding: 20px 0;
min-height: 193px;
}
.contact-info {
margin-bottom: 20px;
font-size: 16px;
}
.contact-info a {
text-decoration: underline;
color: #428BCA;
}
.contact-info a:hover,
.contact-info a:focus,
.contact-info a:active {
color: #2A6496;
}
.reason-text {
margin: 20px 0;
font-size: 16px;
}
ul {
display: inline-block;
list-style: none outside none;
margin: 0;
padding: 0;
}
ul li {
float: left;
text-align: center;
}
.additional-info-items ul li {
```

```
width: 100%;
}
.info-image {
padding: 10px;
}
.info-heading {
font-weight: bold;
text-align: left;
word-break: break-all;
width: 100%;
}
.info-server address {
text-align: left;
}
footer {
text-align: center;
margin: 60px 0;
}
footer a {
text-decoration: none;
}
footer a img {
border: 0;
}
.copyright {
font-size: 10px;
color: #3F4143;
}
@media (min-width: 768px) {
.additional-info {
position: relative;
overflow: hidden;
background-image: none;
}
.additional-info-items {
padding: 20px;
}
.container {
width: 90%;
}
.additional-info-items ul li {
width: 100%;
text-align: left;
}
.additional-info-items ul li:first-child {
padding: 20px;
}
.reason-text {
font-size: 18px;
}
.contact-info {
font-size: 18px;
}
.info-image {
float: left;
}
```

.info-heading {
margin: 62px 0 0 98px;
}
.info-server address {
text-align: left;
position: absolute;
right: 0;
bottom: 0;
margin: 0 10px;
}
.status-reason {
display: inline;
}
}
@media (min-width: 992px) {
.additional-info {
background-image: url(
//5+fn////////////////////////////6+vr
////////////////////////////////////+i5edTAAAAPXRSTlMAAQECAwQFBgcICQoLDA0ODxAREhMUFRYXGBkaGxwdHh8gISIjJCUmJygoKSorLC0uLzAwMTIzNDU2Nzg5H7x0XAAA

TLS Secure Renegotiation Extension Support Information — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Secure Sockets Layer (SSL) Certificate Transparency Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=www.build.northerngreen.org			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	dfa55eab68824f1f6cadeeb85f4e3e5aeacda212a46a5e8e3b12c020445c2a73	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate #0		CN=wordpress.northerngreenexpo.org			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	dfa55eab68824f1f6cadeeb85f4e3e5aeacda212a46a5e8e3b12c020445c2a73	Thu 01 Jan 1970 12:00:00 AM GMT

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 995 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

SSL Certificate - Information — port 26 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52

(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07

(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication

(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6
(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority

(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:
(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b

(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

List of Web Directories Requiring Authentication — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86671
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:09.0

THREAT:

The service has identified a list of Web directories which require authentication to access.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Directories Requiring Authentication

/login/

/login

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

RESULT:

NAME	STATUS
TLSv1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.1	
Extended Master Secret	no

Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

Admin interface detected — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48144
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-25 12:30:36.0

THREAT:

A website as www.abc.com/admin which is accessible over the internet in this case the QID should get flagged. It could be any website that includes /admin and accessible over the internet should be flagged with this QID. QID detection logic:
Qid detects if admin interface or directory exists at default location "/admin"

IMPACT:

NA

SOLUTION:

NA

RESULT:

Admin interface detected on : 2086 .
<title>WHM Login</title>

Information Disclosure — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150247
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-14 13:31:46.0

THREAT:
Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.

IMPACT:
An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

SOLUTION:
Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

Please review the issues reported below:

RESULT:
Number of technologies detected: 2
Technology name: Apache
Matched Components:
header match:
Server:Apache
Matched links: Reporting only first 3 links
https://northerngreen.org/
https://northerngreen.org/comments/feed/
https://northerngreen.org/feed/

Technology name: WordPress
Matched Components:
html response match:
te" type="application/json" href="https://northerngreen.org/wp-json/wp/v2/pages/1166" /><link rel="EditURI" type="application/rsd+xml" title="RSD" href="
https://northerngreen.org/xmlrpc.php?rsd" />
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="https://northerngreen.org/wp-includes/wlwmanifest.xml" />
<meta name="generator" content="WordPress 5.9" />
<link rel="canonical" href="https://northerngreen.org/" />
<link rel='shortlink' href='https://northerngreen.org/' />
<link rel=
script tag match:
<script type='text/javascript' src='https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/bsa.carousel.js?ver=5.9'
id='buy_sell_ads_pro_carousel_js_script-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/chart.js?ver=5.9' id='
buy_sell_ads_pro_chart_js_script-js'></script>

<script type='text/javascript' src='https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/jquery.simplyscroll.js?ver=5.9' id='buy_sell_ads_pro_simply_scroll_js_script-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/jquery.viewportchecker.js?ver=5.9' id='buy_sell_ads_pro_viewport_checker_js_script-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/script.js?ver=5.9' id='buy_sell_ads_pro_js_script-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-content/uploads/fusion-scripts/ab4869bbb2511aa73427cb1bc54185b8.min.js?ver=3.6' id='fusion-scripts-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2' id='jquery-migrate-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-includes/js/jquery/jquery.min.js?ver=3.6.0' id='jquery-core-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-includes/js/shortcode.min.js?ver=5.9' id='shortcode-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-includes/js/thickbox/thickbox.js?ver=3.1-20121105' id='thickbox-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-includes/js/underscore.min.js?ver=1.13.1' id='underscore-js'></script>
header match:
Link:<https://northerngreen.org/wp-json/>; rel="https://api.w.org/"
X-Pingback:https://northerngreen.org/xmlrpc.php
Matched links: Reporting only first 3 links
https://northerngreen.org/
https://northerngreen.org/comments/feed/
https://northerngreen.org/feed/

TLS Secure Renegotiation Extension Support Information — port 110 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

SSL Certificate - Information — port 995 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:

(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:

(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07
(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:

(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6
(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26

(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:
(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:

(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b
(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

Default Web Page (Follow HTTP Redirection) port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

Patch:

Following are links for downloading patches to fix the vulnerabilities:

nas-201911-01

RESULT:

GET / HTTP/1.0

Host: server.northerngreenexpo.org:2095

<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">
<meta name="google" content="notranslate" />
<meta name="apple-itunes-app" content="app-id=1188352635" />
<title>Webmail Login</title>
<link rel="shortcut icon" href="
AAABAAEAICAAAAEAIADSAgAAFgAAAIlQTkcNChoKAAAADUlIRFIAAAAgAAAAIAgGAAAAc3p69AAAAplJREFUWIXt1j2IHGUYB
/DfOzdnjIKFkECIVWIKvUFsIkRExa9KJCLaWAgWJx4DilZWgpDDiI0wiViIoGATP1CCEDYHSeCwUBBkgiiKURQJFiLo4d0eOxYzC8nsO9m9XcXC+8MW+3z+9
/l6l2383xH+iSBpElyTdoda26xsDqp/h0CVZ3vwKm7tMBngAs7h7eRYebG6hMtMBHbMBX89vfARHprQ5U8cwdFQlIOZCVR5di1+w/wWXT
/EY6EoN5NZCODuKZLDwzgSMCuBe2fwfX6QZwtpWzqfBBtLC3txF/ZhxKbBGx0EfsTJS77vwmGjlZrD4mUzUOXZjVjGI65cnTXchB8iupdDUb7QinsQZ7GzZftdQj2JVZ49iC
/w6JjksIo7OnS9tiA5Vn6GtyK2+1MY5NkhfGDygVrBAxH5WkPuMjR7/3UsUFLl2Q68s4XkA3ws3v9zoSjX28Kr5wL1xrTxa6ou+f6OZGvqPg9v1wZeaUjcELE/DVfNhWFSvy
/enOIZ9eq1sTokEMNLWI79oirP8g6fXpVnh7GEvY1sV/OJ4f0UhyKKk6EoX4x5pEkgXv6L6OM99YqNw
/c4kXSwG5nkIfpLCynuiahW1GWeJHkfT4aiXO9atz1XcD6I6yLyHu6bIPk6Hg9FeYZ63y9EjBarPDvQ8VJ1nd9V3D4m+RncForyxFCQ4hSeahlej88Hefauurdwaufr5z/F
/ZHAX6nL+mZE18e36IWiHLkFocqzW9QXcNz1+wUHxJ/f10JRPjvGP4pk/vj5L3F8AtufdD+/p6dJDknzX+05fDLGtife
/766t9MRgFCUffWTudwE3AqBlVCUf0xLYGTQqzzbhydwJ3Y34g318J1tmX+DPBTIz9MS2MY2/nP8DTGaqeTDf30rAAAAAElFTkSuQmCC" type="image/x-icon" />

<!-- EXTERNAL CSS -->
<link href="/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css" rel="stylesheet" type="text/css" />
<link href="/cPanel_magic_revision_1626170558/unprotected/cpanel/style_v2_optimized.css" rel="stylesheet" type="text/css" />

<style type="text/css">
/*
This css is included in the base template in case the css cannot be loaded because of access restrictions
If this css is updated, please update securitypolicy_header.html.tmpl as well
*/
.copyright {

```
background: url(
PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIzNTlwdCIgaGVpZ2h0PSIzMjAiIHZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xp

background-size: 25px auto;
}
</style>
<!--[if IE 6]>
<style type="text/css">
img {
behavior: url(/cPanel_magic_revision_1367939018/unprotected/cp_pngbehavior_login.htc);
}
</style>
<![endif]-->

<script>
window.DOM = { get: function(id) { return document.getElementById(id) } };
</script>
</head>
<body class="wm">




<input type="hidden" id="goto_uri" value="/" />
<input type="hidden" id="goto_app" value="" />
<!-- Do not remove msg_code as it is needed for automated testing - msg_code:[] -->
<div id="login-wrapper" class="group ">
<div class="wrapper">
<div id="notify">
<noscript>
<div class="error-notice">
<img src="/cPanel_magic_revision_1367939222/unprotected/cpanel/images/notice-error.png" alt="Error" align="left"/>
JavaScript is disabled in your browser.
For Webmail to function properly, you must enable JavaScript.
If you do not enable JavaScript, certain features in Webmail will not function correctly.
</div>
</noscript>


<div id=&apos;login-status&apos; class="error-notice" style="visibility: hidden">
<div class="content-wrapper">
<div id="login-detail">
<div id="login-status-icon-container"><span class=&apos;login-status-icon&apos;></span></div>
<div id="login-status-message">You have logged out.</div>
</div>
</div>
</div>
<div id="IE-warning" class="warn-notice IE-warning-hide" style="display: none">
<div class="content-wrapper">
<div id="IE-warning-detail">
<div id="IE-warning-icon-container"><span class="IE-warning-icon"></span></div>
<div id="IE-warning-message">The system has detected that you are using Internet Explorer 11. cPanel &amp;amp; WHM no longer supports Internet Explorer 11. For more
information, read the <a title="cPanel Blog" target="_blank" href="https://go.cpanel.net/ie11deprecation">cPanel Blog</a>.</div>
</div>
</div>
</div>
```

```
</div>

<div style="display:none">
<div id="locale-container" style="visibility:hidden">
<div id="locale-inner-container">
<div id="locale-header">
<div class="locale-head">Please select a locale:</div>
<div class="close"><a href="javascript:void(0)" onclick="toggle_locales(false)">X Close</a></div>
</div>
<div id="locale-map">
<div class="scroller clear">

<div class="locale-cell"><a href="?locale=ar"></a></div>

<div class="locale-cell"><a href="?locale=bg"></a></div>

<div class="locale-cell"><a href="?locale=cs">etina</a></div>

<div class="locale-cell"><a href="?locale=da">dansk</a></div>

<div class="locale-cell"><a href="?locale=de">Deutsch</a></div>

<div class="locale-cell"><a href="?locale=el"></a></div>

<div class="locale-cell"><a href="?locale=en">English</a></div>

<div class="locale-cell"><a href="?locale=es">espaol</a></div>

<div class="locale-cell"><a href="?locale=es_419">espaol latinoamericano</a></div>

<div class="locale-cell"><a href="?locale=es_es">espaol de Espaa</a></div>

<div class="locale-cell"><a href="?locale=fi">suomi</a></div>

<div class="locale-cell"><a href="?locale=fil">Filipino</a></div>

<div class="locale-cell"><a href="?locale=fr">franais</a></div>

<div class="locale-cell"><a href="?locale=he"></a></div>

<div class="locale-cell"><a href="?locale=hu">magyar</a></div>

<div class="locale-cell"><a href="?locale=i_cpanel_snowmen"> cPanel Snowmen - i_cpanel_snowmen</a></div>

