tenable® Nessus

My Basic Network Scan

Vulnerabilities by Host

Vulnerabilities by Host

162.241.216.11

0	6	23	2	231
CRITICAL	HIGH	MEDIUM	LOW	INFO
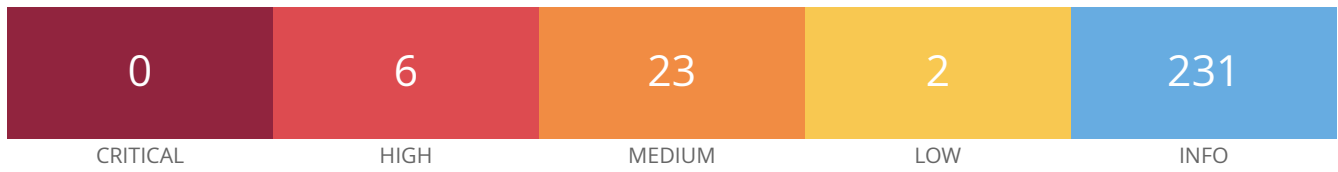
Scan Information

Start time: Sat Jul 26 12:12:23 2025
End time: Sat Jul 26 14:13:34 2025

Host Information

DNS Name: box5331.bluehost.com
IP: 162.241.216.11
OS: Linux Kernel 2.6

Vulnerabilities

35450 - DNS Server Spoofed Request Amplification DDoS

Synopsis

The remote DNS server could be used in a distributed denial of service attack.

Description

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

See Also

https://isc.sans.edu/diary/DNS+queries+for+/5713

Solution

Restrict access to your DNS server from public network or reconfigure it to reject such queries.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

VPR Score

3.6

EPSS Score

0.2875

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE   CVE-2006-0987

Plugin Information

Published: 2009/01/22, Modified: 2023/10/27

Plugin Output

udp/53/dns

```
The DNS query was 17 bytes long, the answer is 95 bytes long.
```

41028 - SNMP Agent Default Community Name (public)

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port, or change the default community string.

Risk Factor

High

VPR Score

5.2

EPSS Score

0.9233

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID   2112
CVE   CVE-1999-0517

Plugin Information

Published: 2002/11/25, Modified: 2022/06/01

Plugin Output

udp/161/snmp

```
The remote SNMP server replies to the following default community
string :

public
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?df5555f5

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

VPR Score

6.1

EPSS Score

0.3833

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE   CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2025/02/12

Plugin Output

tcp/2078/www

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                        Code          KEX        Auth    Encryption              MAC
    --------------------        ----------    ---        ----    --------------------    ---
    DES-CBC3-SHA                0x00, 0x0A    RSA        RSA     3DES-CBC(168)
  SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?df5555f5

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

VPR Score

6.1

EPSS Score

0.3833

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE   CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2025/02/12

Plugin Output

tcp/2083/www

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code          KEX          Auth      Encryption             MAC
    ----------------------        ----------    ---          ----      --------------------   ---
    DES-CBC3-SHA                  0x00, 0x0A    RSA          RSA       3DES-CBC(168)
  SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?df5555f5

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

VPR Score

6.1

EPSS Score

0.3833

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE   CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2025/02/12

Plugin Output

tcp/2087/www

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code           KEX         Auth    Encryption               MAC
    ---------------------         ----------     ---         ----    --------------------     ---
    DES-CBC3-SHA                  0x00, 0x0A     RSA         RSA     3DES-CBC(168)
  SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?df5555f5

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

VPR Score

6.1

EPSS Score

0.3833

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE   CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2025/02/12

Plugin Output

tcp/2096/www

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                      Code          KEX       Auth    Encryption              MAC
    ----------------------    ----------    ---       ----    --------------------    ---
    DES-CBC3-SHA              0x00, 0x0A    RSA       RSA     3DES-CBC(168)
  SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

12217 - DNS Server Cache Snooping Remote Information Disclosure

Synopsis

The remote DNS server is vulnerable to cache snooping attacks.

Description

The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

See Also

http://cs.unc.edu/~fabian/course_papers/cache_snooping.pdf

Solution

Contact the vendor of the DNS software for a fix.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2004/04/27, Modified: 2020/04/07

Plugin Output

udp/53/dns

```
Nessus sent a non-recursive query for example.edu
and received 1 answer :

162.241.216.11
```

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/443/www

```
HTTP/1.1 404 Not Found
Date: Sat, 26 Jul 2025 06:50:34 GMT
Server: Apache
X-Robots-Tag: noindex, nofollow
Content-Length: 315
Connection: close
Content-Type: text/html; charset=iso-8859-1

The remote HTTPS server does not send the HTTP
```

```
"Strict-Transport-Security" header.
```

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/2078/www

```
HTTP/1.1 401 Unauthorized
Date: Sat, 26 Jul 2025 06:50:36 GMT
Server: cPanel
Persistent-Auth: false
Host: box5331.bluehost.com: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

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/2083/www

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Sat, 26 Jul 2025 06:50:41 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=2083; secure
Set-Cookie: cpsession=%3apldJQ0iEafzCl19W%2ca1735f0d9bcfee0094320cb2061bff91; HttpOnly; path=/;
 port=2083; secure
```

```
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2083; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=box5331.bluehost.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
Cache-Control: no-cache, no-store, must-revalidate, private
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37687

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/2087/www

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Sat, 26 Jul 2025 06:50:39 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=2087;
 secure
```

```
Set-Cookie: whostmgrsession=%3amLHeHvFSK0OGrntI%2cf7e5f33ab19a477e1f6df29d6c9f0790; HttpOnly;
 path=/; port=2087; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2087; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=box5331.bluehost.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2087; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;
 secure
Cache-Control: no-cache, no-store, must-revalidate, private
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37669

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/2096/www

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Sat, 26 Jul 2025 06:50:33 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=2096;
 secure
```

```
Set-Cookie: webmailsession=%3as67RJQbPna2Ht4Pq%2cd5603fe1026c33de0f433f2828f1288d; HttpOnly; path=/;
 port=2096; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2096; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=box5331.bluehost.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sun, 26-Jul-2026 06:50:33 GMT; path=/;
 port=2096; secure
Cache-Control: no-cache, no-store, must-revalidate, private
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37699

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/110/pop3

TLSv1 is enabled and the server supports at least one cipher.

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/143/imap

TLSv1 is enabled and the server supports at least one cipher.

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/465/smtp

TLSv1 is enabled and the server supports at least one cipher.

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/993/imap

TLSv1 is enabled and the server supports at least one cipher.

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/995/pop3

TLSv1 is enabled and the server supports at least one cipher.

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/2078/www

TLSv1 is enabled and the server supports at least one cipher.

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/2083/www

TLSv1 is enabled and the server supports at least one cipher.

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/2087/www

TLSv1 is enabled and the server supports at least one cipher.

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/2096/www

TLSv1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/110/pop3

TLSv1.1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/143/imap

TLSv1.1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/993/imap

TLSv1.1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/995/pop3

TLSv1.1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/2078/www

TLSv1.1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/2083/www

TLSv1.1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/2087/www

TLSv1.1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF   CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/2096/www

TLSv1.1 is enabled and the server supports at least one cipher.

54582 - SMTP Service Cleartext Login Permitted

Synopsis

The remote mail server allows cleartext logins.

Description

The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

See Also

https://tools.ietf.org/html/rfc4422

https://tools.ietf.org/html/rfc4954

Solution

Configure the service to support less secure authentication mechanisms only over an encrypted channel.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2011/05/19, Modified: 2021/01/19

Plugin Output

tcp/25/smtp

```
The SMTP server advertises the following SASL methods over an
unencrypted channel on port 25 :

  All supported methods : LOGIN, PLAIN
  Cleartext methods     : LOGIN, PLAIN
```

54582 - SMTP Service Cleartext Login Permitted

Synopsis

The remote mail server allows cleartext logins.

Description

The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

See Also

https://tools.ietf.org/html/rfc4422

https://tools.ietf.org/html/rfc4954

Solution

Configure the service to support less secure authentication mechanisms only over an encrypted channel.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2011/05/19, Modified: 2021/01/19

Plugin Output

tcp/587/smtp

```
The SMTP server advertises the following SASL methods over an
unencrypted channel on port 587 :

  All supported methods : LOGIN, PLAIN
  Cleartext methods     : LOGIN, PLAIN
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
    URL       : http://box5331.bluehost.com/
    Version   : unknown
    Source    : Server: Apache
    backported : 0
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/443/www

```
URL        : https://box5331.bluehost.com/
Version    : unknown
Source     : Server: Apache
backported : 0
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/07/14

Plugin Output

tcp/0

```
 The remote operating system matched the following CPE :

   cpe:/o:linux:linux_kernel -> Linux Kernel

 Following application CPE's matched on the remote system :

   cpe:/a:apache:http_server -> Apache Software Foundation Apache HTTP Server
   cpe:/a:isc:bind:9.11.4-p2-redhat-9.11.4-26.p2.el7_9.9 -> ISC BIND
   cpe:/a:isc:bind:9.11.4:P2 -> ISC BIND
   cpe:/a:mysql:mysql:5.7.23-23 -> MySQL MySQL
   cpe:/a:openbsd:openssh:7.4 -> OpenBSD OpenSSH
   cpe:/a:postgresql:postgresql -> PostgreSQL
```

10028 - DNS Server BIND version Directive Remote Version Detection

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF   IAVT:0001-T-0583

Plugin Information

Published: 1999/10/12, Modified: 2022/10/12

Plugin Output

udp/53/dns

```
Version : 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

https://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53/dns

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

https://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

udp/53/dns

72779 - DNS Server Version Detection

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0937

Plugin Information

Published: 2014/03/03, Modified: 2024/09/24

Plugin Output

tcp/53/dns

```
DNS server answer for "version.bind" (over TCP) :

  9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9
```

35371 - DNS Server hostname.bind Map Hostname Disclosure

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information

Published: 2009/01/15, Modified: 2011/09/14

Plugin Output

udp/53/dns

```
The remote host name is :

box5331.bluehost.com
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 65
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

References

XREF   IAVT:0001-T-0030
XREF   IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 150 allowed.
220-Local time is now 00:44. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
```

42149 - FTP Service AUTH TLS Command Support

Synopsis

The remote directory service supports encrypting traffic.

Description

The remote FTP service supports the use of the 'AUTH TLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc4217

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/15, Modified: 2024/01/16

Plugin Output

tcp/21/ftp

```
The remote FTP service responded to the 'AUTH TLS' command with a
'234' response code, suggesting that it supports that command.  However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

Plugin Output

tcp/443/www

```
HTTP/1.1 404 Not Found
Date: Sat, 26 Jul 2025 06:50:34 GMT
Server: Apache
X-Robots-Tag: noindex, nofollow
Content-Length: 315
Connection: close
Content-Type: text/html; charset=iso-8859-1

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

Plugin Output

tcp/2078/www

```
HTTP/1.1 401 Unauthorized
Date: Sat, 26 Jul 2025 06:50:36 GMT
Server: cPanel
Persistent-Auth: false
Host: box5331.bluehost.com: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

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

Plugin Output

tcp/2083/www

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Sat, 26 Jul 2025 06:50:41 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=2083; secure
Set-Cookie: cpsession=%3apldJQ0iEafzCl19W%2ca1735f0d9bcfee0094320cb2061bff91; HttpOnly; path=/;
 port=2083; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2083; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=box5331.bluehost.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
Cache-Control: no-cache, no-store, must-revalidate, private
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37687

The remote HTTPS server does not send the HTTP
```

```
"Strict-Transport-Security" header.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

Plugin Output

tcp/2087/www

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Sat, 26 Jul 2025 06:50:39 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=2087;
 secure
Set-Cookie: whostmgrsession=%3amLHeHvFSK0OGrntI%2cf7e5f33ab19a477e1f6df29d6c9f0790; HttpOnly;
 path=/; port=2087; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2087; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=box5331.bluehost.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2087; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;
 secure
Cache-Control: no-cache, no-store, must-revalidate, private
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37669
```

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

Plugin Output

tcp/2096/www

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Sat, 26 Jul 2025 06:50:33 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=2096;
 secure
Set-Cookie: webmailsession=%3as67RJQbPna2Ht4Pq%2cd5603fe1026c33de0f433f2828f1288d; HttpOnly; path=/;
 port=2096; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2096; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=box5331.bluehost.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sun, 26-Jul-2026 06:50:33 GMT; path=/;
 port=2096; secure
Cache-Control: no-cache, no-store, must-revalidate, private
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
```

```
Content-Length: 37699

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/2078/www

```
Based on the response to an OPTIONS request :

  - HTTP methods  COPY  DELETE  GET  HEAD  LOCK  MKCOL  MOVE  OPTIONS
     POST  PROPFIND  PROPPATCH  PUT UNLOCK are allowed on :

    /
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF   IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF   IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/443/www

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF   IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/2078/www

```
The remote web server type is :

cPanel
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2015/09/04, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The server supports direct HTTP/2 connections
without encryption.
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2025/03/13

Plugin Output

tcp/0

```
162.241.216.11 resolves as box5331.bluehost.com.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: Yes
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Sat, 26 Jul 2025 07:53:47 GMT
  Server: Apache
  Location: https://box5331.bluehost.com/
  Content-Length: 237
  Keep-Alive: timeout=5, max=75
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://box5331.bluehost.com/">here</a>.</p>
```

```
</body></html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: Yes
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Sat, 26 Jul 2025 07:53:40 GMT
  Server: Apache
  X-Robots-Tag: noindex, nofollow
  Content-Length: 315
  Keep-Alive: timeout=5, max=75
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1

Response Body :
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/2078/www

```
Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : UNLOCK, POST, OPTIONS, PROPFIND, PROPPATCH, DELETE, COPY, LOCK, HEAD, MOVE, PUT,
 MKCOL, GET
Headers :

  Date: Sat, 26 Jul 2025 07:53:57 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: box5331.bluehost.com: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

Response Body :

<html>Authorization Required</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/2083/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Sat, 26 Jul 2025 07:54:24 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=2083;
 secure
  Set-Cookie: cpsession=%3aBEbGtkwThX96xUkM%2cfffd79dabaea27010a0aed050d047249; HttpOnly; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=box5331.bluehost.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Cache-Control: no-cache, no-store, must-revalidate, private
  X-Frame-Options: SAMEORIGIN
```

```
  X-Content-Type-Options: nosniff
  Content-Length: 37687

Response Body :


<!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="data:image/x-
icon;base64,AAABAAEAICAAAAEAIADSAgAAFgAAAIlQTkcNChoKAAAADUlIRFIAAAAgAAAAIAgGAAAAc3p69AAAAplJREFUWIXt1j2IHGUYB/
DfOzdnjIKFkECIVWIKvUFsIkRExa9KJCLaWAgWJx4DilZWgpDDiI0wiViIoGATP1CCEDYHSeCwUBBkgiiKURQJFiLo4d0eOxYzC8nsO9m9XcXC
+8MW+3z+9//l612383xH+iSBpElyTdoda26xsDqp/
h0CVZ3vwKm7tMBngAs7h7eRYebG6hMtMBHbMBX89vfARrpQ5U8cwdFQlIOZCVR5di1+w/wWXT/
EY6EoN5NZCODuKZLDwgSMuBe2fwfX6QZwtpWzpfBBtLC3tF/
ZhxKbBGx0EfsTJS77vwmGjlZrD4mUzUOXZjVjGI65cnTXXXXchB8iupdDUb7QinsQZ7GzZftdQj2JVZ49iC/
w6JjkksIo7OnS9tiA5Vn6GtyK2+
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/2087/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Sat, 26 Jul 2025 07:54:10 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=2087; secure
  Set-Cookie: whostmgrsession=%3aX54ZE8c2t8C6Bv54%2c2f544c131c96f0137e26a782e53e93b8; HttpOnly;
path=/; port=2087; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
port=2087; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=box5331.bluehost.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2087; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;
secure
  Cache-Control: no-cache, no-store, must-revalidate, private
  X-Frame-Options: SAMEORIGIN
```

```
    X-Content-Type-Options: nosniff
    Content-Length: 37669

Response Body :


<!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="data:image/x-
icon;base64,AAABAAEAICAAAAEAIADSAgAAFgAAAIlQTkcNChoKAAAADUlIRFIAAAAgAAAAIAgGAAAAc3p69AAAAplJREFUWIXt1j2IHGUYB/
DfOzdnjIKFkECIVWIKvUFsIkRExa9KJCLaWAgWJx4DilZWgpDDiI0wiViIoGATP1CCEDYHSeCwUBBkgiiKURQJFiLo4d0eOxYzC8nsO9m9XcXC
+8MW+3z+9/l612383xH+iSBpElyTdoda26xsDqp/
h0CVZ3vwKm7tMBngAs7h7eRYebG6hMtMBHbMBX89vfARHprQ5U8cwdFQlIOZCVR5di1+w/wWXT/
EY6EoN5NZCODuKZLDwzgSMCuBe2fwfX6QZwtpWzqfBBtLC3txF/
ZhxKbBGGx0EfsTJS77vwmGj1ZrD4mUzUOXZjVjjGGY65cnTXXchB8iupdDUb7QinsQZ7GzZftdQj2JVZ49iC/w6JjksI7OnS9tia5
  [...]
```

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/2096/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Sat, 26 Jul 2025 07:53:29 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=2096;
 secure
  Set-Cookie: webmailsession=%3aEzZvJFd4f2fwV0cC%2cf65977597b1b9882b218e9be4ecff636; HttpOnly;
 path=/; port=2096; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2096; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=box5331.bluehost.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sun, 26-Jul-2026 07:53:29 GMT; path=/;
 port=2096; secure
```

```
   Cache-Control: no-cache, no-store, must-revalidate, private
   X-Frame-Options: SAMEORIGIN
   X-Content-Type-Options: nosniff
   Content-Length: 37699

Response Body :


<!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="data:image/x-
icon;base64,AAABAAEAICAAAAEAIADSAgAAFgAAAI1QTkcNChoKAAAADUlIRFIAAAAgAAAAIAgGAAAAc3p69AAAAplJREFUWIXt1j2IHGUYB/
DfOzdnjIKFkECIVWIKvUFsIkRExa9KJCLaWAgWJx4DilZWgpDDiI0wiViIoGATP1CCEDYHSeCwUBBkgiiKURQJFiLo4d0eOxYzC8nsO9m9XcXC
+8MW+3z+9/l612383xH+iSBpE1yTdoda26xsDqp/
h0CVZ3vwKm7tMBngAs7h7eRYebG6hMtMBHbMBX89vfARprQ5U8cwdFQlIOZCVR5di1+w/wWXT/
EY6EoN5NZCODuKZLDwzgSMCuBe2fwfX
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