<div class="locale-cell"><a href="?locale=i_en">i_en</a></div>

<div class="locale-cell"><a href="?locale=id">Bahasa Indonesia</a></div>

<div class="locale-cell"><a href="?locale=it">italiano</a></div>

<div class="locale-cell"><a href="?locale=ja"></a></div>

<div class="locale-cell"><a href="?locale=ko"></a></div>

<div class="locale-cell"><a href="?locale=ms">Bahasa Melayu</a></div>
```

norsk bokml

Nederlands

Norwegian

polski

portugus

portugus do Brasil

romn

slovenina

svenska

Trke

Ting Vit

<div id="login-sub"
>

<form action="javascript:void(0)">

<button type="submit" class="clickthrough-cont-btn">Continue</button>
</form>

<form novalidate id="login_form" action="/login/" method="post" target="_top" style="visibility:">
<label for="user">Email Address</label>

<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your email address." class="std_textbox" type="text" tabindex="1" required>

<label for="pass">Password</label>

<input name="pass" id="pass" placeholder="Enter your email password." class="std_textbox" type="password" tabindex="2" required>

<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>

</form>
<!--CLOSE forms -->

<!--CLOSE login-sub -->

<!--CLOSE wrapper -->

<!--CLOSE login-sub-container -->

<!--CLOSE login-container -->

<noscript>
<form method="get" action=".">
<select name="locale">
<option value="">Change locale</option>
<option value='ar'></option><option value='bg'></option><option value='cs'>etina</option><option value='da'
>dansk</option><option value='de'>Deutsch</option><option value='el'></option><option value='en'>English</option><option
value='es'>espaol</option><option value='es_419'>espaol latinoamericano</option><option value='es_es'>espaol de Espaa<
/option><option value='fi'>suomi</option><option value='fil'>Filipino</option><option value='fr'>franais</option><option
value='he'></option><option value='hu'>magyar</option><option value='i_cpanel_snowmen'> cPanel Snowmen -
i_cpanel_snowmen</option><option value='i_en'>i_en</option><option value='id'>Bahasa Indonesia</option><option value='it'
>italiano</option><option value='ja'></option><option value='ko'></option><option value='ms'>Bahasa Melayu</option><option
value='nb'>norsk bokml</option><option value='nl'>Nederlands</option><option value='no'>Norwegian</option><option
value='pl'>polski</option><option value='pt'>portugus</option><option value='pt_br'>portugus do Brasil</option><option
value='ro'>romn</option><option value='ru'></option><option value='sl'>slovenina</option><option value='sv'
>svenska</option><option value='th'></option><option value='tr'>Trke</option><option value='uk'></option><option value='
vi'>Ting Vit</option><option value='zh'></option><option value='zh_cn'></option><option value='zh_tw'></option> </select>
<button style="margin-left: 10px" type="submit">Change</button>
</form>
<style type="text/css">#mobilelocalemenu, #locales_list {display:none}</style>
</noscript>
<ul id="locales_list">

etina

dansk

Deutsch

English

espaol

Select a locale:
English

<!--Close login-wrapper -->

<script>
var MESSAGES = {"ajax_timeout":"The connection timed out. Please try again.","invalid_login":"The login is invalid.","success":"Login successful. Redirecting ","session_locale":"The desired locale has been saved to your browser. To change the locale in this browser again, select another locale on this screen.","network_error":"A network error occurred during your login request. Please try again. If this condition persists, contact your network service provider.","no_username":"You must specify a username to log in.","authenticating":"Authenticating ","internal_error":"An internal error occurred. If this condition persists, contact the system administrator.","read_below":"Read the important information below."};

window.IS_LOGOUT = false;

//login.js
"use strict";var FADE_DURATION=.45;var FADE_DELAY=20;var AJAX_TIMEOUT=3e4;var LOCALE_FADES=[];var HAS_CSS_OPACITY="opacity"in document.body.style;var login_form=DOM.get("login_form");var login_username_el=DOM.get("user");var login_password_el=DOM.get("pass");var login_submit_el=DOM.get("login_submit");var goto_app=DOM.get("goto_app");var goto_uri=DOM.get("goto_uri");var div_cache={"login-page":DOM.get("login-page")||false,"locale-container":DOM.get("locale-container")||false,"login-container":DOM.get("login-container")||false,"locale-footer":DOM.get("locale-footer")||false,"content-cell":DOM.get("content-container")||false,invalid:DOM.get("invalid")||false};var content_cell=div_cache["content-cell"];if(div_cache["locale-footer"]){div_cache["locale-footer"].style.display="block"}var reset_form=DOM.get("reset_form");var set_opacity;if(HAS_CSS_OPACITY){set_opacity=function setOpacity(el,opacity){el.style.opacity=opacity}}else{var filter_regex=/(DXImageTransform\.Microsoft\.Alpha\()[^)]*\)/;set_opacity=function setOpacity(el,opacity){var filter_text=el.currentStyle.filter;if(!filter_text){el.style.filter="progid:DXImageTransform.Microsoft.Alpha(enabled=true)"}else if(!filter_regex.test(filter_text)){el.style.filter+=" progid:DXImageTransform.Microsoft.Alpha(enabled=true)"}else{var new_filter=filter_text.replace(filter_regex,"$1enabled=true)");if(new_filter!==filter_text){el.style.filter=new_filter}}try{el.filters.item("DXImageTransform.Microsoft.Alpha").opacity=opacity*100}catch(e){try{el.filters.item("alpha").opacity=opacity*100}catch(error){}}}}function toggle_locales(show_locales){while(LOCALE_FADES.length){clearInterval(LOCALE_FADES.shift())}var newly_shown=div_cache[show_locales?"locale-container":"login-container"];set_opacity(newly_shown,0);if

(HAS_CSS_OPACITY){content_cell.replaceChild(newly_shown,content_cell.children[0])}else{var old=content_cell.children[0];content_cell.insertBefore(newly_shown,old);newly_shown.style.display="";old.style.display="none"}LOCALE_FADES.push(fade_in(newly_shown));LOCALE_FADES.push((show_locales?fade_out:fade_in)("locale-footer"))}function showIEBanner(){if(navigator.userAgent.indexOf("Trident")!==-1){var ieBannerDiv=document.getElementById("IE-warning");if(ieBannerDiv){ieBannerDiv.classList.remove("IE-warning-hide")}}}showIEBanner();function fade_in(el,duration,_fade_out_instead){el=div_cache[el]||DOM.get(el)||el;var style_obj=el.style;var interval;var cur_style=window.getComputedStyle?getComputedStyle(el,null):el.currentStyle;var visibility=cur_style.visibility;var start_opacity;if(el.offsetWidth&&visibility!=="hidden"){if(window.getComputedStyle){start_opacity=Number(cur_style.opacity)}else{try{start_opacity=el.filters.item("DXImageTransform.Microsoft.Alpha").opacity}catch(e){try{start_opacity=el.filters("alpha").opacity}catch(error){start_opacity=100}start_opacity/=100}if(!start_opacity){start_opacity=0}}else{start_opacity=0;set_opacity(el,0)}if(_fade_out_instead&&start_opacity<.01){if(start_opacity){set_opacity(el,0)}return}if(!duration){duration=FADE_DURATION}var duration_ms=duration*1e3;var start=new Date;var end;if(_fade_out_instead){end=duration_ms+start.getTime()}else{style_obj.visibility="visible"}var fader=function(){var opacity;if(_fade_out_instead){opacity=start_opacity*(end-new Date)/duration_ms;if(opacity<=0){opacity=0;clearInterval(interval);style_obj.visibility="hidden"}}else{opacity=start_opacity+(1-start_opacity)*(new Date-start)/duration_ms;if(opacity>=1){opacity=1;clearInterval(interval)}}set_opacity(el,opacity)};fader();interval=setInterval(fader,FADE_DELAY);return interval}function fade_out(el,timeout){return fade_in(el,timeout,true)}function AjaxObject(url,callbackFunction){this._url=url;this._callback=callbackFunction||function(){}}AjaxObject.prototype.updating=false;AjaxObject.prototype.abort=function(){if(this.updating){this.AJAX.abort();delete this.AJAX}};AjaxObject.prototype.update=function(passData,postMethod){if(this.AJAX){return false}var ajax=null;if(window.XMLHttpRequest){ajax=new XMLHttpRequest}else if(window.ActiveXObject){ajax=new window.ActiveXObject("Microsoft.XMLHTTP")}else{return false}var timeout;var that=this;ajax.onreadystatechange=function(){if(ajax.readyState==4){clearTimeout(timeout);that.updating=false;that._callback(ajax);delete that.AJAX}};try{var uri;timeout=setTimeout(function(){that.abort();show_status(MESSAGES.ajax_timeout,"error")},AJAX_TIMEOUT);if(/post/i.test(postMethod)){uri=this._url+"?login_only=1";ajax.open("POST",uri,true);ajax.setRequestHeader("Content-type","application/x-www-form-urlencoded");ajax.send(passData)}else{uri=this._url+"?"+passData+"&timestamp="+(new Date).getTime();ajax.open("GET",uri,true);ajax.send(null)}this.AJAX=ajax;this.updating=true}catch(e){login_form.submit()}return true};var _text_content="textContent"in document.body?"textContent":"innerText";function _process_parsed_login_success(result){var final_uri;var login_url_regex=/^\/(?:logout|login|openid_connect_callback)\/?/;if(result.redirect&&!login_url_regex.test(result.redirect)){final_uri=result.redirect}var location_obj_to_redirect;if(/^(?:\/cpsess[^/]+)\/$/.test(final_uri)){location_obj_to_redirect=top.location}else{if(result.security_token&&top!==window){for(var f=0;f<top.frames.length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result.security_token);top.frames[f].location.href=href}}}location_obj_to_redirect=location}var redirector=function(){location_obj_to_redirect.href=final_uri+location.hash};if(result.notices&&result.notices.length){show_status(MESSAGES.read_below,"warn");var click_form=DOM.get("clickthrough_form");var container=click_form.querySelector(".notices");for(var n=0;n<result.notices.length;n++){var new_p=document.createElement("p");new_p.textContent=result.notices[n].content;container.appendChild(new_p)}click_form.onsubmit=redirector;fade_out(login_form);fade_in(click_form)}else{show_status(MESSAGES.success,"success");fade_out("content-container",FADE_DURATION/2);redirector()}}var login_button={button:login_submit_el,_suppressed_disabled:null,suppress:function(){if(this._suppressed_disabled===null){this._suppressed_disabled=this.button.disabled;this.button.disabled=true}},release:function(){if(this._suppressed_disabled!==null){this.button.disabled=this._suppressed_disabled;this._suppressed_disabled=null}},queue_disabled:function(state){if(this._suppressed_disabled===null){this.button.disabled=state}else{this._suppressed_disabled=state}}};function login_results(ajax_obj){var result;try{result=JSON.parse(ajax_obj&&ajax_obj.responseText)}catch(e){result=null}var response_status=ajax_obj.status;if(response_status===200){if(result){if(result.session){window.SubmitPost.submit(result.redirect,{session:result.session,goto_uri:result.goto_uri})}else{_process_parsed_login_success(result)}}else{login_form.submit()}return}else{if(parseInt(response_status/100,10)===4){var msg_code=result&&result.message;show_status(MESSAGES[msg_code||"invalid_login"]||MESSAGES.invalid_login,"error");set_status_timeout()}else{show_status(MESSAGES.network_error,"error")}document.body.classList.remove("logging-in");login_button.release();return}}var level_classes={info:"info-notice",error:"error-notice",success:"success-notice",warn:"warn-notice"};var levels_regex="";Object.keys(level_classes).forEach(function(lv){levels_regex+="|"+level_classes[lv]});levels_regex=new RegExp("\\b(?:"+levels_regex.slice(1)+")\\b");function show_status(message,level){DOM.get("login-status-message")[_text_content]=message;var container=DOM.get("login-status");var this_class=level&&level_classes[level]||level_classes.info;var el_class=container.className.replace(levels_regex,this_class);container.className=el_class;fade_in(container);reset_status_timeout()}var STATUS_TIMEOUT=null;function reset_status_timeout(){clearTimeout(STATUS_TIMEOUT);STATUS_TIMEOUT=null}function set_status_timeout(delay){STATUS_TIMEOUT=setTimeout(function(){fade_out("login-status")},delay||8e3)}var LOGIN_SUBMIT_OK=true;document.body.onkeyup=function(){LOGIN_SUBMIT_OK=true};document.body.onmousedown=function(){LOGIN_SUBMIT_OK=true};function do_login(){if(LOGIN_SUBMIT_OK){LOGIN_SUBMIT_OK=false;if(login_username_el.value.length===0){show_status(MESSAGES.no_username,"error");return false}document.body.classList.add("logging-in");login_button.suppress();show_status(MESSAGES.authenticating,"info");var goto_app_query=goto_app&&goto_app.value?"&goto_app="+encodeURIComponent(goto_app.value):"";var goto_uri_query=goto_uri&&goto_uri.value?"&goto_uri="+encodeURIComponent(goto_uri.value):"";var ajax_login=new AjaxObject(login_form.action,login_results);ajax_login.update("user="+encodeURIComponent(login_username_el.value)+"&pass="+encodeURIComponent(login_password_el.value)+goto_app_query+goto_uri_query,"POST")}return false}function show_login(){var select_user_form=document.getElementById("select_user_form");select_user_form.style.display="none";var login_form=document.getElementById("login_form");login_form.style.visibility="";var select_users_option_block=document.getElementById("select_users_option_block");select_users_option_block.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="block"}function show_select_user(){var login_form=document.getElementById("login_form");login_form.style.visibility="hidden";var select_users_option_block=document.getElementById("select_users_option_block");select_users_option_block.style.display="none";var select_user_form=document.getElementById("select_user_form");select_user_form.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="none"}if(!window.JSON){login_button.suppress();var new_script=document.createElement("script");new_script.onreadystatechange=function(){if(this.readyState==="loaded"||this.readyState==="complete"){this.onreadystatechange=null;window.JSON={parse:window.jsonParse};window.jsonParse=undefined;login_button.release()}};new_script.src="/unprotected/json-minified.js";document.getElementsByTagName("head")[0].appendChild(new_script)}try{login_form.onsubmit=do_login;set_opacity(DOM.get("login-wrapper"),0);LOCALE_FADES.push(fade_in("login-wrapper"));var preload=document.createElement("div");preload.id="preload_images";document.body.insertBefore(preload,document.body.firstChild);if(window.IS_LOGOUT){set_status_timeout(1e4)}else if(/(?:\?|&)locale=[^&]/.test(location.search)){show_status(MESSAGES.session_locale)}setTimeout(function(){login_username_el.focus()},100)}catch(e){if(window.console){console.warn(e)}}

//submit_post.js
(function(context){"use strict";var DOC=context.document;function _wrongType(name,value){throw new Error(""+name+" must be a string, number, or array, not "+value)}
var scalarTypeIsOk={number:true,string:true};function submit(url,args){var myform=DOC.createElement("form");myform.method="POST";myform.action=url;myform.style.
display="none";Object.keys(args).forEach(function(name){var values;if("object"===typeof args[name]){if(args[name]instanceof Array){values=args[name]}else{_wrongType
(name,args[name])}}else if(scalarTypeIsOk[typeof args[name]]){values=[args[name]]}else{_wrongType(name,args[name])}values.forEach(function(val){var myvar=DOC.
createElement("input");myvar.type="hidden";myvar.name=name;myvar.value=val;myform.appendChild(myvar)})});DOC.documentElement.appendChild(myform);myform.
submit();DOC.documentElement.removeChild(myform)}context.SubmitPost={submit:submit}})(window);

//jstz.min.js
/*! jstz - v1.0.4 - 2012-12-18 */
(function(e){var t=function(){"use strict";var e="s",n=function(e){var t=-e.getTimezoneOffset();return t!==null?t:0},r=function(e,t,n){var r=new Date;return e!==undefined&&r.
setFullYear(e),r.setDate(n),r.setMonth(t),r},i=function(e){return n(r(e,0,2))},s=function(e){return n(r(e,5,2))},o=function(e){var t=e.getMonth()>7?s(e.getFullYear()):i(e.
getFullYear()),r=n(e);return t-r!==0},u=function(){var t=i(),n=s(),r=i()-s();return r<0?t+",1":r>0?n+",1,"+e:t+",0"},a=function(){var e=u();return new t.TimeZone(t.olson.
timezones[e])},f=function(e){var t=new Date(2010,6,15,1,0,0,0),n={"America/Denver":new Date(2011,2,13,3,0,0,0),"America/Mazatlan":new Date(2011,3,3,3,0,0,0),"
America/Chicago":new Date(2011,2,13,3,0,0,0),"America/Mexico_City":new Date(2011,3,3,3,0,0,0),"America/Asuncion":new Date(2012,9,7,3,0,0,0),"America/Santiago":
new Date(2012,9,3,3,0,0,0),"America/Campo_Grande":new Date(2012,9,21,5,0,0,0),"America/Montevideo":new Date(2011,9,2,3,0,0,0),"America/Sao_Paulo":new Date
(2011,9,16,5,0,0,0),"America/Los_Angeles":new Date(2011,2,13,8,0,0,0),"America/Santa_Isabel":new Date(2011,3,5,8,0,0,0),"America/Havana":new Date
(2012,2,10,2,0,0,0),"America/New_York":new Date(2012,2,10,7,0,0,0),"Asia/Beirut":new Date(2011,2,27,1,0,0,0),"Europe/Helsinki":new Date(2011,2,27,4,0,0,0),"Europe
/Istanbul":new Date(2011,2,28,5,0,0,0),"Asia/Damascus":new Date(2011,3,1,2,0,0,0),"Asia/Jerusalem":new Date(2011,3,1,6,0,0,0),"Asia/Gaza":new Date
(2009,2,28,0,30,0,0),"Africa/Cairo":new Date(2009,3,25,0,30,0,0),"Pacific/Auckland":new Date(2011,8,26,7,0,0,0),"Pacific/Fiji":new Date(2010,11,29,23,0,0,0),"America
/Halifax":new Date(2011,2,13,6,0,0,0),"America/Goose_Bay":new Date(2011,2,13,2,1,0,0),"America/Miquelon":new Date(2011,2,13,5,0,0,0),"America/Godthab":new Date
(2011,2,27,1,0,0,0),"Europe/Moscow":t,"Asia/Yekaterinburg":t,"Asia/Omsk":t,"Asia/Krasnoyarsk":t,"Asia/Irkutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"
Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0,0)};return n[e]};return{determine:a,date_is_dst:o,dst_start_for:f}}();t.TimeZone=function(e){"use strict";var n=
{"America/Denver":["America/Denver","America/Mazatlan"],"America/Chicago":["America/Chicago","America/Mexico_City"],"America/Santiago":["America/Santiago","
America/Asuncion","America/Campo_Grande"],"America/Montevideo":["America/Montevideo","America/Sao_Paulo"],"Asia/Beirut":["Asia/Beirut","Europe/Helsinki","Europe
/Istanbul","Asia/Damascus","Asia/Jerusalem","Asia/Gaza"],"Pacific/Auckland":["Pacific/Auckland","Pacific/Fiji"],"America/Los_Angeles":["America/Los_Angeles","America
/Santa_Isabel"],"America/New_York":["America/Havana","America/New_York"],"America/Halifax":["America/Goose_Bay","America/Halifax"],"America/Godthab":["America
/Miquelon","America/Godthab"],"Asia/Dubai":["Europe/Moscow"],"Asia/Dhaka":["Asia/Yekaterinburg"],"Asia/Jakarta":["Asia/Omsk"],"Asia/Shanghai":["Asia/Krasnoyarsk","
Australia/Perth"],"Asia/Tokyo":["Asia/Irkutsk"],"Australia/Brisbane":["Asia/Yakutsk"],"Pacific/Noumea":["Asia/Vladivostok"],"Pacific/Tarawa":["Asia/Kamchatka"],"Africa
/Johannesburg":["Asia/Gaza","Africa/Cairo"],"Asia/Baghdad":["Europe/Minsk"]},r=e,i=function(){var e=n[r],i=e.length,s=0,o=e[0];for(;s<i;s+=1){o=e[s];if(t.date_is_dst(t.
dst_start_for(o))){r=o;return}}},s=function(){return typeof n[r]!="undefined"};return s()&&i(),{name:function(){return r}}},t.olson={},t.olson.timezones={"-720,0":"Etc
/GMT+12","-660,0":"Pacific/Pago_Pago","-600,1":"America/Adak","-600,0":"Pacific/Honolulu","-570,0":"Pacific/Marquesas","-540,0":"Pacific/Gambier","-540,1":"America
/Anchorage","-480,1":"America/Los_Angeles","-480,0":"Pacific/Pitcairn","-420,0":"America/Phoenix","-420,1":"America/Denver","-360,0":"America/Guatemala","-360,1":"
America/Chicago","-360,1,s":"Pacific/Easter","-300,0":"America/Bogota","-300,1":"America/New_York","-270,0":"America/Caracas","-240,1":"America/Halifax","-240,0":"
America/Santo_Domingo","-240,1,s":"America/Santiago","-210,1":"America/St_Johns","-180,1":"America/Godthab","-180,0":"America/Argentina/Buenos_Aires","-180,1,s":"
America/Montevideo","-120,0":"Etc/GMT+2","-120,1":"Etc/GMT+2","-60,1":"Atlantic/Azores","-60,0":"Atlantic/Cape_Verde","0,0":"Etc/UTC","0,1":"Europe/London","60,1":"
Europe/Berlin","60,0":"Africa/Lagos","60,1,s":"Africa/Windhoek","120,1":"Asia/Beirut","120,0":"Africa/Johannesburg","180,0":"Asia/Baghdad","180,1":"Europe/Moscow","
210,1":"Asia/Tehran","240,0":"Asia/Dubai","240,1":"Asia/Baku","270,0":"Asia/Kabul","300,1":"Asia/Yekaterinburg","300,0":"Asia/Karachi","330,0":"Asia/Kolkata","345,0":"
Asia/Kathmandu","360,0":"Asia/Dhaka","360,1":"Asia/Omsk","390,0":"Asia/Rangoon","420,1":"Asia/Krasnoyarsk","420,0":"Asia/Jakarta","480,0":"Asia/Shanghai","480,1":"
Asia/Irkutsk","525,0":"Australia/Eucla","525,1,s":"Australia/Eucla","540,1":"Asia/Yakutsk","540,0":"Asia/Tokyo","570,0":"Australia/Darwin","570,1,s":"Australia/Adelaide","
600,0":"Australia/Brisbane","600,1":"Asia/Vladivostok","600,1,s":"Australia/Sydney","630,1,s":"Australia/Lord_Howe","660,1":"Asia/Kamchatka","660,0":"Pacific/Noumea","
690,0":"Pacific/Norfolk","720,1,s":"Pacific/Auckland","720,0":"Pacific/Tarawa","765,1,s":"Pacific/Chatham","780,0":"Pacific/Tongatapu","780,1,s":"Pacific/Apia","840,0":"
Pacific/Kiritimati"},typeof exports!="undefined"?exports.jstz=t:e.jstz=t})(this);
//cptimezone_optimized.js
(function(window){"use strict";var JSTZ_RELATIVE_PATH="sharedjs/jstz.min.js";var TIMEZONE_COOKIE="timezone";var COOKIE_TIMEZONE_MISMATCH_CLASS="
if-timezone-cookie-needs-update";var DETECTED_TZ_CLASS="detected-timezone";var SHOWN_CLASS="shown";function _get_cookie(sKey){return
decodeURIComponent(document.cookie.replace(new RegExp("(?:(?:^|.*;)\\s*"+encodeURIComponent(sKey).replace(/[\-\.\+*]/g,"\\$&")+"\\s*\\=\\s*([^;]*).*$)|^.*$"),"$1"))
||null}function _detect_timezone(){return window.jstz.determine().name()}function reset_timezone_and_reload(){return reset_timezone(location.reload.bind(location))}
function _set_cookie(callback){document.cookie=TIMEZONE_COOKIE+"="+_detect_timezone()+"; path=/";if(callback){callback()}}function set_timezone_if_unset
(on_success){return!_get_cookie(TIMEZONE_COOKIE)&&reset_timezone(on_success)}function reset_timezone(on_success){_set_cookie(on_success);return true}
function set_timezone_and_reload_if_unset(){return set_timezone_if_unset(location.reload.bind(location))}function show_cookie_timezone_mismatch_nodes(){var
detected_tz=_detect_timezone();if(detected_tz!==_get_cookie(TIMEZONE_COOKIE)){var detected_nodes=document.querySelectorAll("."+DETECTED_TZ_CLASS);[].
forEach.call(detected_nodes,function(n){n.textContent=detected_tz});var show_nodes=document.querySelectorAll("."+COOKIE_TIMEZONE_MISMATCH_CLASS);[].
forEach.call(show_nodes,function(n){n.className+=" "+SHOWN_CLASS})}}window.CPTimezone={show_cookie_timezone_mismatch_nodes:
show_cookie_timezone_mismatch_nodes,reset_timezone_and_reload:reset_timezone_and_reload,reset_timezone:reset_timezone,set_timezone_and_reload_if_unset:

set_timezone_and_reload_if_unset}})(window);

CPTimezone.reset_timezone();
</script>

<style>
@media (min-width: 481px) {
#select_user_form {
width: px;
}
}
</style>
Copyright2022 cPanel, L.L.C.

Privacy Policy

</body>

</html>

Referrer-Policy HTTP Security Header Not Detected — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:26.0

THREAT:
No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:
The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:
Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

RESULT:
Referrer-Policy HTTP Header missing on 2086 port.

Open TCP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-06-15 18:32:21.0

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.

RESULT:

Port	IANA Assigned Ports /Services	Description	Service Detected	OS On Redirected Port
21	ftp	File Transfer [Control]	ftp	
22	ssh	SSH Remote Login Protocol	ssh	
25	smtp	Simple Mail Transfer	smtp	
26	unknown	unknown	smtp	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
53	domain	Domain Name Server	DNS Server	

80	www-http	World Wide Web HTTP	http	
110	pop3	Post Office Protocol - Version 3	pop3	
143	imap	Internet Message Access Protocol	imap	
443	https	http protocol over TLS/SSL	http over ssl	
465	smtps	smtp protocol over TLS/SSL (was ssmtp)	smtp over ssl	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
587	submission	Submission	smtp	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
993	imaps	imap4 protocol over TLS/SSL	imap over ssl	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
995	pop3s	pop3 protocol over TLS/SSL (was spop3)	pop3 over ssl	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
2077	unknown	unknown	http	
2078	unknown	unknown	http over ssl	
2079	unknown	unknown	http	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
2080	unknown	unknown	http over ssl	
2082	unknown	unknown	http	
2083	unknown	unknown	unknown over ssl	
2086	unknown	unknown	http	
2087	unknown	unknown	unknown over ssl	
2095	nbx-ser	NBX SER	http	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
2096	nbx-dir	NBX DIR	unknown over ssl	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP
3306	mysql	MySQL	mysql	Ubuntu / Tiny Core Linux / Linux 2.6.x / IBM ASM / HP StoreOnce / F5 Networks Big-IP

External Links Discovered — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Number of links: 63
https://book.passkey.com/go/NorthernGreen2022
https://spothero.com/minneapolis-parking?sha_affiliate=meetmn
https://www.biddingforgood.com/auction/item/browse.action?auctionId=341698447
https://www.biddingforgood.com/auction/item/donate.action?auctionId=341698447
https://www.irrigation.org/IA/Certification/Maintain-Your-Certification/IA/Certification/Maintain-Your-Certification.aspx?hkey=94f8c009-ef08-4c73-b44e-e70f486c282f
https://www.gertenswholesale.com/
https://www.ihg.com/holidayinnexpress/hotels/us/en/minneapolis/mspdt/hoteldetail?fromRedirect=true&qSrt=sBR&qIta=99801505&icdv=99801505&qSlH=MSPDT&qGrpCd=MNL&setPMCookies=true&qSHBrC=EX&qDest=225%20South%20Eleventh%20Street,%20Minneapolis,%20MN,%20US&srb_u=1
https://e.issuu.com/embed.html?backgroundColor=%23f3f3f3&backgroundColorFullscreen=%23f3f3f3&d=ng22-advance-program-web&doAutoflipPages=true&hideIssuuLogo=true&logoImageUrl=https%3A%2F%2Fnortherngreen.org%2Fwp-content%2Fuploads%2F2021%2F11%2FNorthernGreenLogo-issuu.png&u=northerngreenexpo
https://e.issuu.com/embed.html?d=ng22-quick-guide-web&u=northerngreenexpo
https://whova.com/
https://whova.com/hybrid-event-platform/
https://whova.com/static/frontend/agenda_webpage/js/embedagenda.js?eid=north1_202201&host=https://whova.com
https://whova.com/static/frontend/xems/js/whova-speaker-widget.js?eid=north1_202201&
https://www.circlekfleetcards.com/
https://mtgf.org/
https://www.dot.state.mn.us/35w94/
https://mnla.biz/
https://www.minneapolis.org/minneapolis-convention-center/about/cleaning-protocols/
https://www.minneapolis.org/minneapolis-convention-center/attendees/
https://gravatar.com/
https://www.bachmanswholesale.com/departments
https://www.zieglercat.com/specials
https://www.zieglercat.com/specials/
https://www.hunterindustries.com/
https://www.rivercitylawnscape.com/careers
https://res.windsurfercrs.com/ibe/details.aspx?propertyid=13527&nights=5&checkin=01/09/2022&group=2201GREENE
https://www.hlsoutdoor.com/en
https://www.baileynurseries.com/
https://www.googletagmanager.com/gtag/js?id=UA-54228640-1
https://s3.amazonaws.com/meet-minneapolis/craft/cms/Attendee-Safety-Security-KBYG.pdf?mtime=20210922113243
https://maps.google.com/maps/embed/v1/place?q=Minneapolis%20Convention%20Center,1301%202nd%20Ave%20S%2C%20Minneapolis%2C%20MN%2C%2055404%2C%20US&center=44.9688369%2C-93.273865&zoom=14&key=AIzaSyAz-iChz547udxDFQBQrRwP3TJMIg0e8xY
https://ncma.org/education/segmental-retaining-walls/srw-installer/
https://ncma.org/programs/srw-certifications/basic-srw-installer-certification/
https://itunes.apple.com/app/apple-store/id716979741?pt=1944835&ct=&mt=8
https://www.apld.org/certification/
https://www.youtube.com/embed/KMTBQVupzbk?wmode=transparent&autoplay=0
https://www.youtube.com/user/NorthernGreenExpo
https://www.hyatt.com/en-US/group-booking/MSPRM/G-MNUR
https://www.turfsupradio.com/
https://play.google.com/store/apps/details?id=com.whova.event&referrer=utm_source%3D%26utm_medium%3Dportal%26utm_content%3Dnorth1_202201
https://www.expocad.com/host/fx/northerngreen/2022ngw/exfx.html
https://www.siteone.com/
https://www.isa-arbor.com/Credentials/Maintaining-Credentials/Post-Approved-CEUs
https://www.mtgf.org/

https://urldefense.com/v3/__https:/gbac.issa.com/issa-gbac-star-facility-accreditation/__;!!EB7VV9psZ_sHIy7zVFY!AkPXxwixCvj_A8ekqRrCNS-FXxGLsM7mE8FgdwZ_5cUYTzHBWT5RGX6vIxmBygWWJwr40XWgbNJg7w$
https://s.w.org/
https://www.mnla.biz/
https://youtu.be/DuyC6MiGZIc
https://globalplasmasolutions.com/how-it-works
https://twitter.com/NorthernGreenMN
https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html
https://www.cdc.gov/coronavirus/2019-ncov/vaccines/fully-vaccinated.html
https://www.bartlett.com/
http://mn.gov/aelslagid/continuinged.html
http://mn.gov/aelslagid/forms/ceform.pdf
http://www.gbac.org/
http://cdn.minneapolis.org/digital_files/154/downtown_minneapolis_parking_map.pdf
http://www.provenwinners-shrubs.com/
http://www.mtgf.org/
http://www.mnla.biz/
http://www.metrotransit.org/ride-free-on-nicollet-mall.aspx
tel:6516334987
tel:763-295-5420

Links Rejected By Crawl Scope or Exclusion List — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:26:14.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

External links discovered:
https://go.cpanel.net/ie11deprecation
https://go.cpanel.net/privacy
http://wikipedia.org/wiki/Case_sensitivity

IP based excluded links:

SSL Server Information Retrieval — port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED SSLv3 PROTOCOL IS DISABLED TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	None			
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM

AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
SEED-SHA	RSA	RSA	SHA1	SEED(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
SEED-SHA	RSA	RSA	SHA1	SEED(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
SEED-SHA	RSA	RSA	SHA1	SEED(128)	MEDIUM
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM

ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH

TLSv1.3 PROTOCOL IS DISABLED

Default Web Page (Follow HTTP Redirection) port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A

Patch:

Following are links for downloading patches to fix the vulnerabilities:

nas-201911-01

RESULT:

GET / HTTP/1.0

Host: server.northerngreenexpo.org

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>421 Misdirected Request</title>
</head><body>
<h1>Misdirected Request</h1>
<p>The client needs a new connection for this
request as the requested host name does not match

the Server Name Indication (SNI) in use for this
connection.</p>
</body></html>
GET / HTTP/1.0
Host: northerngreen.org

SSL Server Information Retrieval — port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM

DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

Links Crawled — port 2079 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 5.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

http://server.northerngreenexpo.org:2079/

Default Web Page (Follow HTTP Redirection) port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:

nas-201911-01

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org

HTTP/1.1 200 OK
Date: Wed, 26 Jan 2022 12:43:51 GMT
Server: Apache
Last-Modified: Thu, 28 Oct 2021 14:25:02 GMT
Accept-Ranges: bytes
Content-Length: 163
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html><head><META HTTP-EQUIV="Cache-control" CONTENT="no-cache"><META HTTP-EQUIV="refresh" CONTENT="0;URL=/cgi-sys/defaultwebpage.cgi"><
/head><body></body></html>

SSL Server Information Retrieval — port 21 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED				
SSLv3 PROTOCOL IS DISABLED				

TLSv1 PROTOCOL IS DISABLED
TLSv1.1 PROTOCOL IS DISABLED
TLSv1.2 PROTOCOL IS ENABLED

TLSv1.2	COMPRESSION METHOD	None			
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ADH-RC4-MD5	DH	None	MD5	RC4(128)	MEDIUM
ADH-DES-CBC3-SHA	DH	None	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
ADH-AES128-SHA	DH	None	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ADH-AES256-SHA	DH	None	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
DHE-RSA-CAMELLIA128-SHA	DH	RSA	SHA1	Camellia(128)	MEDIUM
ADH-CAMELLIA128-SHA	DH	None	SHA1	Camellia(128)	MEDIUM
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
ADH-AES128-SHA256	DH	None	SHA256	AES(128)	MEDIUM
ADH-AES256-SHA256	DH	None	SHA256	AES(256)	HIGH
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
DHE-RSA-CAMELLIA256-SHA	DH	RSA	SHA1	Camellia(256)	HIGH
ADH-CAMELLIA256-SHA	DH	None	SHA1	Camellia(256)	HIGH
SEED-SHA	RSA	RSA	SHA1	SEED(128)	MEDIUM
DHE-RSA-SEED-SHA	DH	RSA	SHA1	SEED(128)	MEDIUM
ADH-SEED-SHA	DH	None	SHA1	SEED(128)	MEDIUM
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ADH-AES128-GCM-SHA256	DH	None	AEAD	AESGCM(128)	MEDIUM
ADH-AES256-GCM-SHA384	DH	None	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH

TLSv1.3 PROTOCOL IS DISABLED

Host Scan Time

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-18 21:41:40.0

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Scan duration: 36976 seconds

Start time: Wed, Jan 26 2022, 12:22:58 GMT

End time: Wed, Jan 26 2022, 22:39:14 GMT

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 587 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

my version	**target version**
0304	0303
0399	0303
0400	0303
0499	0303

SSL Session Caching Information — port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1 session caching is enabled on the target.
TLSv1.1 session caching is enabled on the target.
TLSv1.2 session caching is enabled on the target.

SSL Session Caching Information — port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1 session caching is enabled on the target.
TLSv1.1 session caching is enabled on the target.
TLSv1.2 session caching is enabled on the target.

Default Web Page — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2086

<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">
<meta name="google" content="notranslate" />
<meta name="apple-itunes-app" content="app-id=1188352635" />
<title>WHM Login</title>
<link rel="shortcut icon" href="
AAABAAEAICAAAAEAIADSAgAAFgAAAIlQTkcNChoKAAAADUlIRFIAAAAgAAAAIAgGAAAAc3p69AAAAplJREFUWIXt1j2IHGUYB
/DfOzdnjIKFkECIVWIKvUFsIkRExa9KJCLaWAgWJx4DilZWgpDDiI0wiViIoGATP1CCEDYHSeCwUBBkgiiKURQJFiLo4d0eOxYzC8nsO9m9XcXC+8MW+3z+9
/l6l2383xH+iSBpElyTdoda26xsDqp/h0CVZ3vwKm7tMBngAs7h7eRYebG6hMtMBHbMBX89vfARHprQ5U8cwdFQlIOZCVR5di1+w/wWXT
/EY6EoN5NZCODuKZLDwzgSMCuBe2fwfX6QZwtpWzqfBBtLC3txF/ZhxKbBGx0EfsTJS77vwmGjlZrD4mUzUOXZjVjGI65cnTXchB8iupdDUb7QinsQZ7GzZftdQj2JVZ49iC
/w6JjksIo7OnS9tiA5Vn6GtyK2+1MY5NkhfGDygVrBAxH5WkPuMjR7/3UsUFLl2Q68s4XkA3ws3v9zoSjX28Kr5wL1xrTxa6ou+f6OZGvqPg9v1wZeaUjcELE/DVfNhWFSvy
/enOIZ9eq1sTokEMNLWI79oirP8g6fXpVnh7GEvY1sV/OJ4f0UhyKKk6EoX4x5pEkgXv6L6OM99YqNw
/c4kXSwG5nkIfpLCynuiahW1GWeJHkfT4aiXO9atz1XcD6I6yLyHu6bIPk6Hg9FeYZ63y9EjBarPDvQ8VJ1nd9V3D4m+RncForyxFCQ4hSeahlej88Hefauurdwaufr5z/F
/ZHAX6nL+mZE18e36IWiHLkFocqzW9QXcNz1+wUHxJ/f10JRPjvGP4pk/vj5L3F8AtufdD+/p6dJDknzX+05fDLGtife
/766t9MRgFCUffWTudwE3AqBlVCUf0xLYGTQqzzbhydwJ3Y34g318J1tmX+DPBTIz9MS2MY2/nP8DTGaqeTDf30rAAAAAElFTkSuQmCC" type="image/x-icon" />

<!-- EXTERNAL CSS -->
<link href="/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css" rel="stylesheet" type="text/css" />
<link href="/cPanel_magic_revision_1626170558/unprotected/cpanel/style_v2_optimized.css" rel="stylesheet" type="text/css" />

<style type="text/css">
/*
This css is included in the base template in case the css cannot be loaded because of access restrictions
If this css is updated, please update securitypolicy_header.html.tmpl as well