Plugin Output

tcp/143/imap

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS
 AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

Plugin Output

tcp/993/imap

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN
 AUTH=LOGIN] Dovecot ready.
```

42085 - IMAP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote IMAP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc2595

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2021/02/24

Plugin Output

tcp/143/imap

```
Here is the IMAP server's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

---------------------------- snip -----------------------------
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption
```

```
Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
            1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
            CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
            28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
            71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
            C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
            C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
            33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
            32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
            92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
            81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
            CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
            68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 [...]
```

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

References

XREF   IAVT:0001-T-0802

Plugin Information

Published: 2001/08/13, Modified: 2022/10/12

Plugin Output

tcp/3306/mysql

```
  Version  : 5.7.23-23
  Protocol : 10
  Server Status : SERVER_STATUS_AUTOCOMMIT
  Server Capabilities :
    CLIENT_LONG_PASSWORD (new more secure passwords)
    CLIENT_FOUND_ROWS (Found instead of affected rows)
    CLIENT_LONG_FLAG (Get all column flags)
    CLIENT_CONNECT_WITH_DB (One can specify db on connect)
    CLIENT_NO_SCHEMA (Don't allow database.table.column)
    CLIENT_COMPRESS (Can use compression protocol)
    CLIENT_ODBC (ODBC client)
    CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
    CLIENT_IGNORE_SPACE (Ignore spaces before "(")
    CLIENT_PROTOCOL_41 (New 4.1 protocol)
    CLIENT_INTERACTIVE (This is an interactive client)
    CLIENT_SSL (Switch to SSL after handshake)
    CLIENT_SIGPIPE (IGNORE sigpipes)
    CLIENT_TRANSACTIONS (Client knows about transactions)
    CLIENT_RESERVED (Old flag for 4.1 protocol)
    CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/25/smtp

```
Port 25/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/53/dns

```
Port 53/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/110/pop3

```
Port 110/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/143/imap

```
Port 143/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/443/www

```
Port 443/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/465/smtp

```
Port 465/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/587/smtp

```
Port 587/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/993/imap

```
Port 993/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/995/pop3

```
Port 995/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/2000

```
Port 2000/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/2077

```
Port 2077/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/2078/www

```
Port 2078/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/2082

```
Port 2082/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/2083/www

```
Port 2083/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/2086

```
Port 2086/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/2087/www

```
Port 2087/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/2095

```
Port 2095/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/2096/www

```
Port 2096/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/2222

```
Port 2222/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/3306/mysql

```
Port 3306/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/5060

```
Port 5060/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/5432/postgresql

```
Port 5432/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/06/25

Plugin Output

tcp/0

```
 Information about this scan :

 Nessus version : 10.9.1
 Nessus build : 20006
 Plugin feed version : 202507250213
 Scanner edition used : Nessus Home
 Scanner OS : LINUX
 Scanner distribution : ubuntu1604-x86-64
 Scan type : Normal
 Scan name : My Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.43.138
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 353.141 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/7/26 12:12 IST (UTC +05:30)
Scan duration : 6729 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Ubuntu 16.04 Linux Kernel 4.4
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
    P1:B10113:F0x12:W65280:O0204ffff:M1360:
    P2:B10113:F0x12:W64704:O0204ffff0402080affffffff4445414401030307:M1360:
    P3:B00000:F0x00:W0:O0:M0
    P4:191301_7_p=443R

Following fingerprints could not be used to determine OS :
 SSH:!:SSH-2.0-OpenSSH_7.4
HTTP:!:Server: Apache

SMTP:!:220-box5331.bluehost.com ESMTP Exim 4.98.1 #2 Sat, 26 Jul 2025 00:42:53 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
SSLcert:!:i/CN:Sectigo RSA Domain Validation Secure Server CAi/O:Sectigo Limiteds/CN:*.bluehost.com
aca1c146694cd39f63ec7906412f20dc978e212f
i/CN:Sectigo RSA Domain Validation Secure Server CAi/O:Sectigo Limiteds/CN:*.bluehost.com
```

aca1c146694cd39f63ec7906412f20dc978e212f

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP

Not all fingerprints could give a match. If you think that these
signatures would help us improve OS fingerprinting, please submit
them by visiting https://www.tenable.com/research/submitsignatures.

SSH:!:SSH-2.0-OpenSSH_7.4
SinFP:
    P1:B10113:F0x12:W65280:O0204ffff:M1360:
    P2:B10113:F0x12:W64704:O0204ffff0402080affffffff4445414401030307:M1360:
    P3:B00000:F0x00:W0:O0:M0
    P4:191301_7_p=443R
HTTP:!:Server: Apache

SMTP:!:220-box5331.bluehost.com ESMTP Exim 4.98.1 #2 Sat, 26 Jul 2025 00:42:53 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
SSLcert:!:i/CN:Sectigo RSA Domain Validation Secure Server CAi/O:Sectigo Limiteds/CN:*.bluehost.com
aca1c146694cd39f63ec7906412f20dc978e212f
i/CN:Sectigo RSA Domain Validation Secure Server CAi/O:Sectigo Limiteds/CN:*.bluehost.com
aca1c146694cd39f63ec7906412f20dc978e212f



The remote host is running Linux Kernel 2.6
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF   IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
  The following issues were reported :

   - Plugin      : no_local_checks_credentials.nasl
     Plugin ID   : 110723
     Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
     Message     :
  Credentials were not provided for detected SSH service.
```

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

Steps to resolve this issue include :

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF   IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2023/06/20

Plugin Output

tcp/0

```
Port 2087 was detected as being open but is now unresponsive
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/07/23

Plugin Output

tcp/22/ssh

```
   Service : ssh
   Version : 7.4
   Banner  : SSH-2.0-OpenSSH_7.4
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/110/pop3

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/143/imap

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/465/smtp

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/993/imap

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/995/pop3

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/2078/www

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/2083/www

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/2087/www

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/2096/www

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

See Also

https://en.wikipedia.org/wiki/Post_Office_Protocol

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/110/pop3

```
Remote POP server banner :

+OK Dovecot ready.
```

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

See Also

https://en.wikipedia.org/wiki/Post_Office_Protocol

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/995/pop3

```
Remote POP server banner :

+OK Dovecot ready.
```

42087 - POP3 Service STLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote POP3 service supports the use of the 'STLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc2595

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2021/02/24

Plugin Output

tcp/110/pop3

```
Here is the POP3 server's SSL certificate that Nessus was able to
collect after sending a 'STLS' command :

---------------------------- snip -----------------------------
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption
```

```
Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
            1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
            CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
            28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
            71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
            C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
            C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
            33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
            32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
            92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
            81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
            CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
            68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9  [...]
```

26024 - PostgreSQL Server Detection

Synopsis

A database service is listening on the remote host.

Description

The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

See Also

https://www.postgresql.org/

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2007/09/14, Modified: 2023/05/24

Plugin Output

tcp/5432/postgresql

31422 - Reverse NAT/Intercepting Proxy Detection

Synopsis

The remote IP address seems to connect to different hosts via reverse NAT, or an intercepting proxy is in the way.

Description

Reverse NAT is a technology which lets multiple computers offer public services on different ports via the same IP address.

Based on OS fingerprinting results, it seems that different operating systems are listening on different remote ports.

Note that this behavior may also indicate the presence of a intercepting proxy, a load balancer or a traffic shaper.

See Also

https://en.wikipedia.org/wiki/Proxy_server#Intercepting_proxy_server

Solution

Make sure that this setup is authorized by your security policy

Risk Factor

None

Plugin Information

Published: 2008/03/12, Modified: 2022/04/11

Plugin Output

tcp/0

```
+ On the following port(s) :
 - 5060 (3 hops away)
 - 2000 (3 hops away)

The operating system was identified as :

Linux Kernel 2.2
Linux Kernel 2.4
Linux Kernel 2.6

+ On the following port(s) :
 - 110 (14 hops away)
 - 3306 (14 hops away)
 - 80 (14 hops away)
 - 587 (14 hops away)
 - 2095 (14 hops away)
```

```
- 2096 (14 hops away)
- 2087 (14 hops away)
- 5432 (14 hops away)
- 2086 (14 hops away)
- 2082 (14 hops away)
- 21 (14 hops away)
- 143 (14 hops away)
- 2078 (14 hops away)
- 995 (14 hops away)
- 465 (14 hops away)
- 53 (14 hops away)
- 25 (14 hops away)
- 993 (14 hops away)
- 2083 (14 hops away)
- 2077 (14 hops away)

The operating system was identified as :

Linux Kernel 2.6
```

54580 - SMTP Authentication Methods

Synopsis

The remote mail server supports authentication.

Description

The remote SMTP server advertises that it supports authentication.

See Also

https://tools.ietf.org/html/rfc4422

https://tools.ietf.org/html/rfc4954

Solution

Review the list of methods and whether they're available over an encrypted channel.

Risk Factor

None

Plugin Information

Published: 2011/05/19, Modified: 2019/03/05

Plugin Output

tcp/25/smtp

```
The following authentication methods are advertised by the SMTP
server without encryption :
  LOGIN
  PLAIN
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF   IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/25/smtp

```
Remote SMTP server banner :

220-box5331.bluehost.com ESMTP Exim 4.98.1 #2 Sat, 26 Jul 2025 00:42:53 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF   IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/465/smtp

```
Remote SMTP server banner :

220-box5331.bluehost.com ESMTP Exim 4.98.1 #2 Sat, 26 Jul 2025 00:43:39 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF   IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/587/smtp

```
Remote SMTP server banner :

220-box5331.bluehost.com ESMTP Exim 4.98.1 #2 Sat, 26 Jul 2025 00:42:48 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

Plugin Output

tcp/25/smtp

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

---------------------------- snip ----------------------------
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption
```

```
Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
            1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
            CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
            28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
            71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
            C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
            C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
            33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
            32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
            92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
            81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
            CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
            68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F [...]
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

Plugin Output

tcp/587/smtp

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

---------------------------- snip ----------------------------
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption
```

```
Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
            1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
            CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
            28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
            71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
            C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
            C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
            33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
            32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
            92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
            81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
            CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
            68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F [...]
```

35296 - SNMP Protocol Version Detection

Synopsis

This plugin reports the protocol version negotiated with the remote SNMP agent.

Description

By sending an SNMP 'get-next-request', it is possible to determine the protocol version of the remote SNMP agent.

See Also

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2019/11/22

Plugin Output

udp/161/snmp

```
Nessus has negotiated SNMP communications at SNMPv2c.
```

40448 - SNMP Supported Protocols Detection

Synopsis

This plugin reports all the protocol versions successfully negotiated with the remote SNMP agent.

Description

Extend the SNMP settings data already gathered by testing for\ SNMP versions other than the highest negotiated.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/07/31, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
This host supports SNMP version SNMPv2c.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :

  Client to Server: aes256-ctr
  Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha2-256
  hmac-sha2-512

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  rsa-sha2-256
  rsa-sha2-512
  ssh-dss
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
```

```
    aes192-ctr
    aes256-ctr

The server supports the following options for mac_algorithms_server_to_client :

    hmac-ripemd160
    hmac-ripemd160@openssh.com
    hmac-sha2-256
    hmac-sha2-512

The server supports the following options for kex_algorithms :

    diffie-hellman-group-exchange-sha256
    kex-strict-s-v00@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

    none
    zlib@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

    aes128-ctr
    aes192-ctr
    aes256-ctr
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF   IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.4
SSH supported authentication : publickey,password,keyboard-interactive
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/21/ftp

```
This port supports TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/110/pop3

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/143/imap

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/443/www

```
This port supports TLSv1.3/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/465/smtp

```
This port supports TLSv1.0.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/993/imap

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/995/pop3

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/2078/www

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/2083/www

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/2087/www

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/2096/www

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/21/ftp

```
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
```

```
1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9 E0 F5 FB 6E
81 4C 3C 2E 34 67 42 94 E3 53 54 8A 1E 9A A0 06 A8 94 EA 60
C6 35 06 5A 27 0B 37 62 0F 8B 6C 27 DF DD 95 88 86 2C E1 DA
C9 F6 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/110/pop3

```
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
```

```
1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9 E0 F5 FB 6E
81 4C 3C 2E 34 67 42 94 E3 53 54 8A 1E 9A A0 06 A8 94 EA 60
C6 35 06 5A 27 0B 37 62 0F 8B 6C 27 DF DD 95 88 86 2C E1 DA
C9 F6 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/143/imap

```
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
```

```
1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9 E0 F5 FB 6E
81 4C 3C 2E 34 67 42 94 E3 53 54 8A 1E 9A A0 06 A8 94 EA 60
C6 35 06 5A 27 0B 37 62 0F 8B 6C 27 DF DD 95 88 86 2C E1 DA
C9 F6 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
```

```
1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9 E0 F5 FB 6E
81 4C 3C 2E 34 67 42 94 E3 53 54 8A 1E 9A A0 06 A8 94 EA 60
C6 35 06 5A 27 0B 37 62 0F 8B 6C 27 DF DD 95 88 86 2C E1 DA
C9 F6 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/465/smtp

```
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
```

```
1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9 E0 F5 FB 6E
81 4C 3C 2E 34 67 42 94 E3 53 54 8A 1E 9A A0 06 A8 94 EA 60
C6 35 06 5A 27 0B 37 62 0F 8B 6C 27 DF DD 95 88 86 2C E1 DA
C9 F6 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/993/imap

```
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
```

```
1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9 E0 F5 FB 6E
81 4C 3C 2E 34 67 42 94 E3 53 54 8A 1E 9A A0 06 A8 94 EA 60
C6 35 06 5A 27 0B 37 62 0F 8B 6C 27 DF DD 95 88 86 2C E1 DA
C9 F6 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/995/pop3

```
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
```

```
1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9 E0 F5 FB 6E
81 4C 3C 2E 34 67 42 94 E3 53 54 8A 1E 9A A0 06 A8 94 EA 60
C6 35 06 5A 27 0B 37 62 0F 8B 6C 27 DF DD 95 88 86 2C E1 DA
C9 F6 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/2078/www

```
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
```

```
1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9 E0 F5 FB 6E
81 4C 3C 2E 34 67 42 94 E3 53 54 8A 1E 9A A0 06 A8 94 EA 60
C6 35 06 5A 27 0B 37 62 0F 8B 6C 27 DF DD 95 88 86 2C E1 DA
C9 F6 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/2083/www

```
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
```

```
1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9 E0 F5 FB 6E
81 4C 3C 2E 34 67 42 94 E3 53 54 8A 1E 9A A0 06 A8 94 EA 60
C6 35 06 5A 27 0B 37 62 0F 8B 6C 27 DF DD 95 88 86 2C E1 DA
C9 F6 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/2087/www

```
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
```

```
1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9 E0 F5 FB 6E
81 4C 3C 2E 34 67 42 94 E3 53 54 8A 1E 9A A0 06 A8 94 EA 60
C6 35 06 5A 27 0B 37 62 0F 8B 6C 27 DF DD 95 88 86 2C E1 DA
C9 F6 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/2096/www

```
Subject Name:

Common Name: *.bluehost.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 AE 96 24 18 A0 20 37 BE DB 8B 5F 16 D7 E4 DA 8A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 00:00:00 2025 GMT
Not Valid After: Jan 27 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 AE 33 CB 82 ED 37 CF AD 33 0C B5 49 E6 C8 95 47 E9 8E AB
            78 88 D7 6C 16 14 07 FE 2D 44 14 3C FC 86 85 BF 51 AE 5C 3A
            0D D3 4F E2 21 A7 03 EE A3 B9 89 8A AC FA 8E 71 E0 BA 56 31
            BF D6 DB 3F B7 34 34 6F CA 03 87 FC 85 72 B9 18 F0 CE BE 8F
            8B 75 F2 FE 57 40 72 F7 6E 4A 1B D0 45 4F E8 F0 58 D0 0C 33
            97 17 89 C0 EC CC 05 8E A0 68 10 D8 19 D9 F9 1E 97 75 2D 45
            5D 3D 17 7D 4E 21 DB 4F 02 4B CB 1A B0 FC 32 88 79 E3 64 0C
```

```
1A 1C 7B 2A 6E C1 0E 3C 58 D0 81 BE 1B 1F E6 53 05 69 CA 7F
CB EA 7E 98 9F B5 6B 4A EB 35 62 58 D7 01 67 F9 27 92 C0 07
28 E8 41 CA F0 DB AB 71 23 3D 1F 8A 1C 59 0F 0C 7F 96 B3 09
71 B8 1A 8D A4 C3 24 3C 3B F6 03 9A 5D F4 13 21 98 D4 26 86
C1 AA 6C 02 9A AD DF 07 D1 A1 05 BE 1C FA 9E 9E 2D F1 06 7F
C1 B5 9F 80 D3 54 DB CA D4 FD 39 1E 6B 4F D3 68 AB 3B 8D 46
33 BA 50 20 03 02 D4 5F D8 97 33 E0 81 80 47 4A 44 FC 9B 47
32 8A DA D2 4A 8D 3B D8 66 20 E1 9B 54 75 37 1E 18 7F 82 CB
92 47 50 F4 CF 22 59 E3 9C 75 26 F6 6B 87 A7 2E C1 C8 61 78
81 58 C2 98 F9 7E F7 89 8D AD 44 D7 F0 F6 87 EA A2 44 12 AE
CE F8 24 AB 99 50 6E 57 97 37 89 62 BA 19 84 BA 8F A1 EC FE
68 46 4D E9 7B DF 7A 3F C6 76 28 42 B4 03 F8 D9 E0 F5 FB 6E
81 4C 3C 2E 34 67 42 94 E3 53 54 8A 1E 9A A0 06 A8 94 EA 60
C6 35 06 5A 27 0B 37 62 0F 8B 6C 27 DF DD 95 88 86 2C E1 DA
C9 F6 [...]
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

tcp/21/ftp

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3J1YXR1ciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgc
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

tcp/110/pop3

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject            : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From         : Jan 01 00:00:00 2004 GMT
Valid To           : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMG
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjg
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

tcp/143/imap

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject            : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From         : Jan 01 00:00:00 2004 GMT
Valid To           : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMG
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjg
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3J1YXR1ciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMG
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgo
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

tcp/465/smtp

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From           : Jan 01 00:00:00 2004 GMT
Valid To             : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMG
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgo
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

tcp/993/imap

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMG
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjg
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

tcp/995/pop3

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMG
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgc
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMG
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjg
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject            : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From         : Jan 01 00:00:00 2004 GMT
Valid To           : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3J1YXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn51J8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMG
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgo
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From           : Jan 01 00:00:00 2004 GMT
Valid To             : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMG
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgo
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3J1YXR1ciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgo
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/110/pop3