```
*/
.copyright {
background: url(
PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIzNTlwdCIgaGVpZ2h0PSIzMjAiIHZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xp

background-size: 25px auto;
}
</style>
<!--[if IE 6]>
<style type="text/css">
img {
behavior: url(/cPanel_magic_revision_1367939018/unprotected/cp_pngbehavior_login.htc);
}
</style>
<![endif]-->

<script>
window.DOM = { get: function(id) { return document.getElementById(id) } };
</script>
</head>
<body class="whm">




<input type="hidden" id="goto_uri" value="/" />
<input type="hidden" id="goto_app" value="" />
<!-- Do not remove msg_code as it is needed for automated testing - msg_code:[] -->
<div id="login-wrapper" class="group ">
<div class="wrapper">
<div id="notify">
<noscript>
<div class="error-notice">
<img src="/cPanel_magic_revision_1367939222/unprotected/cpanel/images/notice-error.png" alt="Error" align="left"/>
JavaScript is disabled in your browser.
For WHM to function properly, you must enable JavaScript.
If you do not enable JavaScript, certain features in WHM will not function correctly.
</div>
</noscript>


<div id=&apos;login-status&apos; class="error-notice" style="visibility: hidden">
<div class="content-wrapper">
<div id="login-detail">
<div id="login-status-icon-container"><span class=&apos;login-status-icon&apos;></span></div>
<div id="login-status-message">You have logged out.</div>
</div>
</div>
</div>
<div id="IE-warning" class="warn-notice IE-warning-hide" style="">
<div class="content-wrapper">
<div id="IE-warning-detail">
<div id="IE-warning-icon-container"><span class="IE-warning-icon"></span></div>
<div id="IE-warning-message">The system has detected that you are using Internet Explorer 11. cPanel &amp;amp; WHM no longer supports Internet Explorer 11. For more information, read the <a title="cPanel Blog" target="_blank" href="https://go.cpanel.net/ie11deprecation">cPanel Blog</a>.</div>
</div>
```

```
</div>
</div>
</div>

<div style="display:none">
<div id="locale-container" style="visibility:hidden">
<div id="locale-inner-container">
<div id="locale-header">
<div class="locale-head">Please select a locale:</div>
<div class="close"><a href="javascript:void(0)" onclick="toggle_locales(false)">X Close</a></div>
</div>
<div id="locale-map">
<div class="scroller clear">

<div class="locale-cell"><a href="?locale=ar"></a></div>

<div class="locale-cell"><a href="?locale=bg"></a></div>

<div class="locale-cell"><a href="?locale=cs">etina</a></div>

<div class="locale-cell"><a href="?locale=da">dansk</a></div>

<div class="locale-cell"><a href="?locale=de">Deutsch</a></div>

<div class="locale-cell"><a href="?locale=el"></a></div>

<div class="locale-cell"><a href="?locale=en">English</a></div>

<div class="locale-cell"><a href="?locale=es">espaol</a></div>

<div class="locale-cell"><a href="?locale=es_419">espaol latinoamericano</a></div>

<div class="locale-cell"><a href="?locale=es_es">espaol de Espaa</a></div>

<div class="locale-cell"><a href="?locale=fi">suomi</a></div>

<div class="locale-cell"><a href="?locale=fil">Filipino</a></div>

<div class="locale-cell"><a href="?locale=fr">franais</a></div>

<div class="locale-cell"><a href="?locale=he"></a></div>

<div class="locale-cell"><a href="?locale=hu">magyar</a></div>

<div class="locale-cell"><a href="?locale=i_cpanel_snowmen"> cPanel Snowmen - i_cpanel_snowmen</a></div>

<div class="locale-cell"><a href="?locale=i_en">i_en</a></div>

<div class="locale-cell"><a href="?locale=id">Bahasa Indonesia</a></div>

<div class="locale-cell"><a href="?locale=it">italiano</a></div>

<div class="locale-cell"><a href="?locale=ja"></a></div>

<div class="locale-cell"><a href="?locale=ko"></a></div>
```

Bahasa Melayu

norsk bokml

Nederlands

Norwegian

polski

portugus

portugus do Brasil

romn

slovenina

svenska

Trke

Ting Vit

<div id="login-sub"
>

<form action="javascript:void(0)">

<button type="submit" class="clickthrough-cont-btn">Continue</button>

```
</form>
</div>
<div id="forms">
<form novalidate id="login_form" action="/login/" method="post" target="_top" style="visibility:">
<div class="input-req-login"><label for="user">Username</label></div>
<div class="input-field-login icon username-container">
<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your username." class="std_textbox" type="text" tabindex="1" required>
</div>
<div class="input-req-login login-password-field-label"><label for="pass">Password</label></div>
<div class="input-field-login icon password-container">
<input name="pass" id="pass" placeholder="Enter your account password." class="std_textbox" type="password" tabindex="2" required>
</div>
<div class="controls">
<div class="login-btn">
<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>
</div>

</div>
<div class="clear" id="push"></div>
</form>
<!--CLOSE forms -->
</div>
<!--CLOSE login-sub -->
</div>


<!--CLOSE wrapper -->
</div>
<!--CLOSE login-sub-container -->
</div>
<!--CLOSE login-container -->
</div>