```
  Here is the list of SSL CBC ciphers supported by the remote server :

   High Strength Ciphers (>= 112-bit key)

     Name                        Code           KEX       Auth     Encryption           MAC
     -------------------         ----------     ---       ----     --------------------  ---
     ECDHE-RSA-AES128-SHA        0xC0, 0x13     ECDH      RSA      AES-CBC(128)
  SHA1
     ECDHE-RSA-AES256-SHA        0xC0, 0x14     ECDH      RSA      AES-CBC(256)
  SHA1
     AES128-SHA                  0x00, 0x2F     RSA       RSA      AES-CBC(128)
  SHA1
     AES256-SHA                  0x00, 0x35     RSA       RSA      AES-CBC(256)
  SHA1
     CAMELLIA128-SHA             0x00, 0x41     RSA       RSA      Camellia-CBC(128)
  SHA1
```

```
    CAMELLIA256-SHA            0x00, 0x84      RSA         RSA       Camellia-CBC(256)
SHA1
    IDEA-CBC-SHA               0x00, 0x07      RSA         RSA       IDEA-CBC(128)
SHA1
    SEED-SHA                   0x00, 0x96      RSA         RSA       SEED-CBC(128)
SHA1
    ECDHE-RSA-AES128-SHA256    0xC0, 0x27      ECDH        RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384    0xC0, 0x28      ECDH        RSA       AES-CBC(256)
SHA384
    RSA-AES128-SHA256          0x00, 0x3C      RSA         RSA       AES-CBC(128)
SHA256
    RSA-AES256-SHA256          0x00, 0x3D      RSA         RSA       AES-CBC(256)
SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/143/imap

```
 Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                      Code         KEX      Auth    Encryption            MAC
    --------------------      ----------   ---      ----    --------------------  ---
    ECDHE-RSA-AES128-SHA      0xC0, 0x13   ECDH     RSA     AES-CBC(128)
  SHA1
    ECDHE-RSA-AES256-SHA      0xC0, 0x14   ECDH     RSA     AES-CBC(256)
  SHA1
    AES128-SHA                0x00, 0x2F   RSA      RSA     AES-CBC(128)
  SHA1
    AES256-SHA                0x00, 0x35   RSA      RSA     AES-CBC(256)
  SHA1
    CAMELLIA128-SHA           0x00, 0x41   RSA      RSA     Camellia-CBC(128)
  SHA1
```

```
      CAMELLIA256-SHA               0x00, 0x84      RSA        RSA        Camellia-CBC(256)
   SHA1
      IDEA-CBC-SHA                  0x00, 0x07      RSA        RSA        IDEA-CBC(128)
   SHA1
      SEED-SHA                      0x00, 0x96      RSA        RSA        SEED-CBC(128)
   SHA1
      ECDHE-RSA-AES128-SHA256       0xC0, 0x27      ECDH       RSA        AES-CBC(128)
   SHA256
      ECDHE-RSA-AES256-SHA384       0xC0, 0x28      ECDH       RSA        AES-CBC(256)
   SHA384
      RSA-AES128-SHA256             0x00, 0x3C      RSA        RSA        AES-CBC(128)
   SHA256
      RSA-AES256-SHA256             0x00, 0x3D      RSA        RSA        AES-CBC(256)
   SHA256


The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/465/smtp

```
Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                       Code          KEX       Auth    Encryption           MAC
    --------------------       ----------    ---       ----    --------------------  ---
    DHE-RSA-AES128-SHA         0x00, 0x33    DH        RSA     AES-CBC(128)
  SHA1
    DHE-RSA-AES256-SHA         0x00, 0x39    DH        RSA     AES-CBC(256)
  SHA1
    DHE-RSA-CAMELLIA128-SHA    0x00, 0x45    DH        RSA     Camellia-CBC(128)
  SHA1
    DHE-RSA-CAMELLIA256-SHA    0x00, 0x88    DH        RSA     Camellia-CBC(256)
  SHA1
    ECDHE-RSA-AES128-SHA       0xC0, 0x13    ECDH      RSA     AES-CBC(128)
  SHA1
```

```
     ECDHE-RSA-AES256-SHA          0xC0, 0x14      ECDH         RSA         AES-CBC(256)
SHA1
     AES128-SHA                    0x00, 0x2F      RSA          RSA         AES-CBC(128)
SHA1
     AES256-SHA                    0x00, 0x35      RSA          RSA         AES-CBC(256)
SHA1
     CAMELLIA128-SHA               0x00, 0x41      RSA          RSA         Camellia-CBC(128)
SHA1
     CAMELLIA256-SHA               0x00, 0x84      RSA          RSA         Camellia-CBC(256)
SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/993/imap

```
 Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                        Code         KEX       Auth    Encryption            MAC
    ------------------------    ----------   ---       ----    --------------------  ---
    ECDHE-RSA-AES128-SHA        0xC0, 0x13   ECDH      RSA     AES-CBC(128)
  SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14   ECDH      RSA     AES-CBC(256)
  SHA1
    AES128-SHA                  0x00, 0x2F   RSA       RSA     AES-CBC(128)
  SHA1
    AES256-SHA                  0x00, 0x35   RSA       RSA     AES-CBC(256)
  SHA1
    CAMELLIA128-SHA             0x00, 0x41   RSA       RSA     Camellia-CBC(128)
  SHA1
```

```
    CAMELLIA256-SHA              0x00, 0x84      RSA         RSA         Camellia-CBC(256)
SHA1
    IDEA-CBC-SHA                 0x00, 0x07      RSA         RSA         IDEA-CBC(128)
SHA1
    SEED-SHA                     0x00, 0x96      RSA         RSA         SEED-CBC(128)
SHA1
    ECDHE-RSA-AES128-SHA256      0xC0, 0x27      ECDH        RSA         AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384      0xC0, 0x28      ECDH        RSA         AES-CBC(256)
SHA384
    RSA-AES128-SHA256            0x00, 0x3C      RSA         RSA         AES-CBC(128)
SHA256
    RSA-AES256-SHA256            0x00, 0x3D      RSA         RSA         AES-CBC(256)
SHA256


The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/995/pop3

```
  Here is the list of SSL CBC ciphers supported by the remote server :

    High Strength Ciphers (>= 112-bit key)

      Name                        Code          KEX        Auth    Encryption            MAC
      ---------------------       ----------    ---        ----    --------------------  ---
      ECDHE-RSA-AES128-SHA        0xC0, 0x13    ECDH       RSA     AES-CBC(128)
    SHA1
      ECDHE-RSA-AES256-SHA        0xC0, 0x14    ECDH       RSA     AES-CBC(256)
    SHA1
      AES128-SHA                  0x00, 0x2F    RSA        RSA     AES-CBC(128)
    SHA1
      AES256-SHA                  0x00, 0x35    RSA        RSA     AES-CBC(256)
    SHA1
      CAMELLIA128-SHA             0x00, 0x41    RSA        RSA     Camellia-CBC(128)
    SHA1
```

```
      CAMELLIA256-SHA              0x00, 0x84      RSA       RSA       Camellia-CBC(256)
   SHA1
      IDEA-CBC-SHA                 0x00, 0x07      RSA       RSA       IDEA-CBC(128)
   SHA1
      SEED-SHA                     0x00, 0x96      RSA       RSA       SEED-CBC(128)
   SHA1
      ECDHE-RSA-AES128-SHA256      0xC0, 0x27      ECDH      RSA       AES-CBC(128)
   SHA256
      ECDHE-RSA-AES256-SHA384      0xC0, 0x28      ECDH      RSA       AES-CBC(256)
   SHA384
      RSA-AES128-SHA256            0x00, 0x3C      RSA       RSA       AES-CBC(128)
   SHA256
      RSA-AES256-SHA256            0x00, 0x3D      RSA       RSA       AES-CBC(256)
   SHA256

   The fields above are :

    {Tenable ciphername}
    {Cipher ID code}
    Kex={key exchange}
    Auth={authentication}
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/2078/www

```
 Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                        Code        KEX      Auth    Encryption            MAC
    --------------------        ----------  ---      ----    --------------------  ---
    DES-CBC3-SHA                0x00, 0x0A  RSA      RSA     3DES-CBC(168)
  SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                        Code        KEX      Auth    Encryption            MAC
    --------------------        ----------  ---      ----    --------------------  ---
    DHE-RSA-AES128-SHA          0x00, 0x33  DH       RSA     AES-CBC(128)
  SHA1
    DHE-RSA-AES256-SHA          0x00, 0x39  DH       RSA     AES-CBC(256)
  SHA1
```

```
     DHE-RSA-CAMELLIA128-SHA        0x00, 0x45     DH         RSA        Camellia-CBC(128)
SHA1
     DHE-RSA-CAMELLIA256-SHA        0x00, 0x88     DH         RSA        Camellia-CBC(256)
SHA1
     ECDHE-RSA-AES128-SHA           0xC0, 0x13     ECDH       RSA        AES-CBC(128)
SHA1
     ECDHE-RSA-AES256-SHA           0xC0, 0x14     ECDH       RSA        AES-CBC(256)
SHA1
     AES128-SHA                     0x00, 0x2F     RSA        RSA        AES-CBC(128)
SHA1
     AES256-SHA                     0x00, 0x35     RSA        RSA        AES-CBC(256)
SHA1
     CAMELLIA128-SHA                0x00, 0x41     RSA        RSA        Camellia-CBC(128)
SHA1
     CAMELLIA256-SHA                0x00, 0x84     RSA        RSA        Camellia-CBC(256)
SHA1
     DHE-RSA-AES128-SHA256          0x00, 0x67     DH         RSA        AES-CBC(128)
SHA256
     DHE-RSA-AES256-SHA256          0x00, 0x6B     DH         RSA        AES-CBC(256)
SHA256
     ECDHE-RSA-AES128-SHA256        0xC0, 0x27     ECDH       RSA        AES-CBC(128)
SHA256
     ECDHE-RSA-AES256-SHA384        [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/2083/www

```
  Here is the list of SSL CBC ciphers supported by the remote server :

   Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

     Name                      Code          KEX         Auth      Encryption              MAC
     --------------------      ----------    ---         ----      --------------------    ---
     DES-CBC3-SHA              0x00, 0x0A    RSA         RSA       3DES-CBC(168)
   SHA1

   High Strength Ciphers (>= 112-bit key)

     Name                      Code          KEX         Auth      Encryption              MAC
     --------------------      ----------    ---         ----      --------------------    ---
     DHE-RSA-AES128-SHA        0x00, 0x33    DH          RSA       AES-CBC(128)
   SHA1
     DHE-RSA-AES256-SHA        0x00, 0x39    DH          RSA       AES-CBC(256)
   SHA1
```

```
    DHE-RSA-CAMELLIA128-SHA      0x00, 0x45      DH       RSA       Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA      0x00, 0x88      DH       RSA       Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA         0xC0, 0x13      ECDH     RSA       AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA         0xC0, 0x14      ECDH     RSA       AES-CBC(256)
SHA1
    AES128-SHA                   0x00, 0x2F      RSA      RSA       AES-CBC(128)
SHA1
    AES256-SHA                   0x00, 0x35      RSA      RSA       AES-CBC(256)
SHA1
    CAMELLIA128-SHA              0x00, 0x41      RSA      RSA       Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA              0x00, 0x84      RSA      RSA       Camellia-CBC(256)
SHA1
    DHE-RSA-AES128-SHA256        0x00, 0x67      DH       RSA       AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256        0x00, 0x6B      DH       RSA       AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256      0xC0, 0x27      ECDH     RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384      [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/2087/www

```
  Here is the list of SSL CBC ciphers supported by the remote server :

    Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

      Name                    Code         KEX       Auth    Encryption            MAC
      --------------------    ----------   ---       ----    --------------------  ---
      DES-CBC3-SHA            0x00, 0x0A   RSA       RSA     3DES-CBC(168)
    SHA1

    High Strength Ciphers (>= 112-bit key)

      Name                    Code         KEX       Auth    Encryption            MAC
      --------------------    ----------   ---       ----    --------------------  ---
      DHE-RSA-AES128-SHA      0x00, 0x33   DH        RSA     AES-CBC(128)
    SHA1
      DHE-RSA-AES256-SHA      0x00, 0x39   DH        RSA     AES-CBC(256)
    SHA1
```

```
    DHE-RSA-CAMELLIA128-SHA        0x00, 0x45      DH        RSA        Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA        0x00, 0x88      DH        RSA        Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA           0xC0, 0x13      ECDH      RSA        AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA           0xC0, 0x14      ECDH      RSA        AES-CBC(256)
SHA1
    AES128-SHA                     0x00, 0x2F      RSA       RSA        AES-CBC(128)
SHA1
    AES256-SHA                     0x00, 0x35      RSA       RSA        AES-CBC(256)
SHA1
    CAMELLIA128-SHA                0x00, 0x41      RSA       RSA        Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA                0x00, 0x84      RSA       RSA        Camellia-CBC(256)
SHA1
    DHE-RSA-AES128-SHA256          0x00, 0x67      DH        RSA        AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256          0x00, 0x6B      DH        RSA        AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256        0xC0, 0x27      ECDH      RSA        AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384        [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/2096/www

```
  Here is the list of SSL CBC ciphers supported by the remote server :

    Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

      Name                       Code         KEX       Auth    Encryption            MAC
      --------------------       ----------   ---       ----    --------------------  ---
      DES-CBC3-SHA               0x00, 0x0A   RSA       RSA     3DES-CBC(168)
    SHA1

    High Strength Ciphers (>= 112-bit key)

      Name                       Code         KEX       Auth    Encryption            MAC
      --------------------       ----------   ---       ----    --------------------  ---
      DHE-RSA-AES128-SHA         0x00, 0x33   DH        RSA     AES-CBC(128)
    SHA1
      DHE-RSA-AES256-SHA         0x00, 0x39   DH        RSA     AES-CBC(256)
    SHA1
```

```
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45      DH         RSA        Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88      DH         RSA        Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13      ECDH       RSA        AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14      ECDH       RSA        AES-CBC(256)
SHA1
    AES128-SHA                    0x00, 0x2F      RSA        RSA        AES-CBC(128)
SHA1
    AES256-SHA                    0x00, 0x35      RSA        RSA        AES-CBC(256)
SHA1
    CAMELLIA128-SHA               0x00, 0x41      RSA        RSA        Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA               0x00, 0x84      RSA        RSA        Camellia-CBC(256)
SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67      DH         RSA        AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B      DH         RSA        AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27      ECDH       RSA        AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/110/pop3

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                      Code          KEX       Auth    Encryption            MAC
    ----------------------    ----------    ---       ----    --------------------  ---
    ECDHE-RSA-AES128-SHA256   0xC0, 0x2F    ECDH      RSA     AES-GCM(128)
SHA256
    ECDHE-RSA-AES256-SHA384   0xC0, 0x30    ECDH      RSA     AES-GCM(256)
SHA384
    RSA-AES128-SHA256         0x00, 0x9C    RSA       RSA     AES-GCM(128)
SHA256
    RSA-AES256-SHA384         0x00, 0x9D    RSA       RSA     AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA      0xC0, 0x13    ECDH      RSA     AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA      0xC0, 0x14    ECDH      RSA     AES-CBC(256)
SHA1
    AES128-SHA                0x00, 0x2F    RSA       RSA     AES-CBC(128)
SHA1
```

```
    AES256-SHA                    0x00, 0x35      RSA         RSA         AES-CBC(256)
SHA1
    CAMELLIA128-SHA               0x00, 0x41      RSA         RSA         Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA               0x00, 0x84      RSA         RSA         Camellia-CBC(256)
SHA1
    IDEA-CBC-SHA                  0x00, 0x07      RSA         RSA         IDEA-CBC(128)
SHA1
    SEED-SHA                      0x00, 0x96      RSA         RSA         SEED-CBC(128)
SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27      ECDH        RSA         AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28      ECDH        RSA         AES-CBC(256)
SHA384
    RSA-AES128-SHA256             0x00, 0x3C      RSA         RSA         AES-CBC(128)
SHA256
    RSA-AES256-SHA256             0x00, 0x3D      RSA         RSA         AES-CBC(256)
SHA256


SSL Version : TLSv11
  High [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/143/imap

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                      Code          KEX       Auth     Encryption            MAC
    ----------------------    ----------    ---       ----     --------------------  ---
    ECDHE-RSA-AES128-SHA256   0xC0, 0x2F    ECDH      RSA      AES-GCM(128)
SHA256
    ECDHE-RSA-AES256-SHA384   0xC0, 0x30    ECDH      RSA      AES-GCM(256)
SHA384
    RSA-AES128-SHA256         0x00, 0x9C    RSA       RSA      AES-GCM(128)
SHA256
    RSA-AES256-SHA384         0x00, 0x9D    RSA       RSA      AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA      0xC0, 0x13    ECDH      RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA      0xC0, 0x14    ECDH      RSA      AES-CBC(256)
SHA1
    AES128-SHA                0x00, 0x2F    RSA       RSA      AES-CBC(128)
SHA1
```

AES256-SHA	0x00, 0x35	RSA	RSA	AES-CBC(256) SHA1
CAMELLIA128-SHA	0x00, 0x41	RSA	RSA	Camellia-CBC(128) SHA1
CAMELLIA256-SHA	0x00, 0x84	RSA	RSA	Camellia-CBC(256) SHA1
IDEA-CBC-SHA	0x00, 0x07	RSA	RSA	IDEA-CBC(128) SHA1
SEED-SHA	0x00, 0x96	RSA	RSA	SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256) SHA384
RSA-AES128-SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128) SHA256
RSA-AES256-SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256) SHA256

```
SSL Version : TLSv11
  High [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/443/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code         KEX        Auth     Encryption          MAC
    --------------------          ----------   ---        ----     --------------------  ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01   -          -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02   -          -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03   -          -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code         KEX        Auth     Encryption          MAC
    --------------------          ----------   ---        ----     --------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F   ECDH       RSA      AES-GCM(128)
 SHA256
```

```
    ECDHE-RSA-AES256-SHA384        0xC0, 0x30      ECDH          RSA        AES-GCM(256)
SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8      ECDH          RSA        ChaCha20-Poly1305(256)
SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/465/smtp

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv1
  High Strength Ciphers (>= 112-bit key)