<div id="locale-footer">
<div class="locale-container">
<noscript>
<form method="get" action=".">
<select name="locale">
<option value="">Change locale</option>
<option value=&apos;ar&apos;></option><option value=&apos;bg&apos;></option><option value=&apos;cs&apos;>etina</option><option value=&apos;da&apos;
>dansk</option><option value=&apos;de&apos;>Deutsch</option><option value=&apos;el&apos;></option><option value=&apos;en&apos;>English</option><option
value=&apos;es&apos;>espaol</option><option value=&apos;es_419&apos;>espaol latinoamericano</option><option value=&apos;es_es&apos;>espaol de Espaa<
/option><option value=&apos;fi&apos;>suomi</option><option value=&apos;fil&apos;>Filipino</option><option value=&apos;fr&apos;>franais</option><option
value=&apos;he&apos;></option><option value=&apos;hu&apos;>magyar</option><option value=&apos;i_cpanel_snowmen&apos;> cPanel Snowmen -
i_cpanel_snowmen</option><option value=&apos;i_en&apos;>i_en</option><option value=&apos;id&apos;>Bahasa Indonesia</option><option value=&apos;it&apos;
>italiano</option><option value=&apos;ja&apos;></option><option value=&apos;ko&apos;></option><option value=&apos;ms&apos;>Bahasa Melayu</option><option
value=&apos;nb&apos;>norsk bokml</option><option value=&apos;nl&apos;>Nederlands</option><option value=&apos;no&apos;>Norwegian</option><option
value=&apos;pl&apos;>polski</option><option value=&apos;pt&apos;>portugus</option><option value=&apos;pt_br&apos;>portugus do Brasil</option><option
value=&apos;ro&apos;>romn</option><option value=&apos;ru&apos;></option><option value=&apos;sl&apos;>slovenina</option><option value=&apos;sv&apos;
>svenska</option><option value=&apos;th&apos;></option><option value=&apos;tr&apos;>Trke</option><option value=&apos;uk&apos;></option><option value=&apos;
vi&apos;>Ting Vit</option><option value=&apos;zh&apos;></option><option value=&apos;zh_cn&apos;></option><option value=&apos;zh_tw&apos;></option> </select>
<button style="margin-left: 10px" type="submit">Change</button>
</form>
<style type="text/css">#mobilelocalemenu, #locales_list {display:none}</style>
</noscript>
<ul id="locales_list">
```


etina

dansk

Deutsch

English

espaol

Select a locale:
English

<!--Close login-wrapper -->

<script>
var MESSAGES = {"ajax_timeout":"The connection timed out. Please try again.","invalid_login":"The login is invalid.","success":"Login successful. Redirecting ","session_locale":"The desired locale has been saved to your browser. To change the locale in this browser again, select another locale on this screen.","authenticating":"Authenticating ","no_username":"You must specify a username to log in.","network_error":"A network error occurred during your login request. Please try again. If this condition persists, contact your network service provider.","internal_error":"An internal error occurred. If this condition persists, contact the system administrator.","read_below":"Read the important information below."};

window.IS_LOGOUT = false;

//login.js
"use strict";var FADE_DURATION=.45;var FADE_DELAY=20;var AJAX_TIMEOUT=3e4;var LOCALE_FADES=[];var HAS_CSS_OPACITY="opacity"in document.body.style;var login_form=DOM.get("login_form");var login_username_el=DOM.get("user");var login_password_el=DOM.get("pass");var login_submit_el=DOM.get("login_submit");var goto_app=DOM.get("goto_app");var goto_uri=DOM.get("goto_uri");var div_cache={"login-page":DOM.get("login-page")||false,"locale-container":DOM.get("locale-container")||false,"login-container":DOM.get("login-container")||false,"locale-footer":DOM.get("locale-footer")||false,"content-cell":DOM.get("content-container")||false,invalid:DOM.get("invalid")||false};var content_cell=div_cache["content-cell"];if(div_cache["locale-footer"]){div_cache["locale-footer"].style.display="block"}var reset_form=DOM.get("reset_form");var set_opacity;if(HAS_CSS_OPACITY){set_opacity=function setOpacity(el,opacity){el.style.opacity=opacity}}else{var filter_regex=/(DXImageTransform\.Microsoft\.Alpha\()[^)]*\)/;set_opacity=function setOpacity(el,opacity){var filter_text=el.currentStyle.filter;if(!filter_text){el.style.filter="progid:DXImageTransform.Microsoft.Alpha(enabled=true)"}else if(!filter_regex.test(filter_text)){el.style.filter+=" progid:DXImageTransform.Microsoft.Alpha(enabled=true)"}else{var new_filter=filter_text.replace(filter_regex,"$1enabled=true)");if(new_filter!==filter_text){el.style.filter=new_filter}}try{el.filters.item("DXImageTransform.Microsoft.Alpha").

opacity=opacity*100}catch(e){try{el.filters.item("alpha").opacity=opacity*100}catch(error){}}}}function toggle_locales(show_locales){while(LOCALE_FADES.length)
{clearInterval(LOCALE_FADES.shift())}var newly_shown=div_cache[show_locales?"locale-container":"login-container"];set_opacity(newly_shown,0);if
(HAS_CSS_OPACITY){content_cell.replaceChild(newly_shown,content_cell.children[0])}else{var old=content_cell.children[0];content_cell.insertBefore(newly_shown,old);
newly_shown.style.display="";old.style.display="none"}LOCALE_FADES.push(fade_in(newly_shown));LOCALE_FADES.push((show_locales?fade_out:fade_in)("locale-
footer"))}function showIEBanner(){if(navigator.userAgent.indexOf("Trident")!==-1){var ieBannerDiv=document.getElementById("IE-warning");if(ieBannerDiv){ieBannerDiv.
classList.remove("IE-warning-hide")}}}showIEBanner();function fade_in(el,duration,_fade_out_instead){el=div_cache[el]||DOM.get(el)||el;var style_obj=el.style;var interval;
var cur_style=window.getComputedStyle?getComputedStyle(el,null):el.currentStyle;var visibility=cur_style.visibility;var start_opacity;if(el.offsetWidth&&visibility!=="
hidden"){if(window.getComputedStyle){start_opacity=Number(cur_style.opacity)}else{try{start_opacity=el.filters.item("DXImageTransform.Microsoft.Alpha").opacity}catch
(e){try{start_opacity=el.filters("alpha").opacity}catch(error){start_opacity=100}}start_opacity/=100}if(!start_opacity){start_opacity=0}}else{start_opacity=0;set_opacity(el,0)}if
(_fade_out_instead&&start_opacity<.01){if(start_opacity){set_opacity(el,0)}return}if(!duration){duration=FADE_DURATION}var duration_ms=duration*1e3;var start=new
Date;var end;if(_fade_out_instead){end=duration_ms+start.getTime()}else{style_obj.visibility="visible"}var fader=function(){var opacity;if(_fade_out_instead)
{opacity=start_opacity*(end-new Date)/duration_ms;if(opacity<=0){opacity=0;clearInterval(interval);style_obj.visibility="hidden"}}else{opacity=start_opacity+(1-
start_opacity)*(new Date-start)/duration_ms;if(opacity>=1){opacity=1;clearInterval(interval)}}set_opacity(el,opacity)};fader();interval=setInterval(fader,FADE_DELAY);
return interval}function fade_out(el,timeout){return fade_in(el,timeout,true)}function AjaxObject(url,callbackFunction){this._url=url;this.
_callback=callbackFunction||function(){}}AjaxObject.prototype.updating=false;AjaxObject.prototype.abort=function(){if(this.updating){this.AJAX.abort();delete this.AJAX}};
AjaxObject.prototype.update=function(passData,postMethod){if(this.AJAX){return false}var ajax=null;if(window.XMLHttpRequest){ajax=new XMLHttpRequest}else if
(window.ActiveXObject){ajax=new window.ActiveXObject("Microsoft.XMLHTTP")}else{return false}var timeout;var that=this;ajax.onreadystatechange=function(){if(ajax.
readyState==4){clearTimeout(timeout);that.updating=false;that._callback(ajax);delete that.AJAX}};try{var uri;timeout=setTimeout(function(){that.abort();show_status
(MESSAGES.ajax_timeout,"error")},AJAX_TIMEOUT);if(/post/i.test(postMethod)){uri=this._url+"?login_only=1";ajax.open("POST",uri,true);ajax.setRequestHeader
("Content-type","application/x-www-form-urlencoded");ajax.send(passData)}else{uri=this._url+"?"+passData+"&timestamp="+(new Date).getTime();ajax.open("GET",uri,
true);ajax.send(null)}this.AJAX=ajax;this.updating=true}catch(e){login_form.submit()}return true};var _text_content="textContent"in document.body?"textContent":"
innerText";function _process_parsed_login_success(result){var final_uri;var login_url_regex=/^\/(?:logout|login|openid_connect_callback)\/?/;if(result.redirect&&!
login_url_regex.test(result.redirect)){final_uri=result.redirect}var location_obj_to_redirect;if(/^(?:\/cpsess[^/]+)\/$/.test(final_uri)){location_obj_to_redirect=top.location}else{if
(result.security_token&&top!==window){for(var f=0;f<top.frames.length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result.
security_token);top.frames[f].location.href=href}}}location_obj_to_redirect=location}var redirector=function(){location_obj_to_redirect.href=final_uri+location.hash};if(result.
notices&&result.notices.length){show_status(MESSAGES.read_below,"warn");var click_form=DOM.get("clickthrough_form");var container=click_form.querySelector(".
notices");for(var n=0;n<result.notices.length;n++){var new_p=document.createElement("p");new_p.textContent=result.notices[n].content;container.appendChild(new_p)}
click_form.onsubmit=redirector;fade_out(login_form);fade_in(click_form)}else{show_status(MESSAGES.success,"success");fade_out("content-container",
FADE_DURATION/2);redirector()}}var login_button={button:login_submit_el,_suppressed_disabled:null,suppress:function(){if(this._suppressed_disabled===null){this.
_suppressed_disabled=this.button.disabled;this.button.disabled=true}},release:function(){if(this._suppressed_disabled!==null){this.button.disabled=this.
_suppressed_disabled;this._suppressed_disabled=null}},queue_disabled:function(state){if(this._suppressed_disabled===null){this.button.disabled=state}else{this.
_suppressed_disabled=state}}};function login_results(ajax_obj){var result;try{result=JSON.parse(ajax_obj&&ajax_obj.responseText)}catch(e){result=null}var
response_status=ajax_obj.status;if(response_status===200){if(result){if(result.session){window.SubmitPost.submit(result.redirect,{session:result.session,goto_uri:result.
goto_uri})}else{_process_parsed_login_success(result)}}else{login_form.submit()}return}else{if(parseInt(response_status/100,10)===4){var msg_code=result&&result.
message;show_status(MESSAGES[msg_code||"invalid_login"]||MESSAGES.invalid_login,"error");set_status_timeout()}else{show_status(MESSAGES.network_error,"
error")}document.body.classList.remove("logging-in");login_button.release();return}}var level_classes={info:"info-notice",error:"error-notice",success:"success-notice",
warn:"warn-notice"};var levels_regex="";Object.keys(level_classes).forEach(function(lv){levels_regex+="|"+level_classes[lv]});levels_regex=new RegExp("\\b(?:"
+levels_regex.slice(1)+")\\b");function show_status(message,level){DOM.get("login-status-message")[_text_content]=message;var container=DOM.get("login-status");var
this_class=level&&level_classes[level]||level_classes.info;var el_class=container.className.replace(levels_regex,this_class);container.className=el_class;fade_in
(container);reset_status_timeout()}var STATUS_TIMEOUT=null;function reset_status_timeout(){clearTimeout(STATUS_TIMEOUT);STATUS_TIMEOUT=null}function
set_status_timeout(delay){STATUS_TIMEOUT=setTimeout(function(){fade_out("login-status")},delay||8e3)}var LOGIN_SUBMIT_OK=true;document.body.
onkeyup=function(){LOGIN_SUBMIT_OK=true};document.body.onmousedown=function(){LOGIN_SUBMIT_OK=true};function do_login(){if(LOGIN_SUBMIT_OK)
{LOGIN_SUBMIT_OK=false;if(login_username_el.value.length===0){show_status(MESSAGES.no_username,"error");return false}document.body.classList.add("logging-
in");login_button.suppress();show_status(MESSAGES.authenticating,"info");var goto_app_query=goto_app&&goto_app.value?"&goto_app="+encodeURIComponent
(goto_app.value):"";var goto_uri_query=goto_uri&&goto_uri.value?"&goto_uri="+encodeURIComponent(goto_uri.value):"";var ajax_login=new AjaxObject(login_form.
action,login_results);ajax_login.update("user="+encodeURIComponent(login_username_el.value)+"&pass="+encodeURIComponent(login_password_el.value)
+goto_app_query+goto_uri_query,"POST")}return false}function show_login(){var select_user_form=document.getElementById("select_user_form");select_user_form.
style.display="none";var login_form=document.getElementById("login_form");login_form.style.visibility="";var select_users_option_block=document.getElementById
("select_users_option_block");select_users_option_block.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="block"}
function show_select_user(){var login_form=document.getElementById("login_form");login_form.style.visibility="hidden";var select_users_option_block=document.
getElementById("select_users_option_block");select_users_option_block.style.display="none";var select_user_form=document.getElementById("select_user_form");
select_user_form.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="none"}if(!window.JSON){login_button.suppress();
var new_script=document.createElement("script");new_script.onreadystatechange=function(){if(this.readyState==="loaded"||this.readyState==="complete"){this.
onreadystatechange=null;window.JSON={parse:window.jsonParse};window.jsonParse=undefined;login_button.release()}};new_script.src="/unprotected/json-minified.js";
document.getElementsByTagName("head")[0].appendChild(new_script)}try{login_form.onsubmit=do_login;set_opacity(DOM.get("login-wrapper"),0);LOCALE_FADES.
push(fade_in("login-wrapper"));var preload=document.createElement("div");preload.id="preload_images";document.body.insertBefore(preload,document.body.firstChild);if

(window.IS_LOGOUT){set_status_timeout(1e4)}else if(/(?:\?|&)locale=[^&]/.test(location.search)){show_status(MESSAGES.session_locale)}setTimeout(function(){login_username_el.focus()},100)}catch(e){if(window.console){console.warn(e)}}

//submit_post.js
(function(context){"use strict";var DOC=context.document;function _wrongType(name,value){throw new Error(""+name+" must be a string, number, or array, not "+value)}var scalarTypeIsOk={number:true,string:true};function submit(url,args){var myform=DOC.createElement("form");myform.method="POST";myform.action=url;myform.style.display="none";Object.keys(args).forEach(function(name){var values;if("object"===typeof args[name]){if(args[name]instanceof Array){values=args[name]}else{_wrongType(name,args[name])}}else if(scalarTypeIsOk[typeof args[name]]){values=[args[name]]}else{_wrongType(name,args[name])}values.forEach(function(val){var myvar=DOC.createElement("input");myvar.type="hidden";myvar.name=name;myvar.value=val;myform.appendChild(myvar)})});DOC.documentElement.appendChild(myform);myform.submit();DOC.documentElement.removeChild(myform)}context.SubmitPost={submit:submit}})(window);

//jstz.min.js
/*! jstz - v1.0.4 - 2012-12-18 */
(function(e){var t=function(){"use strict";var e="s",n=function(e){var t=-e.getTimezoneOffset();return t!==null?t:0},r=function(e,t,n){var r=new Date;return e!==undefined&&r.setFullYear(e),r.setDate(n),r.setMonth(t),r},i=function(e){return n(r(e,0,2))},s=function(e){return n(r(e,5,2))},o=function(e){var t=e.getMonth()>7?s(e.getFullYear()):i(e.getFullYear()),r=n(e);return t-r!==0},u=function(){var t=i(),n=s(),r=i()-s();return r<0?t+",1":r>0?n+",1,"+e:t+",0"},a=function(){var e=u();return new t.TimeZone(t.olson.timezones[e])},f=function(e){var t=new Date(2010,6,15,1,0,0,0),n={"America/Denver":new Date(2011,2,13,3,0,0,0),"America/Mazatlan":new Date(2011,3,3,3,0,0,0),"America/Chicago":new Date(2011,2,13,3,0,0,0),"America/Mexico_City":new Date(2011,3,3,3,0,0,0),"America/Asuncion":new Date(2012,9,7,3,0,0,0),"America/Santiago":new Date(2012,9,3,3,0,0,0),"America/Campo_Grande":new Date(2012,9,21,5,0,0,0),"America/Montevideo":new Date(2011,9,2,3,0,0,0),"America/Sao_Paulo":new Date(2011,9,16,5,0,0,0),"America/Los_Angeles":new Date(2011,2,13,8,0,0,0),"America/Santa_Isabel":new Date(2011,3,5,8,0,0,0),"America/Havana":new Date(2012,2,10,2,0,0,0),"America/New_York":new Date(2012,2,10,7,0,0,0),"Asia/Beirut":new Date(2011,2,27,1,0,0,0),"Europe/Helsinki":new Date(2011,2,27,4,0,0,0),"Europe/Istanbul":new Date(2011,2,28,5,0,0,0),"Asia/Damascus":new Date(2011,3,1,2,0,0,0),"Asia/Jerusalem":new Date(2011,3,1,6,0,0,0),"Asia/Gaza":new Date(2009,2,28,0,30,0,0),"Africa/Cairo":new Date(2009,3,25,0,30,0,0),"Pacific/Auckland":new Date(2011,8,26,7,0,0,0),"Pacific/Fiji":new Date(2010,11,29,23,0,0,0),"America/Halifax":new Date(2011,2,13,6,0,0,0),"America/Goose_Bay":new Date(2011,2,13,2,1,0,0),"America/Miquelon":new Date(2011,2,13,5,0,0,0),"America/Godthab":new Date(2011,2,27,1,0,0,0),"Europe/Moscow":t,"Asia/Yekaterinburg":t,"Asia/Omsk":t,"Asia/Krasnoyarsk":t,"Asia/Irkutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0,0)};return n[e]};return{determine:a,date_is_dst:o,dst_start_for:f}}();t.TimeZone=function(e){"use strict";var n={"America/Denver":["America/Denver","America/Mazatlan"],"America/Chicago":["America/Chicago","America/Mexico_City"],"America/Santiago":["America/Santiago","America/Asuncion","America/Campo_Grande"],"America/Montevideo":["America/Montevideo","America/Sao_Paulo"],"Asia/Beirut":["Asia/Beirut","Europe/Helsinki","Europe/Istanbul","Asia/Damascus","Asia/Jerusalem","Asia/Gaza"],"Pacific/Auckland":["Pacific/Auckland","Pacific/Fiji"],"America/Los_Angeles":["America/Los_Angeles","America/Santa_Isabel"],"America/New_York":["America/Havana","America/New_York"],"America/Halifax":["America/Goose_Bay","America/Halifax"],"America/Godthab":["America/Miquelon","America/Godthab"],"Asia/Dubai":["Europe/Moscow"],"Asia/Dhaka":["Asia/Yekaterinburg"],"Asia/Jakarta":["Asia/Omsk"],"Asia/Shanghai":["Asia/Krasnoyarsk","Australia/Perth"],"Asia/Tokyo":["Asia/Irkutsk"],"Australia/Brisbane":["Asia/Yakutsk"],"Pacific/Noumea":["Asia/Vladivostok"],"Pacific/Tarawa":["Asia/Kamchatka"],"Africa/Johannesburg":["Asia/Gaza","Africa/Cairo"],"Asia/Baghdad":["Europe/Minsk"]},r=e,i=function(){var e=n[r],i=e.length,s=0,o=e[0];for(;s<i;s+=1){o=e[s];if(t.date_is_dst(t.dst_start_for(o))){r=o;return}}},s=function(){return typeof n[r]!="undefined"};return s()&&i(),{name:function(){return r}},t.olson={},t.olson.timezones={"-720,0":"Etc/GMT+12","-660,0":"Pacific/Pago_Pago","-600,1":"America/Adak","-600,0":"Pacific/Honolulu","-570,0":"Pacific/Marquesas","-540,0":"Pacific/Gambier","-540,1":"America/Anchorage","-480,1":"America/Los_Angeles","-480,0":"Pacific/Pitcairn","-420,0":"America/Phoenix","-420,1":"America/Denver","-360,0":"America/Guatemala","-360,1":"America/Chicago","-360,1,s":"Pacific/Easter","-300,0":"America/Bogota","-300,1":"America/New_York","-270,0":"America/Caracas","-240,1":"America/Halifax","-240,0":"America/Santo_Domingo","-240,1,s":"America/Santiago","-210,1":"America/St_Johns","-180,1":"America/Godthab","-180,0":"America/Argentina/Buenos_Aires","-180,1,s":"America/Montevideo","-120,0":"Etc/GMT+2","-120,1":"Etc/GMT+2","-60,1":"Atlantic/Azores","-60,0":"Atlantic/Cape_Verde","0,0":"Etc/UTC","0,1":"Europe/London","60,1":"Europe/Berlin","60,0":"Africa/Lagos","60,1,s":"Africa/Windhoek","120,1":"Asia/Beirut","120,0":"Africa/Johannesburg","180,0":"Asia/Baghdad","180,1":"Europe/Moscow","210,1":"Asia/Tehran","240,0":"Asia/Dubai","240,1":"Asia/Baku","270,0":"Asia/Kabul","300,1":"Asia/Yekaterinburg","300,0":"Asia/Karachi","330,0":"Asia/Kolkata","345,0":"Asia/Kathmandu","360,0":"Asia/Dhaka","360,1":"Asia/Omsk","390,0":"Asia/Rangoon","420,1":"Asia/Krasnoyarsk","420,0":"Asia/Jakarta","480,0":"Asia/Shanghai","480,1":"Asia/Irkutsk","525,0":"Australia/Eucla","525,1,s":"Australia/Eucla","540,1":"Asia/Yakutsk","540,0":"Asia/Tokyo","570,0":"Australia/Darwin","570,1,s":"Australia/Adelaide","600,0":"Australia/Brisbane","600,1":"Asia/Vladivostok","600,1,s":"Australia/Sydney","630,1,s":"Australia/Lord_Howe","660,1":"Asia/Kamchatka","660,0":"Pacific/Noumea","690,0":"Pacific/Norfolk","720,1,s":"Pacific/Auckland","720,0":"Pacific/Tarawa","765,1,s":"Pacific/Chatham","780,0":"Pacific/Tongatapu","780,1,s":"Pacific/Apia","840,0":"Pacific/Kiritimati"},typeof exports!="undefined"?exports.jstz=t:e.jstz=t})(this);
//cptimezone_optimized.js
(function(window){"use strict";var JSTZ_RELATIVE_PATH="sharedjs/jstz.min.js";var TIMEZONE_COOKIE="timezone";var COOKIE_TIMEZONE_MISMATCH_CLASS="if-timezone-cookie-needs-update";var DETECTED_TZ_CLASS="detected-timezone";var SHOWN_CLASS="shown";function _get_cookie(sKey){return decodeURIComponent(document.cookie.replace(new RegExp("(?:(?:^|.*;)\\s*"+encodeURIComponent(sKey).replace(/[\-\.\+*]/g,"\\$&")+"\\s*\\=\\s*([^;]*).*$)|^.*$"),"$1"))||null}function _detect_timezone(){return window.jstz.determine().name()}function reset_timezone_and_reload(){return reset_timezone(location.reload.bind(location))}function _set_cookie(callback){document.cookie=TIMEZONE_COOKIE+"="+_detect_timezone()+"; path=/";if(callback){callback()}}function set_timezone_if_unset(on_success){return!_get_cookie(TIMEZONE_COOKIE)&&reset_timezone(on_success)}function reset_timezone(on_success){_set_cookie(on_success);return true}function set_timezone_and_reload_if_unset(){return set_timezone_if_unset(location.reload.bind(location))}function show_cookie_timezone_mismatch_nodes(){var detected_tz=_detect_timezone();if(detected_tz!==_get_cookie(TIMEZONE_COOKIE)){var detected_nodes=document.querySelectorAll("."+DETECTED_TZ_CLASS);[].forEach.call(detected_nodes,function(n){n.textContent=detected_tz});var show_nodes=document.querySelectorAll("."+COOKIE_TIMEZONE_MISMATCH_CLASS);[].

forEach.call(show_nodes,function(n){n.className+=" "+SHOWN_CLASS})}}window.CPTimezone={show_cookie_timezone_mismatch_nodes:
show_cookie_timezone_mismatch_nodes,reset_timezone_and_reload:reset_timezone_and_reload,reset_timezone:reset_timezone,set_timezone_and_reload_if_unset:
set_timezone_and_reload_if_unset}})(window);

CPTimezone.reset_timezone();
</script>

<style>
@media (min-width: 481px) {
#select_user_form {
width: px;
}
}
</style>
Copyright2022 cPanel, L.L.C.

Privacy Policy

</body>

</html>

Web Server Uses Basic HTTP Authentication over SSL — port 2080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86420
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-02-22 22:11:14.0

THREAT:
The web server was detected to accept plain text basic authentication over HTTPS. Although the password is protected in transit through SSL/TLS, Basic Authentication can be brute-forced.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2080
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)

<html>Authorization Required</html>

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 110 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no

Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

Links Crawled — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 19.00
Number of links: 18
(This number excludes form requests and links re-requested during authentication.)

http://server.northerngreenexpo.org:2082/
http://server.northerngreenexpo.org:2082/?locale=ar
http://server.northerngreenexpo.org:2082/?locale=bg
http://server.northerngreenexpo.org:2082/?locale=cs
http://server.northerngreenexpo.org:2082/?locale=da
http://server.northerngreenexpo.org:2082/?locale=de
http://server.northerngreenexpo.org:2082/?locale=el
http://server.northerngreenexpo.org:2082/?locale=en
http://server.northerngreenexpo.org:2082/?locale=es

http://server.northerngreenexpo.org:2082/?locale=es_419
http://server.northerngreenexpo.org:2082/?locale=es_es
http://server.northerngreenexpo.org:2082/?locale=fi
http://server.northerngreenexpo.org:2082/?locale=fil
http://server.northerngreenexpo.org:2082/?locale=fr
http://server.northerngreenexpo.org:2082/?locale=he
http://server.northerngreenexpo.org:2082/?locale=hu
http://server.northerngreenexpo.org:2082/?locale=i_cpanel_snowmen
http://server.northerngreenexpo.org:2082/crossdomain.xml

Secure Sockets Layer (SSL) Certificate Transparency Information — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:

00 AM GMT

SSL Server Information Retrieval — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
SEED-SHA	RSA	RSA	SHA1	SEED(128)	MEDIUM
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
CAMELLIA128-SHA256	RSA	RSA	SHA256	Camellia(128)	MEDIUM
CAMELLIA256-SHA256	RSA	RSA	SHA256	Camellia(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM

ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
ARIA128-GCM-SHA256	RSA	RSA	AEAD	ARIAGCM(128)	MEDIUM
ARIA256-GCM-SHA384	RSA	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-ARIA128-GCM-SHA256	ECDH	RSA	AEAD	ARIAGCM(128)	MEDIUM
ECDHE-RSA-ARIA256-GCM-SHA384	ECDH	RSA	AEAD	ARIAGCM(256)	HIGH
ECDHE-RSA-CAMELLIA128-SHA256	ECDH	RSA	SHA256	Camellia(128)	MEDIUM
ECDHE-RSA-CAMELLIA256-SHA384	ECDH	RSA	SHA384	Camellia(256)	HIGH
AES128-CCM	RSA	RSA	AEAD	AESCCM(128)	MEDIUM
AES256-CCM	RSA	RSA	AEAD	AESCCM(256)	HIGH
AES128-CCM-8	RSA	RSA	AEAD	AESCCM8(128)	MEDIUM
AES256-CCM-8	RSA	RSA	AEAD	AESCCM8(256)	HIGH
ECDHE-RSA-CHACHA20-POLY1305	ECDH	RSA	AEAD	CHACHA20/POLY1305(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS ENABLED					
TLS13-AES-128-GCM-SHA256	N/A	N/A	AEAD	AESGCM(128)	MEDIUM
TLS13-AES-256-GCM-SHA384	N/A	N/A	AEAD	AESGCM(256)	HIGH
TLS13-CHACHA20-POLY1305-SHA256	N/A	N/A	AEAD	CHACHA20/POLY1305(256)	HIGH

External Links Discovered — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:
Number of links: 3
https://go.cpanel.net/cleardnscache
http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=500referral
http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=cpanelwhmreferral

SSL Server Information Retrieval — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM

DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS
TLSv1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

SSL Session Caching Information — port 110 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

RESULT:

TLSv1.2 session caching is disabled on the target.

Apache HTTP Server Detected — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	45391
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-05-03 12:30:47.0

THREAT:
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Apache HTTP Server was detected on the target.

QID Detection Logic (Authenticated):
Operating System: Linux
The detection looks for Apache HTTP Server installation path using ps command. The version is extracted from the Apache HTTP Server's binary.
Operating System: Windows
This QID checks Windows registry to see if Apache HTTP Server is installed. If found, it displays the installed version.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Apache web server detected on port 80 - Apache/2.x

Scan Diagnostics — port 2080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page https://server.northerngreenexpo.org:2080/ fetched. Status code:401, Content-Type:text/html, load time:265 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 0 requests, 6 seconds. Completed 0 requests of 38 estimated requests (0%). All tests completed.

HSTS Analysis no tests enabled.
Collected 1 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(9 x 1) + paths:(0 x 1) = total (9)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 1 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 9 requests, 1 seconds. Completed 9 requests of 9 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #4 WebCgiOob: estimated time < 1 minute (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 58 estimated requests (1.72414%). All tests completed.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (46 tests, 0 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (46 tests, 1 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 59 requests, 3 seconds. Completed 59 requests of 126 estimated requests (46.8254%). XSS optimization removed 29 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
cve_2017_9805 no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(4 x 1) + paths:(11 x 1) = total (15)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 1 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 14 requests, 1 seconds. Completed 14 requests of 15 estimated requests (93.3333%). All tests completed.
Tomcat Vuln manipulation no tests enabled.
Time based path manipulation no tests enabled.
Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 0) + files:(10 x 0) + directories:(94 x 1) + paths:(9 x 1) = total (103)
Batch #5 Path manipulation: estimated time < 1 minute (116 tests, 1 inputs)
Batch #5 Path manipulation: 116 vulnsigs tests, completed 102 requests, 4 seconds. Completed 102 requests of 103 estimated requests (99.0291%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 1 minute (125 tests, 1 inputs)
Batch #5 WebCgiGeneric: 125 vulnsigs tests, completed 57 requests, 3 seconds. Completed 57 requests of 173 estimated requests (32.948%). All tests completed.
Total requests made: 286
Average server response time: 0.28 seconds

Average browser load time: 0.30 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Secure Sockets Layer (SSL) Certificate Transparency Information **port 143 / tcp over ssl**

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT

SSL Session Caching Information — port 143 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1.2 session caching is enabled on the target.

HTTP Response Method and Header Information Collected — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP header and method information collected on port 80.

GET / HTTP/1.0
Host: northerngreen.org

HTTP/1.1 301 Moved Permanently
Date: Wed, 26 Jan 2022 14:40:11 GMT
Server: Apache
Location: https://northerngreen.org/
Cache-Control: max-age=604800
Expires: Wed, 02 Feb 2022 14:40:11 GMT
Content-Length: 234
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

SSL Certificate - Information — port 587 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US

stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none

(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07
(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited

commonName	COMODO RSA Certification Authority
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4

(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6
(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:

(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:
(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b
(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

List of Web Directories — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Directory	Source
/login/	brute force
/login/	web page
/login	brute force

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

Information Disclosure — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150247
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-14 13:31:46.0

THREAT:

Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.

IMPACT:

An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

SOLUTION:

Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

Please review the issues reported below:
RESULT:
Number of technologies detected: 2
Technology name: Apache
Matched Components:
header match:
Server:Apache
Matched links: Reporting only first 3 links
http://northerngreen.org/
https://northerngreen.org/
https://northerngreen.org/feed/

Technology name: WordPress
Matched Components:
html response match:
te" type="application/json" href="https://northerngreen.org/wp-json/wp/v2/pages/1166" /><link rel="EditURI" type="application/rsd+xml" title="RSD" href="
https://northerngreen.org/xmlrpc.php?rsd" />
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="https://northerngreen.org/wp-includes/wlwmanifest.xml" />
<meta name="generator" content="WordPress 5.9" />
<link rel="canonical" href="https://northerngreen.org/" />
<link rel='shortlink' href='https://northerngreen.org/' />
<link rel=
script tag match:
<script type='text/javascript' src='https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/bsa.carousel.js?ver=5.9'
id='buy_sell_ads_pro_carousel_js_script-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/chart.js?ver=5.9' id='
buy_sell_ads_pro_chart_js_script-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/jquery.simplyscroll.js?ver=5.9'
id='buy_sell_ads_pro_simply_scroll_js_script-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/jquery.viewportchecker.js?ver=5.
9' id='buy_sell_ads_pro_viewport_checker_js_script-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-content/plugins/bsa-plugin-pro-scripteo/frontend/js/script.js?ver=5.9' id='
buy_sell_ads_pro_js_script-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-content/uploads/fusion-scripts/ab4869bbb2511aa73427cb1bc54185b8.min.js?ver=3.
6' id='fusion-scripts-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2' id='jquery-migrate-
js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-includes/js/jquery/jquery.min.js?ver=3.6.0' id='jquery-core-js'><
/script>
<script type='text/javascript' src='https://northerngreen.org/wp-includes/js/shortcode.min.js?ver=5.9' id='shortcode-js'></script>
<script type='text/javascript' src='https://northerngreen.org/wp-includes/js/thickbox/thickbox.js?ver=3.1-20121105' id='thickbox-js'><
/script>
<script type='text/javascript' src='https://northerngreen.org/wp-includes/js/underscore.min.js?ver=1.13.1' id='underscore-js'><
/script>
header match:
Link:<https://northerngreen.org/wp-json/>; rel="https://api.w.org/"
X-Pingback:https://northerngreen.org/xmlrpc.php
Matched links: Reporting only first 3 links
https://northerngreen.org/
https://northerngreen.org/comments/feed/
https://northerngreen.org/feed/

SSL Session Caching Information **port 26 / tcp over ssl**

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1 session caching is disabled on the target.
TLSv1.1 session caching is disabled on the target.
TLSv1.2 session caching is disabled on the target.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 26 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

HTTP Response Method and Header Information Collected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP header and method information collected on port 443.

GET / HTTP/1.0
Host: northerngreen.org

HTTP/1.1 421 Misdirected Request
Date: Wed, 26 Jan 2022 13:12:52 GMT
Server: Apache
Content-Length: 322
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

Maximum Number of Links Reached During Crawl — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150026
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:46.0

THREAT:
The maximum number of links specified for this scan has been reached. The links crawled to reach this threshold can include requests made via HTML form submissions and links requested in anonymous and authenticated states. Consequently, the list of links crawled (QID 150009) may reflect a lower number than the combination of links and forms requested during the crawl.

IMPACT:
Some links that lead to different areas of the site's functionality may have been missed.

SOLUTION:
Increase the maximum number of links in order to ensure broader coverage of the Web application. It is important to note that increasing the number of links crawled can dramatically increase the time required to test the Web application.

RESULT:
Maximum request count reached: 300

SSL/TLS Server supports TLS_FALLBACK_SCSV — port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1

QID:	38610
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-06-08 22:10:22.0

THREAT:
TLS cipher suite TLS_FALLBACK_SCSV is a signaling cipher suite value (SCSV). TLS servers support TLS_FALLBACK_SCSV will prevent downgrade attack.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS_FALLBACK_SCSV is supported on port 2087.

ICMP Replies Received

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2003-01-16 20:14:30.0

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 51101	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 24416	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Time Stamp (type=14 code=0)	Time Stamp Request	12:23:00 GMT
Unreachable (type=3 code=3)	UDP Port 443	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 6912	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 26274	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 80	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1238	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 98	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 21	Port Unreachable

Referrer-Policy HTTP Security Header Not Detected — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:26.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin

4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:
The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:
Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

RESULT:
Referrer-Policy HTTP Header missing on 2095 port.

Default Web Page (Follow HTTP Redirection) port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:

nas-201911-01

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2082

```
<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">
<meta name="google" content="notranslate" />
<meta name="apple-itunes-app" content="app-id=1188352635" />
<title>cPanel Login</title>
<link rel="shortcut icon" href="
AAABAAEAICAAAAEAIADSAgAAFgAAAIlQTkcNChoKAAAADUlIRFIAAAAgAAAAIAgGAAAAc3p69AAAAplJREFUWIXt1j2IHGUYB
/DfOzdnjIKFkECIVWIKvUFsIkRExa9KJCLaWAgWJx4DilZWgpDDiI0wiViIoGATP1CCEDYHSeCwUBBkgiiKURQJFiLo4d0eOxYzC8nsO9m9XcXC+8MW+3z+9
/l6l2383xH+iSBpElyTdoda26xsDqp/h0CVZ3vwKm7tMBngAs7h7eRYebG6hMtMBHbMBX89vfARHprQ5U8cwdFQlIOZCVR5di1+w/wWXT
/EY6EoN5NZCODuKZLDwzgSMCuBe2fwfX6QZwtpWzqfBBtLC3txF/ZhxKbBGx0EfsTJS77vwmGjlZrD4mUzUOXZjVjGI65cnTXchB8iupdDUb7QinsQZ7GzZftdQj2JVZ49iC
/w6JjksIo7OnS9tiA5Vn6GtyK2+1MY5NkhfGDygVrBAxH5WkPuMjR7/3UsUFLl2Q68s4XkA3ws3v9zoSjX28Kr5wL1xrTxa6ou+f6OZGvqPg9v1wZeaUjcELE/DVfNhWFSvy
/enOIZ9eq1sTokEMNLWI79oirP8g6fXpVnh7GEvY1sV/OJ4f0UhyKKk6EoX4x5pEkgXv6L6OM99YqNw
/c4kXSwG5nkIfpLCynuiahW1GWeJHkfT4aiXO9atz1XcD6I6yLyHu6bIPk6Hg9FeYZ63y9EjBarPDvQ8VJ1nd9V3D4m+RncForyxFCQ4hSeahlej88Hefauurdwaufr5z/F
/ZHAX6nL+mZE18e36IWiHLkFocqzW9QXcNz1+wUHxJ/f10JRPjvGP4pk/vj5L3F8AtufdD+/p6dJDknzX+05fDLGtife
/766t9MRgFCUffWTudwE3AqBlVCUf0xLYGTQqzzbhydwJ3Y34g318J1tmX+DPBTlz9MS2MY2/nP8DTGaqeTDf30rAAAAAElFTkSuQmCC" type="image/x-icon" />

<!-- EXTERNAL CSS -->
<link href="/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css" rel="stylesheet" type="text/css" />
<link href="/cPanel_magic_revision_1626170558/unprotected/cpanel/style_v2_optimized.css" rel="stylesheet" type="text/css" />

<style type="text/css">
/*
This css is included in the base template in case the css cannot be loaded because of access restrictions
If this css is updated, please update securitypolicy_header.html.tmpl as well
*/
.copyright {
background: url(
PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIzNTlwdCIgaGVpZ2h0PSIzMjAiIHZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xp

background-size: 25px auto;
}
</style>
<!--[if IE 6]>
<style type="text/css">
img {
behavior: url(/cPanel_magic_revision_1367939018/unprotected/cp_pngbehavior_login.htc);
}
</style>
<![endif]-->

<script>
window.DOM = { get: function(id) { return document.getElementById(id) } };
</script>
</head>
<body class="cp">




<input type="hidden" id="goto_uri" value="/" />
```

<input type="hidden" id="goto_app" value="" />
<!-- Do not remove msg_code as it is needed for automated testing - msg_code:[] -->

<noscript>

JavaScript is disabled in your browser.
For cPanel to function properly, you must enable JavaScript.
If you do not enable JavaScript, certain features in cPanel will not function correctly.

</noscript>

You have logged out.

The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the cPanel Blog.

Please select a locale:
X Close

etina

dansk

Deutsch

English

espaol

espaol latinoamericano

espaol de Espaa

suomi

Filipino

franais

magyar

 cPanel Snowmen - i_cpanel_snowmen

i_en

Bahasa Indonesia

italiano

Bahasa Melayu

norsk bokml

Nederlands

Norwegian

polski

portugus

portugus do Brasil

romn

slovenina

svenska

Trke

```
<div class="locale-cell"><a href="?locale=uk"></a></div>

<div class="locale-cell"><a href="?locale=vi">Ting Vit</a></div>

<div class="locale-cell"><a href="?locale=zh"></a></div>

<div class="locale-cell"><a href="?locale=zh_cn"></a></div>

<div class="locale-cell"><a href="?locale=zh_tw"></a></div>

</div>
</div>
</div>
</div>
</div>
<div id="content-container">
<div id="login-container">

<div id="login-sub-container">
<div id="login-sub-header">

<img class="main-logo" src="/cPanel_magic_revision_1454480641/unprotected/cpanel/images/cpanel-logo.svg" alt="logo" />

</div>
<div id="login-sub"
>
<div id="clickthrough_form" style="visibility:hidden">
<form action="javascript:void(0)">
<div class="notices"></div>
<button type="submit" class="clickthrough-cont-btn">Continue</button>
</form>
</div>
<div id="forms">
<form novalidate id="login_form" action="/login/" method="post" target="_top" style="visibility:">
<div class="input-req-login"><label for="user">Username</label></div>
<div class="input-field-login icon username-container">
<input name="user" id="user" autofocus="autofocus" value="" placeholder="Enter your username." class="std_textbox" type="text" tabindex="1" required>
</div>
<div class="input-req-login login-password-field-label"><label for="pass">Password</label></div>
<div class="input-field-login icon password-container">
<input name="pass" id="pass" placeholder="Enter your account password." class="std_textbox" type="password" tabindex="2" required>
</div>
<div class="controls">
<div class="login-btn">
<button name="login" type="submit" id="login_submit" tabindex="3">Log in</button>
</div>