    Name                      Code         KEX     Auth    Encryption            MAC
    ----------------------    ----------   ---     ----    --------------------  ---
    DHE-RSA-AES128-SHA        0x00, 0x33   DH      RSA     AES-CBC(128)
  SHA1
    DHE-RSA-AES256-SHA        0x00, 0x39   DH      RSA     AES-CBC(256)
  SHA1
    DHE-RSA-CAMELLIA128-SHA   0x00, 0x45   DH      RSA     Camellia-CBC(128)
  SHA1
    DHE-RSA-CAMELLIA256-SHA   0x00, 0x88   DH      RSA     Camellia-CBC(256)
  SHA1
    ECDHE-RSA-AES128-SHA      0xC0, 0x13   ECDH    RSA     AES-CBC(128)
  SHA1
    ECDHE-RSA-AES256-SHA      0xC0, 0x14   ECDH    RSA     AES-CBC(256)
  SHA1
    AES128-SHA                0x00, 0x2F   RSA     RSA     AES-CBC(128)
  SHA1
```

```
     AES256-SHA                    0x00, 0x35      RSA        RSA       AES-CBC(256)
  SHA1
     CAMELLIA128-SHA               0x00, 0x41      RSA        RSA       Camellia-CBC(128)
  SHA1
     CAMELLIA256-SHA               0x00, 0x84      RSA        RSA       Camellia-CBC(256)
  SHA1

  The fields above are :

   {Tenable ciphername}
   {Cipher ID code}
   Kex={key exchange}
   Auth={authentication}
   Encrypt={symmetric encryption method}
   MAC={message authentication code}
   {export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/993/imap

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                    Code        KEX     Auth   Encryption           MAC
    --------------------    ----------  ---     ----   --------------------  ---
    ECDHE-RSA-AES128-SHA256  0xC0, 0x2F  ECDH    RSA    AES-GCM(128)
SHA256
    ECDHE-RSA-AES256-SHA384  0xC0, 0x30  ECDH    RSA    AES-GCM(256)
SHA384
    RSA-AES128-SHA256       0x00, 0x9C  RSA     RSA    AES-GCM(128)
SHA256
    RSA-AES256-SHA384       0x00, 0x9D  RSA     RSA    AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA     0xC0, 0x13  ECDH    RSA    AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA     0xC0, 0x14  ECDH    RSA    AES-CBC(256)
SHA1
    AES128-SHA              0x00, 0x2F  RSA     RSA    AES-CBC(128)
SHA1
```

```
    AES256-SHA                      0x00, 0x35    RSA       RSA       AES-CBC(256)
SHA1
    CAMELLIA128-SHA                 0x00, 0x41    RSA       RSA       Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA                 0x00, 0x84    RSA       RSA       Camellia-CBC(256)
SHA1
    IDEA-CBC-SHA                    0x00, 0x07    RSA       RSA       IDEA-CBC(128)
SHA1
    SEED-SHA                        0x00, 0x96    RSA       RSA       SEED-CBC(128)
SHA1
    ECDHE-RSA-AES128-SHA256         0xC0, 0x27    ECDH      RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384         0xC0, 0x28    ECDH      RSA       AES-CBC(256)
SHA384
    RSA-AES128-SHA256               0x00, 0x3C    RSA       RSA       AES-CBC(128)
SHA256
    RSA-AES256-SHA256               0x00, 0x3D    RSA       RSA       AES-CBC(256)
SHA256


SSL Version : TLSv11
  High [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/995/pop3

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                      Code          KEX        Auth     Encryption            MAC
    --------------------      ----------    ---        ----     --------------------  ---
    ECDHE-RSA-AES128-SHA256   0xC0, 0x2F    ECDH       RSA      AES-GCM(128)
  SHA256
    ECDHE-RSA-AES256-SHA384   0xC0, 0x30    ECDH       RSA      AES-GCM(256)
  SHA384
    RSA-AES128-SHA256         0x00, 0x9C    RSA        RSA      AES-GCM(128)
  SHA256
    RSA-AES256-SHA384         0x00, 0x9D    RSA        RSA      AES-GCM(256)
  SHA384
    ECDHE-RSA-AES128-SHA      0xC0, 0x13    ECDH       RSA      AES-CBC(128)
  SHA1
    ECDHE-RSA-AES256-SHA      0xC0, 0x14    ECDH       RSA      AES-CBC(256)
  SHA1
    AES128-SHA                0x00, 0x2F    RSA        RSA      AES-CBC(128)
  SHA1
```

AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)	
CAMELLIA128-SHA SHA1	0x00, 0x41	RSA	RSA	Camellia-CBC(128)	
CAMELLIA256-SHA SHA1	0x00, 0x84	RSA	RSA	Camellia-CBC(256)	
IDEA-CBC-SHA SHA1	0x00, 0x07	RSA	RSA	IDEA-CBC(128)	
SEED-SHA SHA1	0x00, 0x96	RSA	RSA	SEED-CBC(128)	
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)	
RSA-AES128-SHA256 SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)	
RSA-AES256-SHA256 SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)	

```
SSL Version : TLSv11
  High [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/2078/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                     Code         KEX      Auth    Encryption           MAC
    ---------------------    ----------   ---      ----    --------------------  ---
    DES-CBC3-SHA             0x00, 0x0A   RSA      RSA     3DES-CBC(168)
  SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                     Code         KEX      Auth    Encryption           MAC
    ---------------------    ----------   ---      ----    --------------------  ---
    DHE-RSA-AES128-SHA256    0x00, 0x9E   DH       RSA     AES-GCM(128)
  SHA256
    DHE-RSA-AES256-SHA384    0x00, 0x9F   DH       RSA     AES-GCM(256)
  SHA384
    ECDHE-RSA-AES128-SHA256  0xC0, 0x2F   ECDH     RSA     AES-GCM(128)
  SHA256
    ECDHE-RSA-AES256-SHA384  0xC0, 0x30   ECDH     RSA     AES-GCM(256)
  SHA384
```

```
    RSA-AES128-SHA256          0x00, 0x9C     RSA          RSA          AES-GCM(128)
SHA256
    RSA-AES256-SHA384          0x00, 0x9D     RSA          RSA          AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA         0x00, 0x33     DH           RSA          AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA         0x00, 0x39     DH           RSA          AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA    0x00, 0x45     DH           RSA          Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA    0x00, 0x88     DH           RSA          Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA       0xC0, 0x13     ECDH         RSA          AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA       0xC0, 0x14     ECDH         RSA          AES-CBC(256)
SHA1
    AES128-SHA                 0x00, 0x2F     RSA          RSA          [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/2083/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                     Code         KEX       Auth    Encryption           MAC
    --------------------     ----------   ---       ----    --------------------  ---
    DES-CBC3-SHA             0x00, 0x0A   RSA       RSA     3DES-CBC(168)
  SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                     Code         KEX       Auth    Encryption           MAC
    --------------------     ----------   ---       ----    --------------------  ---
    DHE-RSA-AES128-SHA256    0x00, 0x9E   DH        RSA     AES-GCM(128)
  SHA256
    DHE-RSA-AES256-SHA384    0x00, 0x9F   DH        RSA     AES-GCM(256)
  SHA384
    ECDHE-RSA-AES128-SHA256  0xC0, 0x2F   ECDH      RSA     AES-GCM(128)
  SHA256
    ECDHE-RSA-AES256-SHA384  0xC0, 0x30   ECDH      RSA     AES-GCM(256)
  SHA384
```

```
    RSA-AES128-SHA256          0x00, 0x9C      RSA         RSA         AES-GCM(128)
SHA256
    RSA-AES256-SHA384          0x00, 0x9D      RSA         RSA         AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA         0x00, 0x33      DH          RSA         AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA         0x00, 0x39      DH          RSA         AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA    0x00, 0x45      DH          RSA         Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA    0x00, 0x88      DH          RSA         Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA       0xC0, 0x13      ECDH        RSA         AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA       0xC0, 0x14      ECDH        RSA         AES-CBC(256)
SHA1
    AES128-SHA                 0x00, 0x2F      RSA         RSA         [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/2087/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                      Code          KEX        Auth      Encryption           MAC
    --------------------      ----------    ---        ----      --------------------  ---
    DES-CBC3-SHA              0x00, 0x0A    RSA        RSA       3DES-CBC(168)
  SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                      Code          KEX        Auth      Encryption           MAC
    --------------------      ----------    ---        ----      --------------------  ---
    DHE-RSA-AES128-SHA256     0x00, 0x9E    DH         RSA       AES-GCM(128)
  SHA256
    DHE-RSA-AES256-SHA384     0x00, 0x9F    DH         RSA       AES-GCM(256)
  SHA384
    ECDHE-RSA-AES128-SHA256   0xC0, 0x2F    ECDH       RSA       AES-GCM(128)
  SHA256
    ECDHE-RSA-AES256-SHA384   0xC0, 0x30    ECDH       RSA       AES-GCM(256)
  SHA384
```