</div>
<div class="clear" id="push"></div>
</form>
<!--CLOSE forms -->
</div>
<!--CLOSE login-sub -->
</div>
```

<!--CLOSE wrapper -->

<!--CLOSE login-sub-container -->

<!--CLOSE login-container -->

<noscript>
<form method="get" action=".">
<select name="locale">
<option value="">Change locale</option>
<option value='ar'></option><option value='bg'></option><option value='cs'>etina</option><option value='da'
>dansk</option><option value='de'>Deutsch</option><option value='el'></option><option value='en'>English</option><option
value='es'>espaol</option><option value='es_419'>espaol latinoamericano</option><option value='es_es'>espaol de Espaa<
/option><option value='fi'>suomi</option><option value='fil'>Filipino</option><option value='fr'>franais</option><option
value='he'></option><option value='hu'>magyar</option><option value='i_cpanel_snowmen'> cPanel Snowmen -
i_cpanel_snowmen</option><option value='i_en'>i_en</option><option value='id'>Bahasa Indonesia</option><option value='it'
>italiano</option><option value='ja'></option><option value='ko'></option><option value='ms'>Bahasa Melayu</option><option
value='nb'>norsk bokml</option><option value='nl'>Nederlands</option><option value='no'>Norwegian</option><option
value='pl'>polski</option><option value='pt'>portugus</option><option value='pt_br'>portugus do Brasil</option><option
value='ro'>romn</option><option value='ru'></option><option value='sl'>slovenina</option><option value='sv'
>svenska</option><option value='th'></option><option value='tr'>Trke</option><option value='uk'></option><option value='
vi'>Ting Vit</option><option value='zh'></option><option value='zh_cn'></option><option value='zh_tw'></option> </select>
<button style="margin-left: 10px" type="submit">Change</button>
</form>
<style type="text/css">#mobilelocalemenu, #locales_list {display:none}</style>
</noscript>
<ul id="locales_list">

etina

dansk

Deutsch

English

espaol

Select a locale:
English

<!--Close login-wrapper -->

<script>
var MESSAGES = {"invalid_login":"The login is invalid.","success":"Login successful. Redirecting ","ajax_timeout":"The connection timed out. Please try again.","internal_error":"An internal error occurred. If this condition persists, contact the system administrator.","read_below":"Read the important information below.","session_locale":"The desired locale has been saved to your browser. To change the locale in this browser again, select another locale on this screen.","authenticating":"Authenticating ","no_username":"You must specify a username to log in.","network_error":"A network error occurred during your login request. Please try again. If this condition persists, contact your network service provider."};

window.IS_LOGOUT = false;

//login.js
"use strict";var FADE_DURATION=.45;var FADE_DELAY=20;var AJAX_TIMEOUT=3e4;var LOCALE_FADES=[];var HAS_CSS_OPACITY="opacity"in document.body.style;var login_form=DOM.get("login_form");var login_username_el=DOM.get("user");var login_password_el=DOM.get("pass");var login_submit_el=DOM.get("login_submit");var goto_app=DOM.get("goto_app");var goto_uri=DOM.get("goto_uri");var div_cache={"login-page":DOM.get("login-page")||false,"locale-container":DOM.get("locale-container")||false,"login-container":DOM.get("login-container")||false,"locale-footer":DOM.get("locale-footer")||false,"content-cell":DOM.get("content-container")||false,invalid:DOM.get("invalid")||false};var content_cell=div_cache["content-cell"];if(div_cache["locale-footer"]){div_cache["locale-footer"].style.display="block"}var reset_form=DOM.get("reset_form");var set_opacity;if(HAS_CSS_OPACITY){set_opacity=function setOpacity(el,opacity){el.style.opacity=opacity}}else{var filter_regex=/(DXImageTransform\.Microsoft\.Alpha\()[^)]*\)/;set_opacity=function setOpacity(el,opacity){var filter_text=el.currentStyle.filter;if(!filter_text){el.style.filter="progid:DXImageTransform.Microsoft.Alpha(enabled=true)"}else if(!filter_regex.test(filter_text)){el.style.filter+=" progid:DXImageTransform.Microsoft.Alpha(enabled=true)"}else{var new_filter=filter_text.replace(filter_regex,"$1enabled=true)");if(new_filter!==filter_text){el.style.filter=new_filter}}try{el.filters.item("DXImageTransform.Microsoft.Alpha").opacity=opacity*100}catch(e){try{el.filters.item("alpha").opacity=opacity*100}catch(error){}}}}function toggle_locales(show_locales){while(LOCALE_FADES.length){clearInterval(LOCALE_FADES.shift())}var newly_shown=div_cache[show_locales?"locale-container":"login-container"];set_opacity(newly_shown,0);if(HAS_CSS_OPACITY){content_cell.replaceChild(newly_shown,content_cell.children[0])}else{var old=content_cell.children[0];content_cell.insertBefore(newly_shown,old);newly_shown.style.display="";old.style.display="none"}LOCALE_FADES.push(fade_in(newly_shown));LOCALE_FADES.push((show_locales?fade_out:fade_in)("locale-footer"))}function showIEBanner(){if(navigator.userAgent.indexOf("Trident")!==-1){var ieBannerDiv=document.getElementById("IE-warning");if(ieBannerDiv){ieBannerDiv.classList.remove("IE-warning-hide")}}}showIEBanner();function fade_in(el,duration,_fade_out_instead){el=div_cache[el]||DOM.get(el)||el;var style_obj=el.style;var interval;var cur_style=window.getComputedStyle?getComputedStyle(el,null):el.currentStyle;var visibility=cur_style.visibility;var start_opacity;if(el.offsetWidth&&visibility!=="hidden"){if(window.getComputedStyle){start_opacity=Number(cur_style.opacity)}else{try{start_opacity=el.filters.item("DXImageTransform.Microsoft.Alpha").opacity}catch(e){try{start_opacity=el.filters("alpha").opacity}catch(error){start_opacity=100}}start_opacity/=100}if(!start_opacity){start_opacity=0}}else{start_opacity=0;set_opacity(el,0)}if(_fade_out_instead&&start_opacity<.01){if(start_opacity){set_opacity(el,0)}return}if(!duration){duration=FADE_DURATION}var duration_ms=duration*1e3;var start=new Date;var end;if(_fade_out_instead){end=duration_ms+start.getTime()}else{style_obj.visibility="visible"}var fader=function(){var opacity;if(_fade_out_instead){opacity=start_opacity*(end-new Date)/duration_ms;if(opacity<=0){opacity=0;clearInterval(interval);style_obj.visibility="hidden"}}else{opacity=start_opacity+(1-start_opacity)*(new Date-start)/duration_ms;if(opacity>=1){opacity=1;clearInterval(interval)}}set_opacity(el,opacity)};fader();interval=setInterval(fader,FADE_DELAY);return interval}function fade_out(el,timeout){return fade_in(el,timeout,true)}function AjaxObject(url,callbackFunction){this._url=url;this._callback=callbackFunction||function(){}}AjaxObject.prototype.updating=false;AjaxObject.prototype.abort=function(){if(this.updating){this.AJAX.abort();delete this.AJAX}};AjaxObject.prototype.update=function(passData,postMethod){if(this.AJAX){return false}var ajax=null;if(window.XMLHttpRequest){ajax=new XMLHttpRequest}else if(window.ActiveXObject){ajax=new window.ActiveXObject("Microsoft.XMLHTTP")}else{return false}var timeout;var that=this;ajax.onreadystatechange=function(){if(ajax.readyState==4){clearTimeout(timeout);that.updating=false;that._callback(ajax);delete that.AJAX}};try{var uri;timeout=setTimeout(function(){that.abort();show_status(MESSAGES.ajax_timeout,"error")},AJAX_TIMEOUT);if(/post/i.test(postMethod)){uri=this._url+"?login_only=1";ajax.open("POST",uri,true);ajax.setRequestHeader("Content-type","application/x-www-form-urlencoded");ajax.send(passData)}else{uri=this._url+"?"+passData+"&timestamp="+(new Date).getTime();ajax.open("GET",uri,true);ajax.send(null)}this.AJAX=ajax;this.updating=true}catch(e){login_form.submit()}return true};var _text_content="textContent"in document.body?"textContent":"innerText";function _process_parsed_login_success(result){var final_uri;var login_url_regex=/^\/(?:logout|login|openid_connect_callback)\/?/;if(result.redirect&&!login_url_regex.test(result.redirect)){final_uri=result.redirect}var location_obj_to_redirect;if(/^(?:\/cpsess[^/]+)\/$/.test(final_uri)){location_obj_to_redirect=top.location}else{if(result.security_token&&top!==window){for(var f=0;f<top.frames.length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[\d]+/,result.security_token);top.frames[f].location.href=href}}}location_obj_to_redirect=location}var redirector=function(){location_obj_to_redirect.href=final_uri+location.hash};if(result.notices&&result.notices.length){show_status(MESSAGES.read_below,"warn");var click_form=DOM.get("clickthrough_form");var container=click_form.querySelector(".

notices");for(var n=0;n<result.notices.length;n++){var new_p=document.createElement("p");new_p.textContent=result.notices[n].content;container.appendChild(new_p)}
click_form.onsubmit=redirector;fade_out(login_form);fade_in(click_form)}else{show_status(MESSAGES.success,"success");fade_out("content-container",
FADE_DURATION/2);redirector()}}var login_button={button:login_submit_el,_suppressed_disabled:null,suppress:function(){if(this._suppressed_disabled===null){this.
_suppressed_disabled=this.button.disabled;this.button.disabled=true}},release:function(){if(this._suppressed_disabled!==null){this.button.disabled=this.
_suppressed_disabled;this._suppressed_disabled=null}},queue_disabled:function(state){if(this._suppressed_disabled===null){this.button.disabled=state}else{this.
_suppressed_disabled=state}}};function login_results(ajax_obj){var result;try{result=JSON.parse(ajax_obj&&ajax_obj.responseText)}catch(e){result=null}var
response_status=ajax_obj.status;if(response_status===200){if(result){if(result.session){window.SubmitPost.submit(result.redirect,{session:result.session,goto_uri:result.
goto_uri})}else{_process_parsed_login_success(result)}}else{login_form.submit()}return}else{if(parseInt(response_status/100,10)===4){var msg_code=result&&result.
message;show_status(MESSAGES[msg_code||"invalid_login"]||MESSAGES.invalid_login,"error");set_status_timeout()}else{show_status(MESSAGES.network_error,"
error")}document.body.classList.remove("logging-in");login_button.release();return}}var level_classes={info:"info-notice",error:"error-notice",success:"success-notice",
warn:"warn-notice"};var levels_regex="";Object.keys(level_classes).forEach(function(lv){levels_regex+="|"+level_classes[lv]});levels_regex=new RegExp("\\b(?:"
+levels_regex.slice(1)+")\\b");function show_status(message,level){DOM.get("login-status-message")[_text_content]=message;var container=DOM.get("login-status");var
this_class=level&&level_classes[level]||level_classes.info;var el_class=container.className.replace(levels_regex,this_class);container.className=el_class;fade_in
(container);reset_status_timeout()}var STATUS_TIMEOUT=null;function reset_status_timeout(){clearTimeout(STATUS_TIMEOUT);STATUS_TIMEOUT=null}function
set_status_timeout(delay){STATUS_TIMEOUT=setTimeout(function(){fade_out("login-status")},delay||8e3)}var LOGIN_SUBMIT_OK=true;document.body.
onkeyup=function(){LOGIN_SUBMIT_OK=true};document.body.onmousedown=function(){LOGIN_SUBMIT_OK=true};function do_login(){if(LOGIN_SUBMIT_OK)
{LOGIN_SUBMIT_OK=false;if(login_username_el.value.length===0){show_status(MESSAGES.no_username,"error");return false}document.body.classList.add("logging-
in");login_button.suppress();show_status(MESSAGES.authenticating,"info");var goto_app_query=goto_app&&goto_app.value?"&goto_app="+encodeURIComponent
(goto_app.value):"";var goto_uri_query=goto_uri&&goto_uri.value?"&goto_uri="+encodeURIComponent(goto_uri.value):"";var ajax_login=new AjaxObject(login_form.
action,login_results);ajax_login.update("user="+encodeURIComponent(login_username_el.value)+"&pass="+encodeURIComponent(login_password_el.value)
+goto_app_query+goto_uri_query,"POST")}return false}function show_login(){var select_user_form=document.getElementById("select_user_form");select_user_form.
style.display="none";var login_form=document.getElementById("login_form");login_form.style.visibility="";var select_users_option_block=document.getElementById
("select_users_option_block");select_users_option_block.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="block"}
function show_select_user(){var login_form=document.getElementById("login_form");login_form.style.visibility="hidden";var select_users_option_block=document.
getElementById("select_users_option_block");select_users_option_block.style.display="none";var select_user_form=document.getElementById("select_user_form");
select_user_form.style.display="block";var login_sub=document.getElementById("login-sub");login_sub.style.display="none"}if(!window.JSON){login_button.suppress();
var new_script=document.createElement("script");new_script.onreadystatechange=function(){if(this.readyState==="loaded"||this.readyState==="complete"){this.
onreadystatechange=null;window.JSON={parse:window.jsonParse};window.jsonParse=undefined;login_button.release()}};new_script.src="/unprotected/json-minified.js";
document.getElementsByTagName("head")[0].appendChild(new_script)}try{login_form.onsubmit=do_login;set_opacity(DOM.get("login-wrapper"),0);LOCALE_FADES.
push(fade_in("login-wrapper"));var preload=document.createElement("div");preload.id="preload_images";document.body.insertBefore(preload,document.body.firstChild);if
(window.IS_LOGOUT){set_status_timeout(1e4)}else if(/(?:\?|&)locale=[^&]/.test(location.search)){show_status(MESSAGES.session_locale)}setTimeout(function()
{login_username_el.focus()},100)}catch(e){if(window.console){console.warn(e)}}

//submit_post.js

(function(context){"use strict";var DOC=context.document;function _wrongType(name,value){throw new Error(""+name+" must be a string, number, or array, not "+value)}
var scalarTypeIsOk={number:true,string:true};function submit(url,args){var myform=DOC.createElement("form");myform.method="POST";myform.action=url;myform.style.
display="none";Object.keys(args).forEach(function(name){var values;if("object"===typeof args[name]){if(args[name]instanceof Array){values=args[name]}else{_wrongType
(name,args[name])}}else if(scalarTypeIsOk[typeof args[name]]){values=[args[name]]}else{_wrongType(name,args[name])}values.forEach(function(val){var myvar=DOC.
createElement("input");myvar.type="hidden";myvar.name=name;myvar.value=val;myform.appendChild(myvar)})});DOC.documentElement.appendChild(myform);myform.
submit();DOC.documentElement.removeChild(myform)}context.SubmitPost={submit:submit}})(window);

//jstz.min.js

/*! jstz - v1.0.4 - 2012-12-18 */
(function(e){var t=function(){"use strict";var e="s",n=function(e){var t=-e.getTimezoneOffset();return t!==null?t:0},r=function(e,t,n){var r=new Date;return e!==undefined&&r.
setFullYear(e),r.setDate(n),r.setMonth(t),r},i=function(e){return n(r(e,0,2))},s=function(e){return n(r(e,5,2))},o=function(e){var t=e.getMonth()>7?s(e.getFullYear()):i(e.
getFullYear()),r=n(e);return t-r!==0},u=function(){var t=i(),n=s(),r=i()-s();return r<0?t+",1":r>0?n+",1,"+e:t+",0"},a=function(){var e=u();return new t.TimeZone(t.olson.
timezones[e])},f=function(e){var t=new Date(2010,6,15,1,0,0,0),n={"America/Denver":new Date(2011,2,13,3,0,0,0),"America/Mazatlan":new Date(2011,3,3,3,0,0,0),"
America/Chicago":new Date(2011,2,13,3,0,0,0),"America/Mexico_City":new Date(2011,3,3,3,0,0,0),"America/Asuncion":new Date(2012,9,7,3,0,0,0),"America/Santiago":
new Date(2012,9,3,3,0,0,0),"America/Campo_Grande":new Date(2012,9,21,5,0,0,0),"America/Montevideo":new Date(2011,9,2,3,0,0,0),"America/Sao_Paulo":new Date
(2011,9,16,5,0,0,0),"America/Los_Angeles":new Date(2011,2,13,8,0,0,0),"America/Santa_Isabel":new Date(2011,3,5,8,0,0,0),"America/Havana":new Date
(2012,2,10,2,0,0,0),"America/New_York":new Date(2012,2,10,7,0,0,0),"Asia/Beirut":new Date(2011,2,27,1,0,0,0),"Europe/Helsinki":new Date(2011,2,27,4,0,0,0),"Europe
/Istanbul":new Date(2011,2,28,5,0,0,0),"Asia/Damascus":new Date(2011,3,1,2,0,0,0),"Asia/Jerusalem":new Date(2011,3,1,6,0,0,0),"Asia/Gaza":new Date
(2009,2,28,0,30,0,0),"Africa/Cairo":new Date(2009,3,25,0,30,0,0),"Pacific/Auckland":new Date(2011,8,26,7,0,0,0),"Pacific/Fiji":new Date(2010,11,29,23,0,0,0),"America
/Halifax":new Date(2011,2,13,6,0,0,0),"America/Goose_Bay":new Date(2011,2,13,2,1,0,0),"America/Miquelon":new Date(2011,2,13,5,0,0,0),"America/Godthab":new Date
(2011,2,27,1,0,0,0),"Europe/Moscow":t,"Asia/Yekaterinburg":t,"Asia/Omsk":t,"Asia/Krasnoyarsk":t,"Asia/Irkutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"
Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0,0)};return n[e]};return{determine:a,date_is_dst:o,dst_start_for:f}}();t.TimeZone=function(e){"use strict";var n=

{"America/Denver":["America/Denver","America/Mazatlan"],"America/Chicago":["America/Chicago","America/Mexico_City"],"America/Santiago":["America/Santiago","America/Asuncion","America/Campo_Grande"],"America/Montevideo":["America/Montevideo","America/Sao_Paulo"],"Asia/Beirut":["Asia/Beirut","Europe/Helsinki","Europe/Istanbul","Asia/Damascus","Asia/Jerusalem","Asia/Gaza"],"Pacific/Auckland":["Pacific/Auckland","Pacific/Fiji"],"America/Los_Angeles":["America/Los_Angeles","America/Santa_Isabel"],"America/New_York":["America/Havana","America/New_York"],"America/Halifax":["America/Goose_Bay","America/Halifax"],"America/Godthab":["America/Miquelon","America/Godthab"],"Asia/Dubai":["Europe/Moscow"],"Asia/Dhaka":["Asia/Yekaterinburg"],"Asia/Jakarta":["Asia/Omsk"],"Asia/Shanghai":["Asia/Krasnoyarsk","Australia/Perth"],"Asia/Tokyo":["Asia/Irkutsk"],"Australia/Brisbane":["Asia/Yakutsk"],"Pacific/Noumea":["Asia/Vladivostok"],"Pacific/Tarawa":["Asia/Kamchatka"],"Africa/Johannesburg":["Asia/Gaza","Africa/Cairo"],"Asia/Baghdad":["Europe/Minsk"]},r=e,i=function(){var e=n[r],i=e.length,s=0,o=e[0];for(;s<i;s+=1){o=e[s];if(t.date_is_dst(t.dst_start_for(o))){r=o;return}}},s=function(){return typeof n[r]!="undefined"};return s()&&i(),{name:function(){return r}}},t.olson={},t.olson.timezones={"-720,0":"Etc/GMT+12","-660,0":"Pacific/Pago_Pago","-600,1":"America/Adak","-600,0":"Pacific/Honolulu","-570,0":"Pacific/Marquesas","-540,0":"Pacific/Gambier","-540,1":"America/Anchorage","-480,1":"America/Los_Angeles","-480,0":"Pacific/Pitcairn","-420,0":"America/Phoenix","-420,1":"America/Denver","-360,0":"America/Guatemala","-360,1":"America/Chicago","-360,1,s":"Pacific/Easter","-300,0":"America/Bogota","-300,1":"America/New_York","-270,0":"America/Caracas","-240,1":"America/Halifax","-240,0":"America/Santo_Domingo","-240,1,s":"America/Santiago","-210,1":"America/St_Johns","-180,1":"America/Godthab","-180,0":"America/Argentina/Buenos_Aires","-180,1,s":"America/Montevideo","-120,0":"Etc/GMT+2","-120,1":"Etc/GMT+2","-60,1":"Atlantic/Azores","-60,0":"Atlantic/Cape_Verde","0,0":"Etc/UTC","0,1":"Europe/London","60,1":"Europe/Berlin","60,0":"Africa/Lagos","60,1,s":"Africa/Windhoek","120,1":"Asia/Beirut","120,0":"Africa/Johannesburg","180,0":"Asia/Baghdad","180,1":"Europe/Moscow","210,1":"Asia/Tehran","240,0":"Asia/Dubai","240,1":"Asia/Baku","270,0":"Asia/Kabul","300,1":"Asia/Yekaterinburg","300,0":"Asia/Karachi","330,0":"Asia/Kolkata","345,0":"Asia/Kathmandu","360,0":"Asia/Dhaka","360,1":"Asia/Omsk","390,0":"Asia/Rangoon","420,1":"Asia/Krasnoyarsk","420,0":"Asia/Jakarta","480,0":"Asia/Shanghai","480,1":"Asia/Irkutsk","525,0":"Australia/Eucla","525,1,s":"Australia/Eucla","540,1":"Asia/Yakutsk","540,0":"Asia/Tokyo","570,0":"Australia/Darwin","570,1,s":"Australia/Adelaide","600,0":"Australia/Brisbane","600,1":"Asia/Vladivostok","600,1,s":"Australia/Sydney","630,1,s":"Australia/Lord_Howe","660,1":"Asia/Kamchatka","660,0":"Pacific/Noumea","690,0":"Pacific/Norfolk","720,1,s":"Pacific/Auckland","720,0":"Pacific/Tarawa","765,1,s":"Pacific/Chatham","780,0":"Pacific/Tongatapu","780,1,s":"Pacific/Apia","840,0":"Pacific/Kiritimati"},typeof exports!="undefined"?exports.jstz=t:e.jstz=t})(this);
//cptimezone_optimized.js
(function(window){"use strict";var JSTZ_RELATIVE_PATH="sharedjs/jstz.min.js";var TIMEZONE_COOKIE="timezone";var COOKIE_TIMEZONE_MISMATCH_CLASS="if-timezone-cookie-needs-update";var DETECTED_TZ_CLASS="detected-timezone";var SHOWN_CLASS="shown";function _get_cookie(sKey){return decodeURIComponent(document.cookie.replace(new RegExp("(?:(?:^|.*;)\\s*"+encodeURIComponent(sKey).replace(/[\-\.\+*]/g,"\\$&")+"\\s*\\=\\s*([^;]*).*$)|^.*$"),"$1"))||null}function _detect_timezone(){return window.jstz.determine().name()}function reset_timezone_and_reload(){return reset_timezone(location.reload.bind(location))}function _set_cookie(callback){document.cookie=TIMEZONE_COOKIE+"="+_detect_timezone()+"; path=/";if(callback){callback()}}function set_timezone_if_unset(on_success){return!_get_cookie(TIMEZONE_COOKIE)&&reset_timezone(on_success)}function reset_timezone(on_success){_set_cookie(on_success);return true}function set_timezone_and_reload_if_unset(){return set_timezone_if_unset(location.reload.bind(location))}function show_cookie_timezone_mismatch_nodes(){var detected_tz=_detect_timezone();if(detected_tz!==_get_cookie(TIMEZONE_COOKIE)){var detected_nodes=document.querySelectorAll("."+DETECTED_TZ_CLASS);[].forEach.call(detected_nodes,function(n){n.textContent=detected_tz});var show_nodes=document.querySelectorAll("."+COOKIE_TIMEZONE_MISMATCH_CLASS);[].forEach.call(show_nodes,function(n){n.className+=" "+SHOWN_CLASS})}}window.CPTimezone={show_cookie_timezone_mismatch_nodes:show_cookie_timezone_mismatch_nodes,reset_timezone_and_reload:reset_timezone_and_reload,reset_timezone:reset_timezone,set_timezone_and_reload_if_unset:set_timezone_and_reload_if_unset}})(window);

CPTimezone.reset_timezone();
</script>

<style>
@media (min-width: 481px) {
#select_user_form {
width: px;
}
}
</style>
Copyright2022 cPanel, L.L.C.

Privacy Policy

</body>

</html>

Secure Sockets Layer (SSL) Certificate Transparency Information **port 995 / tcp over ssl**

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT

Information Disclosure — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150247
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-14 13:31:46.0

THREAT:
Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.

IMPACT:
An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

SOLUTION:
Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

Please review the issues reported below:

RESULT:
Number of technologies detected: 1
Technology name: Apache
Matched Components:
header match:
Server:Apache
Matched links: Reporting only first 3 links
http://server.northerngreenexpo.org/
http://server.northerngreenexpo.org/cgi-sys/defaultwebpage.cgi

SSL Certificate - Information — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	

(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07
(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40

(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	

(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6
(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption

(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:
(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b
(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9

(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

SSL Session Caching Information — port 993 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

RESULT:

TLSv1.2 session caching is disabled on the target.

Secure Sockets Layer (SSL) Certificate Transparency Information — port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT

SSL Certificate - Information — port 21 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:

(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:

(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07
(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:

(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6
(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	

countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:
(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4

(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b
(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

TLS Secure Renegotiation Extension Support Information — port 993 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and

thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Links Rejected By Crawl Scope or Exclusion List — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:26:14.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

External links discovered:
https://go.cpanel.net/ie11deprecation
https://go.cpanel.net/privacy

http://wikipedia.org/wiki/Case_sensitivity

IP based excluded links:

Admin interface detected — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48144
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-25 12:30:36.0

THREAT:
A website as www.abc.com/admin which is accessible over the internet in this case the QID should get flagged. It could be any website that includes /admin and accessible over the internet should be flagged with this QID. QID detection logic:
Qid detects if admin interface or directory exists at default location "/admin"

IMPACT:
NA

SOLUTION:
NA

RESULT:
Admin interface detected on : 2095 .
<title>Webmail Login</title>

SSL/TLS Server supports TLS_FALLBACK_SCSV — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38610
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-06-08 22:10:22.0

THREAT:

TLS cipher suite TLS_FALLBACK_SCSV is a signaling cipher suite value (SCSV). TLS servers support TLS_FALLBACK_SCSV will prevent downgrade attack.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

TLS_FALLBACK_SCSV is supported on port 2096.

Secure Sockets Layer (SSL) Certificate Transparency Information — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT Thu 01 Jan

Certificate no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	1970 12:00:00 AM GMT Thu 01 Jan
Certificate no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	1970 12:00:00 AM GMT

Scan Activity per Port

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-06-24 12:42:21.0

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Protocol	Port	Time
TCP	21	0:05:59
TCP	22	0:36:41
TCP	25	0:38:15
TCP	26	0:09:53
TCP	53	0:00:05
TCP	80	43:58:28
TCP	110	0:02:05
TCP	143	0:02:10
TCP	443	9:18:29
TCP	465	0:04:25
TCP	587	0:08:15
TCP	993	0:01:59
TCP	995	0:02:00
TCP	2077	3:17:24

TCP	2078	3:32:40
TCP	2079	3:15:54
TCP	2080	3:33:15
TCP	2082	6:57:56
TCP	2083	0:06:09
TCP	2086	6:32:36
TCP	2087	0:06:07
TCP	2095	6:22:22
TCP	2096	0:06:28
UDP	53	0:00:15
UDP	123	0:01:24

Secure Sockets Layer (SSL) Certificate Transparency Information — port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT Thu 01 Jan

Certificate no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	1970 12:00:00 AM GMT Thu 01 Jan
Certificate no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	1970 12:00:00 AM GMT

Scan Diagnostics — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page http://server.northerngreenexpo.org:2086/ fetched. Status code:200, Content-Type:text/html, load time:233 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 1 requests, 5 seconds. Completed 1 requests of 38 estimated requests (2.63158%). All tests completed.
HSTS Analysis no tests enabled.
No more requeues, redundant link threshold has been surpassed.
Collected 42 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 1) + directories:(9 x 25) + paths:(0 x 26) = total (225)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 26 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 81 requests, 2 seconds. Completed 81 requests of 225 estimated requests (36%). All tests completed.
WSEnumeration no tests enabled.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (68 tests, 6 inputs)
Batch #1 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 336 requests, 256 seconds. Completed 336 requests of 408 estimated requests

(82.3529%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 6 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 48 requests, 36 seconds. Completed 48 requests of 144 estimated requests (33.3333%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 6 inputs)
Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 84 requests, 76 seconds. Completed 84 requests of 84 estimated requests (100%). All tests completed.
Time based tests for Apache Struts Vulnerabilities - no tests enabled.
Batch #2 URI parameter manipulation (no auth): estimated time < 10 minutes (68 tests, 6 inputs)
Batch #2 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 336 requests, 267 seconds. Completed 336 requests of 408 estimated requests (82.3529%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 6 inputs)
Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 48 requests, 23 seconds. Completed 48 requests of 144 estimated requests (33.3333%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 6 inputs)
Batch #2 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 84 requests, 52 seconds. Completed 84 requests of 84 estimated requests (100%). All tests completed.
Batch #3 URI parameter manipulation (no auth): estimated time < 10 minutes (68 tests, 4 inputs)
Batch #3 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 224 requests, 170 seconds. Completed 224 requests of 272 estimated requests (82.3529%). All tests completed.
Batch #3 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 4 inputs)
Batch #3 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 32 requests, 12 seconds. Completed 32 requests of 96 estimated requests (33.3333%). All tests completed.
Batch #3 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 4 inputs)
Batch #3 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 56 requests, 28 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.
Batch #4 WebCgiOob: estimated time < 30 minutes (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 12 requests, 1 seconds. Completed 12 requests of 1508 estimated requests (0.795756%). All tests completed.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 10 minutes (1 tests, 18 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 18 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 30 minutes (46 tests, 11 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 1424 requests, 81 seconds. Completed 1424 requests of 1424 estimated requests (100%). XSS optimization removed 116 links. All tests completed.
Batch #4 Header manipulation: estimated time < 30 minutes (46 tests, 18 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 1062 requests, 58 seconds. Completed 1062 requests of 2268 estimated requests (46.8254%). XSS optimization removed 522 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 18 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 18 requests, 2 seconds. Completed 18 requests of 18 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
cve_2017_9805 no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 1) + directories:(4 x 25) + paths:(11 x 26) = total (386)
Batch #5 Path XSS manipulation: estimated time < 10 minutes (15 tests, 26 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 145 requests, 4 seconds. Completed 145 requests of 386 estimated requests (37.5648%). All tests completed.
Tomcat Vuln manipulation no tests enabled.
Time based path manipulation no tests enabled.
Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 1) + files:(10 x 1) + directories:(94 x 25) + paths:(9 x 26) = total (2597)
Batch #5 Path manipulation: estimated time < 10 minutes (116 tests, 26 inputs)
Batch #5 Path manipulation: 116 vulnsigs tests, completed 932 requests, 25 seconds. Completed 932 requests of 2597 estimated requests (35.8876%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 30 minutes (125 tests, 1 inputs)
Batch #5 WebCgiGeneric: 125 vulnsigs tests, completed 140 requests, 7 seconds. Completed 140 requests of 4498 estimated requests (3.11249%). All tests completed.
Total requests made: 5127
Average server response time: 1.14 seconds

Average browser load time: 1.16 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 993 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		1024	yes	80	low

ECDHE secp384r1 384	yes	192	low

SSL Server Information Retrieval — port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	None			
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
SEED-SHA	RSA	RSA	SHA1	SEED(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM

ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
SEED-SHA	RSA	RSA	SHA1	SEED(128)	MEDIUM
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
IDEA-CBC-SHA	RSA	RSA	SHA1	IDEA(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
SEED-SHA	RSA	RSA	SHA1	SEED(128)	MEDIUM
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-RC4-SHA	ECDH	RSA	SHA1	RC4(128)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
AECDH-RC4-SHA	ECDH	None	SHA1	RC4(128)	MEDIUM
AECDH-DES-CBC3-SHA	ECDH	None	SHA1	3DES(168)	MEDIUM
AECDH-AES128-SHA	ECDH	None	SHA1	AES(128)	MEDIUM
AECDH-AES256-SHA	ECDH	None	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

List of Web Directories Requiring Authentication — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86671
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:09.0

THREAT:
The service has identified a list of Web directories which require authentication to access.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Directories Requiring Authentication
/login/
/login

SSL Session Caching Information — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

RESULT:

TLSv1 session caching is enabled on the target.
TLSv1.1 session caching is enabled on the target.
TLSv1.2 session caching is enabled on the target.

SSL Server Information Retrieval — port 143 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

ENCRYPTION(KEY-

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

Admin interface detected — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48144
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-10-25 12:30:36.0

THREAT:
A website as www.abc.com/admin which is accessible over the internet in this case the QID should get flagged. It could be any website that includes /admin and accessible over the internet should be flagged with this QID. QID detection logic:
Qid detects if admin interface or directory exists at default location "/admin"

IMPACT:
NA

SOLUTION:
NA

RESULT:
Admin interface detected on : 2082 .
<title>cPanel Login</title>

WordPress Present — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	13061
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2014-10-27 23:53:36.0

THREAT:
WordPress is an open source blogging tool and a content management system (CMS). WordPress is present on the target.

IMPACT:
n/a

SOLUTION:
n/a

RESULT:
WordPress 5.9 was detected at https://northerngreen.org/

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 993 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

my version	**target version**
0304	0303
0399	0303
0400	0303
0499	0303

TLS Secure Renegotiation Extension Support Information — port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and

thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Cookies Collected — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150028
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:46:27.0

THREAT:
The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:
Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:
Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:
Total cookies: 2
session_locale=i_cpanel_snowmen; expires=Thu Jan 26 16:15:04 2023; path=/; domain=server.northerngreenexpo.org; max-age=31535990
cpsession=%3aRa70PPXbHza7cRNE%2c2215951a6e316f6e3f0360cc84d700b5; path=/; domain=server.northerngreenexpo.org; httponly

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1					
RSA		2048	no	110	low
ECDHE	secp256r1	256	yes	128	low
ECDHA	secp256r1	256	yes	128	low
TLSv1.1					
RSA		2048	no	110	low
ECDHE	secp256r1	256	yes	128	low
ECDHA	secp256r1	256	yes	128	low
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp256r1	256	yes	128	low
ECDHA	secp256r1	256	yes	128	low

Secure Sockets Layer (SSL) Certificate Transparency Information — port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT

TLS Secure Renegotiation Extension Support Information — port 143 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Last Update: 2016-03-21 16:40:23.0

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 465 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1				
RSA	2048	no	110	low
DHE	2048	yes	110	low
ECDHE secp256r1	256	yes	128	low
TLSv1.1				
RSA	2048	no	110	low
DHE	2048	yes	110	low

ECDHE secp256r1	256	yes	128	low
TLSv1.2				
RSA	2048	no	110	low
DHE	2048	yes	110	low
ECDHE secp256r1	256	yes	128	low

HTTP Response Method and Header Information Collected — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
HTTP header and method information collected on port 80.

GET / HTTP/1.0
Host: server.northerngreenexpo.org

HTTP/1.1 200 OK
Date: Wed, 26 Jan 2022 12:32:14 GMT
Server: Apache
Last-Modified: Thu, 28 Oct 2021 14:25:02 GMT
Accept-Ranges: bytes
Content-Length: 163
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0

Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

SSL Server Information Retrieval — port 26 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH

DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

List of Web Directories — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:

N/A

SOLUTION:
N/A

RESULT:

Directory	Source
/webmail/	brute force
/mailman/	brute force
/mailman	brute
/listinfo/	force
/img-sys/	web page
/mailman/	web page

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-08-27 03:28:53.0

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Host Name	Source
server.northerngreenexpo.org	FQDN

Secure Sockets Layer (SSL) Certificate Transparency Information — port 587 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT

HTTP Response Method and Header Information Collected — port 2080 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
HTTP header and method information collected on port 2080.

GET / HTTP/1.0
Host: server.northerngreenexpo.org:2080

HTTP/1.1 401 Unauthorized
Date: Wed, 26 Jan 2022 16:26:31 GMT
Server: cPanel
Persistent-Auth: false
Host: server.northerngreenexpo.org:2080
Cache-Control: no-cache, no-store, must-revalidate, private
Connection: close
Vary: Accept-Encoding
WWW-Authenticate: Basic realm="Horde DAV Server"
Content-Length: 35
Content-Type: text/html; charset="utf-8"
Expires: Fri, 01 Jan 1990 00:00:00 GMT

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 587 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38706

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS
TLSv1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled	

by	client
OCSP stapling	no
SCT extension	no

TLS Secure Renegotiation Extension Support Information — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1				
RSA	2048	no	110	low
DHE	2048	yes	110	low
ECDHE secp256r1	256	yes	128	low
TLSv1.1				
RSA	2048	no	110	low
DHE	2048	yes	110	low
ECDHE secp256r1	256	yes	128	low
TLSv1.2				
RSA	2048	no	110	low
DHE	2048	yes	110	low
ECDHE secp256r1	256	yes	128	low

HTTP Response Method and Header Information Collected — port 2078 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:

This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

HTTP header and method information collected on port 2078.

GET / HTTP/1.0
Host: server.northerngreenexpo.org:2078

HTTP/1.1 401 Unauthorized
Date: Wed, 26 Jan 2022 17:37:23 GMT
Server: cPanel
Persistent-Auth: false
Host: server.northerngreenexpo.org:2078
Cache-Control: no-cache, no-store, must-revalidate, private
Connection: close
Vary: Accept-Encoding
WWW-Authenticate: Basic realm="Restricted Area"
Content-Length: 35
Content-Type: text/html; charset="utf-8"
Expires: Fri, 01 Jan 1990 00:00:00 GMT

HTTP Methods Returned by OPTIONS Request — port 2077 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2006-01-16 22:00:56.0

THREAT:

The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:

N/A

SOLUTION:
N/A

RESULT:
Allow: PUT, UNLOCK, HEAD, POST, PROPPATCH, DELETE, MOVE, GET, COPY, MKCOL, LOCK, OPTIONS, PROPFIND

HTTP Methods Returned by OPTIONS Request — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2006-01-16 22:00:56.0

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Allow: OPTIONS,HEAD,GET,POST

SSL Session Caching Information — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Last Update:	2020-03-19 22:48:23.0

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1.1 session caching is enabled on the target.
TLSv1.2 session caching is enabled on the target.

SSL Certificate - Information — port 143 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX

localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256

(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07
(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority

(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6

(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:

(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b
(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

TLS Secure Renegotiation Extension Support Information — port 587 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

TLS Secure Renegotiation Extension Status: supported.

Links Rejected By Crawl Scope or Exclusion List — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150020
Category:	Web Application
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:26:14.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

External links discovered:
https://go.cpanel.net/cleardnscache
http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=500referral
http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=cpanelwhmreferral

IP based excluded links:

Scan Diagnostics — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page http://server.northerngreenexpo.org/ fetched. Status code:200, Content-Type:text/html, load time:92 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 2 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 3 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 2) + files:(0 x 2) + directories:(9 x 3) + paths:(0 x 5) = total (27)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 5 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 27 requests, 1 seconds. Completed 27 requests of 27 estimated requests (100%). All tests completed.
WSEnumeration no tests enabled.
Batch #4 WebCgiOob: estimated time < 1 minute (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 5 requests, 0 seconds. Completed 5 requests of 290 estimated requests (1.72414%). All tests completed.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 3 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 3 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (46 tests, 0 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 1 minute (46 tests, 2 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 118 requests, 1 seconds. Completed 118 requests of 252 estimated requests (46.8254%). XSS optimization removed 58 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 2 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 2 requests, 1 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
cve_2017_9805 no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 2) + files:(0 x 2) + directories:(4 x 3) + paths:(11 x 5) = total (67)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 5 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 66 requests, 0 seconds. Completed 66 requests of 67 estimated requests (98.5075%). All tests completed.
Tomcat Vuln manipulation no tests enabled.
Time based path manipulation no tests enabled.
Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 2) + files:(10 x 2) + directories:(94 x 3) + paths:(9 x 5) = total (353)
Batch #5 Path manipulation: estimated time < 1 minute (116 tests, 5 inputs)

Batch #5 Path manipulation: 116 vulnsigs tests, completed 349 requests, 3 seconds. Completed 349 requests of 353 estimated requests (98.8669%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 1 minute (125 tests, 1 inputs)
Batch #5 WebCgiGeneric: 125 vulnsigs tests, completed 121 requests, 5 seconds. Completed 121 requests of 865 estimated requests (13.9884%). All tests completed.
Total requests made: 737
Average server response time: 0.07 seconds

Average browser load time: 0.07 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

my version	target version
0304	rejected
0399	rejected
0400	rejected
0499	rejected

Scan Diagnostics — port 2095 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:
No action is required.

RESULT:
Target web application page http://server.northerngreenexpo.org:2095/ fetched. Status code:200, Content-Type:text/html, load time:246 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 1 requests, 9 seconds. Completed 1 requests of 38 estimated requests (2.63158%). All tests completed.
HSTS Analysis no tests enabled.
No more requeues, redundant link threshold has been surpassed.
Collected 42 links overall in 0 hours 0 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 1) + directories:(9 x 25) + paths:(0 x 26) = total (225)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 26 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 81 requests, 3 seconds. Completed 81 requests of 225 estimated requests (36%). All tests completed.
WSEnumeration no tests enabled.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (68 tests, 6 inputs)
Batch #1 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 336 requests, 263 seconds. Completed 336 requests of 408 estimated requests (82.3529%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 6 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 48 requests, 26 seconds. Completed 48 requests of 144 estimated requests (33.3333%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 6 inputs)
Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 84 requests, 52 seconds. Completed 84 requests of 84 estimated requests (100%). All tests completed.
Time based tests for Apache Struts Vulnerabilities - no tests enabled.
Batch #2 URI parameter manipulation (no auth): estimated time < 10 minutes (68 tests, 6 inputs)
Batch #2 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 336 requests, 291 seconds. Completed 336 requests of 408 estimated requests (82.3529%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 6 inputs)

Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 48 requests, 46 seconds. Completed 48 requests of 144 estimated requests (33.3333%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 6 inputs)
Batch #2 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 84 requests, 82 seconds. Completed 84 requests of 84 estimated requests (100%). All tests completed.
Batch #3 URI parameter manipulation (no auth): estimated time < 10 minutes (68 tests, 4 inputs)
Batch #3 URI parameter manipulation (no auth): 68 vulnsigs tests, completed 224 requests, 225 seconds. Completed 224 requests of 272 estimated requests (82.3529%). All tests completed.
Batch #3 URI blind SQL manipulation (no auth): estimated time < 10 minutes (8 tests, 4 inputs)
Batch #3 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 32 requests, 15 seconds. Completed 32 requests of 96 estimated requests (33.3333%). All tests completed.
Batch #3 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 4 inputs)
Batch #3 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 56 requests, 31 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.
Batch #4 WebCgiOob: estimated time < 30 minutes (54 tests, 1 inputs)
Batch #4 WebCgiOob: 54 vulnsigs tests, completed 12 requests, 1 seconds. Completed 12 requests of 1508 estimated requests (0.795756%). All tests completed.
XXE tests no tests enabled.
Arbitrary File Upload no tests enabled.
Arbitrary File Upload On Status OK no tests enabled.
HTTP call manipulation no tests enabled.
SSL Downgrade. no tests enabled.
Open Redirect no tests enabled.
CSRF no tests enabled.
Batch #4 File Inclusion analysis: estimated time < 10 minutes (1 tests, 18 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 18 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 30 minutes (46 tests, 12 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 2223 requests, 104 seconds. Completed 2223 requests of 2223 estimated requests (100%). XSS optimization removed 87 links. All tests completed.
Batch #4 Header manipulation: estimated time < 30 minutes (46 tests, 18 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 1062 requests, 47 seconds. Completed 1062 requests of 2268 estimated requests (46.8254%). XSS optimization removed 522 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 18 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 18 requests, 1 seconds. Completed 18 requests of 18 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
httpoxy no tests enabled.
cve_2017_9805 no tests enabled.
Static Session ID no tests enabled.
Login Brute Force no tests enabled.
Login Brute Force manipulation estimated time: no tests enabled
Insecurely Served Credential Forms no tests enabled.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 1) + files:(0 x 1) + directories:(4 x 25) + paths:(11 x 26) = total (386)
Batch #5 Path XSS manipulation: estimated time < 10 minutes (15 tests, 26 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 145 requests, 4 seconds. Completed 145 requests of 386 estimated requests (37.5648%). All tests completed.
Tomcat Vuln manipulation no tests enabled.
Time based path manipulation no tests enabled.
Path manipulation: Estimated requests (payloads x links): files with extension:(3 x 1) + files:(10 x 1) + directories:(94 x 25) + paths:(9 x 26) = total (2597)
Batch #5 Path manipulation: estimated time < 10 minutes (116 tests, 26 inputs)
Batch #5 Path manipulation: 116 vulnsigs tests, completed 932 requests, 29 seconds. Completed 932 requests of 2597 estimated requests (35.8876%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 30 minutes (125 tests, 1 inputs)

Batch #5 WebCgiGeneric: 125 vulnsigs tests, completed 140 requests, 6 seconds. Completed 140 requests of 4498 estimated requests (3.11249%). All tests completed.
Total requests made: 5926
Average server response time: 1.11 seconds

Average browser load time: 1.12 seconds
Scan launched using PCI WAS combined mode.
HTML form authentication unavailable, no WEBAPP entry found

Information Disclosure — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150247
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-14 13:31:46.0

THREAT:
Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.
IMPACT:
An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

SOLUTION:
Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

Please review the issues reported below:
RESULT:
Number of technologies detected: 1
Technology name: Apache
Matched Components:
header match:
Server:Apache
Matched links: Reporting only first 3 links
https://server.northerngreenexpo.org/
https://server.northerngreenexpo.org/cgi-sys/defaultwebpage.cgi

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

Default Web Page (Follow HTTP Redirection) — port 2078 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:

nas-201911-01

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2078

<html>Authorization Required</html>

SSL Server Information Retrieval — port 110 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

CIPHER	KEY-EXCHANGE	AUTHENTICATION MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED				
SSLv3 PROTOCOL IS DISABLED				

TLSv1 PROTOCOL IS DISABLED
TLSv1.1 PROTOCOL IS DISABLED
TLSv1.2 PROTOCOL IS ENABLED

TLSv1.2	COMPRESSION METHOD	None			
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH

TLSv1.3 PROTOCOL IS DISABLED

HTTP Response Method and Header Information Collected — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
HTTP header and method information collected on port 2086.

GET / HTTP/1.0
Host: server.northerngreenexpo.org:2086

HTTP/1.0 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Wed, 26 Jan 2022 17:49:00 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086
Set-Cookie: whostmgrsession=%3aU2TXcg56ITqBwj6x%2cb1e2e3543c19e26532934addaf14dde6; HttpOnly; path=/; port=2086
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086
Set-Cookie: Horde=expired; HttpOnly; domain=.server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086
Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086
Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086
Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2086
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086
Set-Cookie: imp_key=expired; HttpOnly; domain=server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2086
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Content-Length: 37893

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2003-05-09 18:28:51.0

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Hops	IP	Round Trip Time	Probe	Port
1	139.87.10.36	0.23ms	ICMP	
2	4.15.10.202	0.77ms	ICMP	
3	4.15.10.201	1.08ms	ICMP	
4	4.69.219.70	37.02ms	ICMP	
5	4.53.7.174	46.01ms	ICMP	
6	69.195.64.111	45.86ms	ICMP	
7	162.144.240.23	45.66ms	TCP	80
8	162.144.102.68	45.75ms	ICMP	

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 26 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1					
RSA		2048	no	110	low
DHE		2048	yes	110	low

ECDHE secp256r1	256	yes	128	low
TLSv1.1				
RSA	2048	no	110	low
DHE	2048	yes	110	low
ECDHE secp256r1	256	yes	128	low
TLSv1.2				
RSA	2048	no	110	low
DHE	2048	yes	110	low
ECDHE secp256r1	256	yes	128	low

Secure Sockets Layer (SSL) Certificate Transparency Information — port 26 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT Thu 01 Jan

Certificate no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	1970 12:00:00 AM GMT Thu 01 Jan
Certificate no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	1970 12:00:00 AM GMT

Referrer-Policy HTTP Security Header Not Detected — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:26.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

RESULT:

Referrer-Policy HTTP Header missing on 80 port.

HTTP Response Method and Header Information Collected — port 2082 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
HTTP header and method information collected on port 2082.

GET / HTTP/1.0
Host: server.northerngreenexpo.org:2082

HTTP/1.0 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Wed, 26 Jan 2022 16:59:21 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082
Set-Cookie: cpsession=%3ajA1tsla4mCN0hgn8%2ca0d81a092b3b76318e55dd7334878ae5; HttpOnly; path=/; port=2082
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082
Set-Cookie: Horde=expired; HttpOnly; domain=.server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082
Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082
Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082
Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=2082
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082
Set-Cookie: imp_key=expired; HttpOnly; domain=server.northerngreenexpo.org; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2082
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Content-Length: 37911

TLS Secure Renegotiation Extension Support Information — port 995 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

TLS Secure Renegotiation Extension Status: supported.

Secure Sockets Layer (SSL) Certificate Online Certificate Status Protocol (OCSP) Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:08:17.0

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Certificate #0 CN=www.build.northerngreen.org OCSP status: good
Certificate #0 CN=wordpress.northerngreenexpo.org OCSP status: good

Secure Sockets Layer (SSL) Certificate Transparency Information — port 2096 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT Thu 01 Jan

Certificate no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	1970 12:00: 00 AM GMT Thu 01 Jan
Certificate no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	1970 12:00: 00 AM GMT

SSL/TLS Server supports TLS_FALLBACK_SCSV — port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38610
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-06-08 22:10:22.0

THREAT:

TLS cipher suite TLS_FALLBACK_SCSV is a signaling cipher suite value (SCSV). TLS servers support TLS_FALLBACK_SCSV will prevent downgrade attack.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

TLS_FALLBACK_SCSV is supported on port 2083.

SSL Session Caching Information — port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1 session caching is disabled on the target.
TLSv1.1 session caching is disabled on the target.
TLSv1.2 session caching is disabled on the target.

SSL Certificate - Information — port 993 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f

(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:

(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07
(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB

stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20

(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6
(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:

(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:
(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b
(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af

(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

Links Rejected By Crawl Scope or Exclusion List — port 2078 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-03-16 23:26:14.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.e

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150026,150041,150143,150170)

IP based excluded links:

Links Crawled — port 2078 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 9.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

https://server.northerngreenexpo.org:2078/

Web Server Uses Basic HTTP Authentication over SSL — port 2078 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	86420
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-02-22 22:11:14.0

THREAT:
The web server was detected to accept plain text basic authentication over HTTPS. Although the password is protected in transit through SSL/TLS, Basic Authentication can be brute-forced.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.0
Host: server.northerngreenexpo.org:2078
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR 1.1.4322)

<html>Authorization Required</html>

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 21 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		3072	yes	132	low
DHA		3072	yes	132	low
ECDHE	secp256r1	256	yes	128	low
ECDHA	secp256r1	256	yes	128	low

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 21 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

WordPress Installation Detected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1

QID:	11764
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2018-10-06 03:31:11.0

THREAT:
WordPress is a free and open-source content management system (CMS) based on PHP and MySQL.

This QID detects WordPress installations based on the following criteria:
Existence of the wlwmanifest.xml file.
Response to a HTTP POST request to the xmlrpc.php source file.
Response to a HTTP GET request to the wp-links-opml.php source file.
Response to a HTTP GET request to the /feed/ directory.
Response of the Generator META tag.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
WordPress installation detected via the wlwmanifest.xml file on 443 over TCP.
<?xml version="1.0" encoding="utf-8" ?>

<manifest xmlns="http://schemas.microsoft.com/wlw/manifest/weblog">

<options>
<clientType>WordPress</clientType>
<supportsKeywords>Yes</supportsKeywords>
<supportsGetTags>Yes</supportsGetTags>
</options>

<weblog>
<serviceName>WordPress</serviceName>
<imageUrl>images/wlw/wp-icon.png</imageUrl>
<watermarkImageUrl>images/wlw/wp-watermark.png</watermarkImageUrl>
<homepageLinkText>View site</homepageLinkText>
<adminLinkText>Dashboard</adminLinkText>
<adminUrl>
<![CDATA[
{blog-postapi-url}/../wp-admin/
]]>
</adminUrl>
<postEditingUrl>
<![CDATA[
{blog-postapi-url}/../wp-admin/post.php?action=edit&post={post-id}
]]>
</postEditingUrl>
</weblog>

<buttons>
<button>
<id>0</id>
<text>Manage Comments</text>
<imageUrl>images/wlw/wp-comments.png</imageUrl>

<clickUrl>
<![CDATA[
{blog-postapi-url}/../wp-admin/edit-comments.php
]]>
</clickUrl>
</button>

</buttons>

</manifest>

SSL Session Caching Information — port 587 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1 session caching is disabled on the target.
TLSv1.1 session caching is disabled on the target.
TLSv1.2 session caching is disabled on the target.

SSL Server default Diffie-Hellman prime information — port 26 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38609
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-05-26 22:09:34.0

THREAT:
Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS. - For fixed primes: 1024 and below are considered unsafe. - For variable primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
SSL server default to use Diffie-Hellman key exchange method with variable 2048(bits) prime

TLS Secure Renegotiation Extension Support Information — port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 23:14:58.0

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

HTTP Methods Returned by OPTIONS Request — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2006-01-16 22:00:56.0

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Allow: GET,POST,OPTIONS,HEAD

SSL Certificate - Information — port 2087 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption

(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47

(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64
(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07
(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester

localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50

(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6
(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:

(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:
(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl
(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b
(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea

(2) 21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

List of Web Directories — port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Directory	Source
/login/	brute force
/login/	web page
/login	brute force

SSH daemon information retrieving — port 22 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38047
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2018-04-04 16:20:22.0

THREAT:

SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

```
For Red Hat ES 4:-
SSH1 supported                              yes
Supported authentification methods for SSH1     RSA,password
Supported ciphers for SSH1                  3des,blowfish
SSH2 supported                              yes
Supported keys exchange algorithm for SSH2      diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-
Supported decryption ciphers for SSH2           aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rij
Supported encryption ciphers for SSH2           aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rij
Supported decryption mac for SSH2               hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac
Supported encryption mac for SSH2               hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac
Supported authentification methods for SSH2     publickey,gssapi-with-mic,password
```

IMPACT:

Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:

SSH version 2 is preferred over SSH version 1.

RESULT:

SSH1 supported	**no**
SSH2 supported	yes
Supported key exchange algorithms for SSH2	diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
Supported host key algorithms for SSH2	ssh-rsa,ssh-dss
Supported decryption ciphers for SSH2	aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc, arcfour,rijndael-cbc@lysator.liu.se
Supported encryption ciphers for SSH2	aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc, arcfour,rijndael-cbc@lysator.liu.se
Supported decryption macs for SSH2	hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com, hmac-sha1-96,hmac-md5-96
Supported encryption macs for SSH2	hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com, hmac-sha1-96,hmac-md5-96
Supported decompression for SSH2	none,zlib@openssh.com
Supported compression for SSH2	none,zlib@openssh.com
Supported authentication methods for SSH2	publickey,gssapi-keyex,gssapi-with-mic,password

Secure Sockets Layer (SSL) Certificate Transparency Information — port 21 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT

Links Crawled port 2086 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 11.00
Number of links: 18
(This number excludes form requests and links re-requested during authentication.)

http://server.northerngreenexpo.org:2086/
http://server.northerngreenexpo.org:2086/?locale=ar
http://server.northerngreenexpo.org:2086/?locale=bg
http://server.northerngreenexpo.org:2086/?locale=cs
http://server.northerngreenexpo.org:2086/?locale=da
http://server.northerngreenexpo.org:2086/?locale=de
http://server.northerngreenexpo.org:2086/?locale=el
http://server.northerngreenexpo.org:2086/?locale=en
http://server.northerngreenexpo.org:2086/?locale=es
http://server.northerngreenexpo.org:2086/?locale=es_419
http://server.northerngreenexpo.org:2086/?locale=es_es
http://server.northerngreenexpo.org:2086/?locale=fi
http://server.northerngreenexpo.org:2086/?locale=fil
http://server.northerngreenexpo.org:2086/?locale=fr
http://server.northerngreenexpo.org:2086/?locale=he
http://server.northerngreenexpo.org:2086/?locale=hu
http://server.northerngreenexpo.org:2086/?locale=i_cpanel_snowmen
http://server.northerngreenexpo.org:2086/crossdomain.xml

TLS Secure Renegotiation Extension Support Information — port 26 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS
TLSv1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

Secure Sockets Layer (SSL) Certificate Transparency Information — port 110 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=server.northerngreenexpo.org			
Certificate	yes	Google ' Xenon2022' log	ct.googleapis.com/logs/xenon2022/	46a555eb75fa912030b5a28969f4f37d112c4174befd49b885abf2fc70fe6d47	Thu 09 Dec 2021 11:04:11 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 2083 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:52.0

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1				
RSA	2048	no	110	low
ECDHE secp256r1	256	yes	128	low
ECDHA secp256r1	256	yes	128	low
TLSv1.				
1				
RSA	2048	no	110	low
ECDHE secp256r1	256	yes	128	low
ECDHA secp256r1	256	yes	128	low
TLSv1.				
2				
RSA	2048	no	110	low
ECDHE secp256r1	256	yes	128	low
ECDHA secp256r1	256	yes	128	low

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 26 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Last Update: 2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

RESULT:

NAME	STATUS
TLSv1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

SSL Session Caching Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

RESULT:

TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is enabled on the target.

SSL Certificate - Information — port 2080 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	25:ed:0a:c2:98:43:d6:13:e1:fe:c7:5a:02:1b:2f:8f
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(0)SUBJECT NAME	
commonName	server.northerngreenexpo.org
(0)Valid From	Dec 9 00:00:00 2021 GMT
(0)Valid Till	Dec 9 23:59:59 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:a2:2d:18:76:7e:8b:83:13:32:7b:00:43:18:63:
(0)	7f:63:16:60:12:8a:3a:88:44:a4:fd:8a:62:3e:be:
(0)	75:34:17:38:6d:40:07:ea:b4:d3:a5:fb:78:85:60:
(0)	e8:4f:76:b2:fd:cb:fe:2e:03:8e:30:13:b0:5d:f0:
(0)	b1:f6:91:fa:a0:9a:ff:b3:b1:43:5e:06:42:31:da:
(0)	d1:66:4b:2a:23:61:5b:09:41:11:d4:79:ba:2c:06:
(0)	34:a9:2a:b0:a7:38:22:68:c9:1f:52:bc:39:df:61:
(0)	2f:47:c3:5f:27:6c:9c:9d:4b:d4:aa:84:5e:23:90:
(0)	41:cc:ae:6a:e6:19:7c:1e:4c:05:55:2d:f7:1f:91:
(0)	f0:8c:83:6b:4f:3e:1a:86:7e:25:c4:56:56:9f:d5:
(0)	02:ef:6e:21:4d:38:32:46:e6:52:1a:b1:e9:3f:8c:
(0)	3a:8a:36:d6:4a:71:61:df:91:1f:c0:fd:35:bc:95:
(0)	e9:11:a8:ed:c2:64:37:3a:fa:e6:ec:e4:52:fc:3e:
(0)	7f:2d:55:9a:82:f4:3d:4c:f4:6a:ae:f2:7d:47:b4:
(0)	1c:c8:7c:cf:6e:67:c8:80:30:b5:f2:db:98:47:1f:
(0)	7e:54:13:0a:a5:d9:91:0e:69:6b:85:fb:fb:93:3d:
(0)	52:b8:2c:8a:5a:b2:a0:a7:2b:c5:1f:7e:94:a4:c0:
(0)	57:b3
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Authority Key Identifier	keyid:7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(0)X509v3 Subject Key Identifier	16:9D:09:08:84:08:26:FF:C9:B0:AF:9E:B5:6F:91:FC:BB:0F:7A:CC
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Basic Constraints	critical

(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(0)	CPS: https://sectigo.com/CPS
(0)	Policy: 2.23.140.1.2.1
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
(0)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
(0)	OCSP - URI:http://ocsp.comodoca.com
(0)X509v3 Subject Alternative Name	DNS:server.northerngreenexpo.org
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
(0)	11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
(0)	Timestamp : Dec 9 11:04:11.477 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:22:7D:09:0B:7C:DD:59:99:A5:7F:DE:60:
(0)	EF:11:DC:A6:2F:BB:40:2C:A4:44:09:36:D3:43:2B:A4:
(0)	44:2B:E1:29:02:21:00:A5:DE:49:7E:29:AB:EC:71:15:
(0)	00:17:7B:9B:F0:B1:83:C4:4E:00:3B:29:08:BC:83:66:
(0)	0F:15:E0:D9:72:78:96
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Dec 9 11:04:11.404 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:9E:10:39:F9:AE:D5:FA:ED:6C:0E:37:
(0)	80:E0:E5:14:F6:F8:AE:0B:1E:D8:D6:2D:16:50:4A:D6:
(0)	E0:F7:B3:45:A8:02:21:00:E3:39:B3:06:46:54:46:8C:
(0)	1E:3A:E4:64:1E:F9:16:7E:EB:61:8F:82:CF:80:1E:9B:
(0)	81:A3:A4:15:DA:51:0F:B1
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Dec 9 11:04:11.370 2021 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:1F:1E:52:0D:33:D7:D7:54:56:95:7D:18:
(0)	EB:4F:94:16:6C:78:C9:2A:2F:5A:FF:F1:39:D7:09:FC:
(0)	35:00:E2:EA:02:21:00:A2:F7:1F:B6:63:7E:80:F7:B6:
(0)	41:8A:80:98:07:A3:BD:E6:9E:97:DD:C0:04:24:0B:12:
(0)	FC:23:F7:18:3B:3D:F0
(0)Signature	(256 octets)
(0)	42:41:68:58:90:9d:ab:08:9e:2f:5d:e4:0b:df:95:ea
(0)	b0:52:19:94:58:57:61:e0:6f:a8:62:ac:45:e4:1e:2b
(0)	fc:93:e2:fd:01:3c:88:37:db:03:10:8c:00:d2:0d:79
(0)	4a:f1:58:6e:cb:64:c5:03:a3:9d:e8:ea:3a:d1:74:a3
(0)	c1:bf:01:63:77:4d:bf:2b:47:3f:01:d2:90:a2:e7:d9
(0)	78:ec:d1:63:65:a3:7a:0a:3c:f3:35:af:da:cf:c8:64

(0)	dd:2d:0d:04:a5:1e:65:a8:57:36:71:30:38:06:06:9c
(0)	de:69:11:cb:d6:80:c7:a9:e4:e3:4d:67:ca:ff:05:e3
(0)	83:01:aa:6b:74:1d:f5:34:d4:b6:c1:56:aa:7d:90:07
(0)	b5:13:dc:2b:46:2f:b9:1c:55:d0:1e:86:2c:9d:8d:98
(0)	66:63:4e:3b:83:c7:1c:64:6c:d3:c8:6c:66:21:f6:d0
(0)	4a:4c:53:ab:03:c5:aa:87:67:87:ee:86:30:2a:67:40
(0)	db:e9:f8:0f:8f:45:d6:85:25:ce:b5:33:d6:7d:6d:19
(0)	02:cc:d3:6c:79:dc:02:04:2f:46:15:89:9b:b3:ad:8d
(0)	3c:40:68:8c:68:e2:34:b3:ee:e5:e3:bf:c3:6b:2c:19
(0)	a7:3b:28:59:86:ea:a1:44:33:21:88:9b:4e:12:5b:05
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	f0:1d:4b:ee:7b:7c:a3:7b:3c:05:66:ac:05:97:24:58
(1)Signature Algorithm	sha384WithRSAEncryption
(1)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	TX
localityName	Houston
organizationName	"cPanel, Inc."
commonName	"cPanel, Inc. Certification Authority"
(1)Valid From	May 18 00:00:00 2015 GMT
(1)Valid Till	May 17 23:59:59 2025 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:8b:5e:01:56:b9:ec:6b:11:ef:48:e9:43:9e:9b:
(1)	c8:ba:53:91:a5:bd:ab:2a:fa:5e:3a:35:e1:0d:5c:
(1)	35:ea:52:a8:99:34:28:0f:7e:59:2b:48:6b:e7:b4:
(1)	d7:4b:7d:2f:83:cf:fe:8b:26:c3:59:79:1f:60:a1:
(1)	69:a7:5a:cb:9f:37:21:ef:18:bd:9b:fd:41:eb:75:
(1)	7c:b7:96:d9:5e:86:cb:2a:12:e2:a7:f7:03:e4:ce:
(1)	e6:05:f7:41:9b:1e:bc:d2:f6:d1:66:69:51:0c:de:
(1)	b5:ed:3c:0b:27:cf:88:8e:20:3d:e3:4e:95:8f:15:
(1)	34:c6:26:cb:f7:3f:64:e9:f5:30:25:7d:cd:a9:39:
(1)	9b:3f:ea:7a:69:2b:8b:c4:7d:0b:f8:56:93:b6:6b:
(1)	96:ca:ec:cf:d2:7b:bd:43:be:d3:f5:89:da:4d:74:
(1)	49:21:c4:bd:f5:30:bc:bc:49:a9:65:15:b3:d6:ff:
(1)	bf:1d:90:94:9c:08:25:b6:ad:cf:fc:c7:d9:fb:55:
(1)	d5:19:d0:4a:bf:62:46:e5:24:ed:8f:be:64:98:0c:
(1)	6a:51:9e:7a:80:73:20:a9:b4:d9:bf:43:6a:9e:10:
(1)	ad:2b:a0:cd:64:ad:40:39:d2:e2:b8:db:c2:f2:3a:
(1)	a3:e2:b7:16:97:1f:1e:f6:cf:df:3c:1e:58:e9:00:
(1)	07:6b
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Authority Key Identifier	keyid:BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(1)X509v3 Subject Key Identifier	7E:03:5A:65:41:6B:A7:7E:0A:E1:B8:9D:08:EA:1D:8E:1D:6A:C7:65
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign

(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(1)X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.6449.1.2.2.52
(1)	Policy: 2.23.140.1.2.1
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.comodoca.com/COMODORSACertificationAuthority.crl
(1)Authority Information Access	CA Issuers - URI:http://crt.comodoca.com/COMODORSAAddTrustCA.crt
(1)	OCSP - URI:http://ocsp.comodoca.com
(1)Signature	(512 octets)
(1)	10:9f:a0:60:08:81:74:a1:a0:84:78:60:4c:39:39:da
(1)	64:77:ef:19:0a:72:39:23:94:3b:91:7d:7f:34:8b:97
(1)	58:4e:59:0a:2d:68:c3:10:42:b0:a0:7a:81:8c:7b:ab
(1)	31:32:20:39:e4:22:73:e0:de:c9:17:5d:83:c5:75:2d
(1)	e1:11:47:59:01:9e:5d:c0:f4:dd:12:6a:d0:6d:30:20
(1)	e8:b3:ca:4f:df:9a:e0:a7:17:9f:1a:2f:87:7e:eb:50
(1)	e1:53:f3:f8:47:d9:8c:60:f2:c9:65:65:9c:f0:da:01
(1)	e6:b2:f2:d8:07:98:87:df:37:89:98:55:12:42:c9:e4
(1)	2d:de:2d:be:aa:64:94:4e:d9:2e:e6:c2:d5:f2:c0:e6
(1)	e9:ea:19:3e:37:0b:89:5f:c9:3a:f8:4f:47:40:3e:af
(1)	1a:7f:a2:f6:85:01:88:17:36:b5:23:ea:b9:fe:ba:6b
(1)	48:0b:02:20:39:ae:c3:61:eb:95:a5:a1:73:c7:1c:5f
(1)	54:33:73:57:4b:36:8b:9b:5b:28:e3:3e:b1:0b:78:5c
(1)	6b:14:a7:10:cc:e5:da:3f:ba:e9:d6:b2:2d:1d:70:54
(1)	ba:5e:ab:7d:4f:29:89:10:e0:3a:90:04:c5:ee:b9:8e
(1)	43:a2:e3:63:58:7f:49:8b:71:3e:57:62:23:40:d1:5d
(1)	96:64:22:61:56:9f:96:67:47:87:bc:e5:00:20:a4:68
(1)	e2:c1:a0:81:7b:68:73:08:c4:6d:4e:70:79:e8:dd:55
(1)	d7:09:5c:b9:9d:0a:95:a6:0c:d9:db:e2:8a:55:eb:b9
(1)	e1:e7:9a:95:14:4c:58:06:41:c1:10:aa:aa:b1:3a:e2
(1)	a5:4a:4a:e0:d9:c9:1f:c2:a0:97:bb:06:ef:19:00:db
(1)	02:be:96:f1:fb:54:8f:93:9a:fa:30:22:36:a9:77:26
(1)	1f:94:28:93:e9:13:3d:45:d1:3a:35:48:1e:98:0d:82
(1)	70:c0:0b:5a:28:87:a1:78:51:3f:b5:a7:5c:a6:91:22
(1)	00:42:4c:b9:80:15:80:2a:b1:2d:89:4f:f7:ba:1e:18
(1)	c4:8c:59:1e:73:49:a3:a8:7b:bc:1f:f7:56:4d:50:9f
(1)	67:16:a7:c7:17:48:e7:6d:54:57:76:6e:97:58:5b:78
(1)	64:a4:ed:62:b4:00:3b:06:7e:79:b8:58:5f:6e:84:d6
(1)	43:bc:4f:db:39:aa:28:f0:c1:89:09:c5:fb:e3:18:44
(1)	b7:e5:b2:8b:5d:95:f9:23:5a:0b:72:f7:69:3a:d6:57
(1)	8b:e1:e9:f4:60:be:c4:51:2b:11:ac:fe:48:b3:72:73
(1)	ca:13:50:73:0d:04:76:ca:01:e1:42:c2:d7:21:cf:f9
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	67:de:f4:3e:f1:7b:da:e2:4f:f5:94:06:06:d2:c0:84
(2)Signature Algorithm	sha384WithRSAEncryption
(2)ISSUER NAME	
countryName	GB
stateOrProvinceName	Greater Manchester
localityName	Salford
organizationName	Comodo CA Limited
commonName	AAA Certificate Services
(2)SUBJECT NAME	
countryName	GB
stateOrProvinceName	Greater Manchester

localityName	Salford
organizationName	COMODO CA Limited
commonName	COMODO RSA Certification Authority
(2)Valid From	Jan 1 00:00:00 2004 GMT
(2)Valid Till	Dec 31 23:59:59 2028 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(4096 bit)
(2)	RSA Public-Key: (4096 bit)
(2)	Modulus:
(2)	00:91:e8:54:92:d2:0a:56:b1:ac:0d:24:dd:c5:cf:
(2)	44:67:74:99:2b:37:a3:7d:23:70:00:71:bc:53:df:
(2)	c4:fa:2a:12:8f:4b:7f:10:56:bd:9f:70:72:b7:61:
(2)	7f:c9:4b:0f:17:a7:3d:e3:b0:04:61:ee:ff:11:97:
(2)	c7:f4:86:3e:0a:fa:3e:5c:f9:93:e6:34:7a:d9:14:
(2)	6b:e7:9c:b3:85:a0:82:7a:76:af:71:90:d7:ec:fd:
(2)	0d:fa:9c:6c:fa:df:b0:82:f4:14:7e:f9:be:c4:a6:
(2)	2f:4f:7f:99:7f:b5:fc:67:43:72:bd:0c:00:d6:89:
(2)	eb:6b:2c:d3:ed:8f:98:1c:14:ab:7e:e5:e3:6e:fc:
(2)	d8:a8:e4:92:24:da:43:6b:62:b8:55:fd:ea:c1:bc:
(2)	6c:b6:8b:f3:0e:8d:9a:e4:9b:6c:69:99:f8:78:48:
(2)	30:45:d5:ad:e1:0d:3c:45:60:fc:32:96:51:27:bc:
(2)	67:c3:ca:2e:b6:6b:ea:46:c7:c7:20:a0:b1:1f:65:
(2)	de:48:08:ba:a4:4e:a9:f2:83:46:37:84:eb:e8:cc:
(2)	81:48:43:67:4e:72:2a:9b:5c:bd:4c:1b:28:8a:5c:
(2)	22:7b:b4:ab:98:d9:ee:e0:51:83:c3:09:46:4e:6d:
(2)	3e:99:fa:95:17:da:7c:33:57:41:3c:8d:51:ed:0b:
(2)	b6:5c:af:2c:63:1a:df:57:c8:3f:bc:e9:5d:c4:9b:
(2)	af:45:99:e2:a3:5a:24:b4:ba:a9:56:3d:cf:6f:aa:
(2)	ff:49:58:be:f0:a8:ff:f4:b8:ad:e9:37:fb:ba:b8:
(2)	f4:0b:3a:f9:e8:43:42:1e:89:d8:84:cb:13:f1:d9:
(2)	bb:e1:89:60:b8:8c:28:56:ac:14:1d:9c:0a:e7:71:
(2)	eb:cf:0e:dd:3d:a9:96:a1:48:bd:3c:f7:af:b5:0d:
(2)	22:4c:c0:11:81:ec:56:3b:f6:d3:a2:e2:5b:b7:b2:
(2)	04:22:52:95:80:93:69:e8:8e:4c:65:f1:91:03:2d:
(2)	70:74:02:ea:8b:67:15:29:69:52:02:bb:d7:df:50:
(2)	6a:55:46:bf:a0:a3:28:61:7f:70:d0:c3:a2:aa:2c:
(2)	21:aa:47:ce:28:9c:06:45:76:bf:82:18:27:b4:d5:
(2)	ae:b4:cb:50:e6:6b:f4:4c:86:71:30:e9:a6:df:16:
(2)	86:e0:d8:ff:40:dd:fb:d0:42:88:7f:a3:33:3a:2e:
(2)	5c:1e:41:11:81:63:ce:18:71:6b:2b:ec:a6:8a:b7:
(2)	31:5c:3a:6a:47:e0:c3:79:59:d6:20:1a:af:f2:6a:
(2)	98:aa:72:bc:57:4a:d2:4b:9d:bb:10:fc:b0:4c:41:
(2)	e5:ed:1d:3d:5e:28:9d:9c:cc:bf:b3:51:da:a7:47:
(2)	e5:84:53
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Authority Key Identifier	keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4
(2)X509v3 Subject Key Identifier	BB:AF:7E:02:3D:FA:A6:F1:3C:84:8E:AD:EE:38:98:EC:D9:32:32:D4
(2)X509v3 Key Usage	critical
(2)	Digital Signature, Certificate Sign, CRL Sign
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(2)X509v3 CRL Distribution Points	
(2)	Full Name:
(2)	URI:http://crl.comodoca.com/AAACertificateServices.crl

(2)Authority Information Access	OCSP - URI:http://ocsp.comodoca.com
(2)Signature	(256 octets)
(2)	7f:f2:56:35:b0:6d:95:4a:4e:74:af:3a:e2:6f:01:8b
(2)	87:d3:32:97:ed:f8:40:d2:77:53:11:d7:c7:16:2e:c6
(2)	9d:e6:48:56:be:80:a9:f8:bc:78:d2:c8:63:17:ae:8c
(2)	ed:16:31:fa:1f:18:c9:0e:c7:ee:48:79:9f:c7:c9:b9
(2)	bc:cc:88:15:e3:68:61:d1:9f:1d:4b:61:81:d7:56:04
(2)	63:c2:08:69:26:f0:f0:e5:2f:df:c0:0a:2b:a9:05:f4
(2)	02:5a:6a:89:d7:b4:84:42:95:e3:eb:f7:76:20:5e:35
(2)	d9:c0:cd:25:08:13:4c:71:38:8e:87:b0:33:84:91:99
(2)	1e:91:f1:ac:9e:3f:a7:1d:60:81:2c:36:41:54:a0:e2
(2)	46:06:0b:ac:1b:c7:99:36:8c:5e:a1:0b:a4:9e:d9:42
(2)	46:24:c5:c5:5b:81:ae:ad:a0:a0:dc:9f:36:b8:8d:c2
(2)	1d:15:fa:88:ad:81:10:39:1f:44:f0:2b:9f:dd:10:54
(2)	0c:07:34:b1:36:d1:14:fd:07:02:3d:ff:72:55:ab:27
(2)	d6:2c:81:41:71:29:8d:41:f4:50:57:1a:7e:65:60:af
(2)	cb:c5:28:76:98:ae:b3:a8:53:76:8b:e6:21:52:6b:ea
(2)	21:d0:84:0e:49:4e:88:53:da:92:2e:e7:1d:08:66:d7

SSH Banner — port 22 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	38050
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-10-30 16:31:24.0

THREAT:

Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

QID Detection Logic:

The QID checks for SSH in the banner of the response.

IMPACT:

NA

SOLUTION:

NA

RESULT:

SSH-2.0-OpenSSH_5.3

Appendices

Hosts Scanned

162.144.102.68

Hosts Not Alive

96.78.85.97, 35.174.132.21

Option Profile

Scan	
Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing	Standard
Vulnerability Detection	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off

Advanced	
Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Payment Card Industry (PCI) Status

An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards. A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host.

An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards. A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host.

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information,

			intruders can easily exploit known vulnerabilities specific to software versions.
	3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilites at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
LOW	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
MED	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity		Level	Description
	1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
	2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
	3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.