```
    RSA-AES128-SHA256          0x00, 0x9C    RSA      RSA      AES-GCM(128)
SHA256
    RSA-AES256-SHA384          0x00, 0x9D    RSA      RSA      AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA         0x00, 0x33    DH       RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA         0x00, 0x39    DH       RSA      AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA    0x00, 0x45    DH       RSA      Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA    0x00, 0x88    DH       RSA      Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA       0xC0, 0x13    ECDH     RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA       0xC0, 0x14    ECDH     RSA      AES-CBC(256)
SHA1
    AES128-SHA                 0x00, 0x2F    RSA      RSA      [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/2096/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                      Code          KEX        Auth    Encryption            MAC
    ---------------------     ----------    ---        ----    --------------------  ---
    DES-CBC3-SHA              0x00, 0x0A    RSA        RSA     3DES-CBC(168)
  SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                      Code          KEX        Auth    Encryption            MAC
    ---------------------     ----------    ---        ----    --------------------  ---
    DHE-RSA-AES128-SHA256     0x00, 0x9E    DH         RSA     AES-GCM(128)
  SHA256
    DHE-RSA-AES256-SHA384     0x00, 0x9F    DH         RSA     AES-GCM(256)
  SHA384
    ECDHE-RSA-AES128-SHA256   0xC0, 0x2F    ECDH       RSA     AES-GCM(128)
  SHA256
    ECDHE-RSA-AES256-SHA384   0xC0, 0x30    ECDH       RSA     AES-GCM(256)
  SHA384
```

```
    RSA-AES128-SHA256           0x00, 0x9C      RSA         RSA         AES-GCM(128)
SHA256
    RSA-AES256-SHA384           0x00, 0x9D      RSA         RSA         AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA          0x00, 0x33      DH          RSA         AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA          0x00, 0x39      DH          RSA         AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA     0x00, 0x45      DH          RSA         Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA     0x00, 0x88      DH          RSA         Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA        0xC0, 0x13      ECDH        RSA         AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14      ECDH        RSA         AES-CBC(256)
SHA1
    AES128-SHA                  0x00, 0x2F      RSA         RSA         [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/110/pop3

```
  Here is the list of SSL PFS ciphers supported by the remote server :

   High Strength Ciphers (>= 112-bit key)

     Name                        Code          KEX       Auth    Encryption            MAC
     --------------------        ----------    ---       ----    --------------------  ---
     ECDHE-RSA-AES128-SHA256     0xC0, 0x2F    ECDH      RSA     AES-GCM(128)
  SHA256
     ECDHE-RSA-AES256-SHA384     0xC0, 0x30    ECDH      RSA     AES-GCM(256)
  SHA384
     ECDHE-RSA-AES128-SHA        0xC0, 0x13    ECDH      RSA     AES-CBC(128)
  SHA1
     ECDHE-RSA-AES256-SHA        0xC0, 0x14    ECDH      RSA     AES-CBC(256)
  SHA1
     ECDHE-RSA-AES128-SHA256     0xC0, 0x27    ECDH      RSA     AES-CBC(128)
  SHA256
```

```
    ECDHE-RSA-AES256-SHA384        0xC0, 0x28       ECDH         RSA        AES-CBC(256)
  SHA384

The fields above are :

   {Tenable ciphername}
   {Cipher ID code}
   Kex={key exchange}
   Auth={authentication}
   Encrypt={symmetric encryption method}
   MAC={message authentication code}
   {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/143/imap

```
  Here is the list of SSL PFS ciphers supported by the remote server :

   High Strength Ciphers (>= 112-bit key)

     Name                         Code         KEX       Auth    Encryption            MAC
     --------------------         ----------   ---       ----    --------------------  ---
     ECDHE-RSA-AES128-SHA256      0xC0, 0x2F   ECDH      RSA     AES-GCM(128)
  SHA256
     ECDHE-RSA-AES256-SHA384      0xC0, 0x30   ECDH      RSA     AES-GCM(256)
  SHA384
     ECDHE-RSA-AES128-SHA         0xC0, 0x13   ECDH      RSA     AES-CBC(128)
  SHA1
     ECDHE-RSA-AES256-SHA         0xC0, 0x14   ECDH      RSA     AES-CBC(256)
  SHA1
     ECDHE-RSA-AES128-SHA256      0xC0, 0x27   ECDH      RSA     AES-CBC(128)
  SHA256
```

```
     ECDHE-RSA-AES256-SHA384        0xC0, 0x28       ECDH        RSA       AES-CBC(256)
  SHA384
```

The fields above are :

```
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/443/www

```
  Here is the list of SSL PFS ciphers supported by the remote server :

    High Strength Ciphers (>= 112-bit key)

      Name                        Code          KEX        Auth    Encryption              MAC
      --------------------        ----------    ---        ----    --------------------    ---
      ECDHE-RSA-AES128-SHA256     0xC0, 0x2F    ECDH       RSA     AES-GCM(128)
  SHA256
      ECDHE-RSA-AES256-SHA384     0xC0, 0x30    ECDH       RSA     AES-GCM(256)
  SHA384
      ECDHE-RSA-CHACHA20-POLY1305 0xCC, 0xA8    ECDH       RSA     ChaCha20-Poly1305(256)
  SHA256

  The fields above are :

    {Tenable ciphername}
    {Cipher ID code}
```

```
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/465/smtp

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                       Code          KEX      Auth    Encryption            MAC
    --------------------       ----------    ---      ----    --------------------  ---
    DHE-RSA-AES128-SHA         0x00, 0x33    DH       RSA     AES-CBC(128)
  SHA1
    DHE-RSA-AES256-SHA         0x00, 0x39    DH       RSA     AES-CBC(256)
  SHA1
    DHE-RSA-CAMELLIA128-SHA    0x00, 0x45    DH       RSA     Camellia-CBC(128)
  SHA1
    DHE-RSA-CAMELLIA256-SHA    0x00, 0x88    DH       RSA     Camellia-CBC(256)
  SHA1
    ECDHE-RSA-AES128-SHA       0xC0, 0x13    ECDH     RSA     AES-CBC(128)
  SHA1
```

```
    ECDHE-RSA-AES256-SHA          0xC0, 0x14      ECDH        RSA       AES-CBC(256)
  SHA1


The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/993/imap

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                        Code        KEX      Auth    Encryption            MAC
    --------------------        ----------  ---      ----    --------------------  ---
    ECDHE-RSA-AES128-SHA256     0xC0, 0x2F  ECDH     RSA     AES-GCM(128)
SHA256
    ECDHE-RSA-AES256-SHA384     0xC0, 0x30  ECDH     RSA     AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA        0xC0, 0x13  ECDH     RSA     AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14  ECDH     RSA     AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA256     0xC0, 0x27  ECDH     RSA     AES-CBC(128)
  SHA256
```

```
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28      ECDH          RSA       AES-CBC(256)
  SHA384


The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/995/pop3

```
  Here is the list of SSL PFS ciphers supported by the remote server :

   High Strength Ciphers (>= 112-bit key)

     Name                        Code          KEX       Auth    Encryption            MAC
     --------------------        ----------    ---       ----    --------------------  ---
     ECDHE-RSA-AES128-SHA256     0xC0, 0x2F    ECDH      RSA     AES-GCM(128)
  SHA256
     ECDHE-RSA-AES256-SHA384     0xC0, 0x30    ECDH      RSA     AES-GCM(256)
  SHA384
     ECDHE-RSA-AES128-SHA        0xC0, 0x13    ECDH      RSA     AES-CBC(128)
  SHA1
     ECDHE-RSA-AES256-SHA        0xC0, 0x14    ECDH      RSA     AES-CBC(256)
  SHA1
     ECDHE-RSA-AES128-SHA256     0xC0, 0x27    ECDH      RSA     AES-CBC(128)
  SHA256
```

```
     ECDHE-RSA-AES256-SHA384        0xC0, 0x28        ECDH          RSA        AES-CBC(256)
  SHA384


The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/2078/www

```
 Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code          KEX        Auth    Encryption            MAC
    --------------------          ----------    ---        ----    --------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E    DH         RSA     AES-GCM(128)
  SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F    DH         RSA     AES-GCM(256)
  SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F    ECDH       RSA     AES-GCM(128)
  SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30    ECDH       RSA     AES-GCM(256)
  SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33    DH         RSA     AES-CBC(128)
  SHA1
```

```
    DHE-RSA-AES256-SHA            0x00, 0x39      DH        RSA       AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45      DH        RSA       Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88      DH        RSA       Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13      ECDH      RSA       AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14      ECDH      RSA       AES-CBC(256)
SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67      DH        RSA       AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B      DH        RSA       AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27      ECDH      RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28      ECDH      RSA       AES-CBC(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/2083/www

```
  Here is the list of SSL PFS ciphers supported by the remote server :

   High Strength Ciphers (>= 112-bit key)

    Name                        Code         KEX       Auth    Encryption             MAC
    --------------------        ----------   ---       ----    --------------------   ---
    DHE-RSA-AES128-SHA256       0x00, 0x9E   DH        RSA     AES-GCM(128)
  SHA256
    DHE-RSA-AES256-SHA384       0x00, 0x9F   DH        RSA     AES-GCM(256)
  SHA384
    ECDHE-RSA-AES128-SHA256     0xC0, 0x2F   ECDH      RSA     AES-GCM(128)
  SHA256
    ECDHE-RSA-AES256-SHA384     0xC0, 0x30   ECDH      RSA     AES-GCM(256)
  SHA384
    DHE-RSA-AES128-SHA          0x00, 0x33   DH        RSA     AES-CBC(128)
  SHA1
```

```
    DHE-RSA-AES256-SHA          0x00, 0x39    DH      RSA    AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA      0x00, 0x45    DH      RSA    Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA      0x00, 0x88    DH      RSA    Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA         0xC0, 0x13    ECDH    RSA    AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA         0xC0, 0x14    ECDH    RSA    AES-CBC(256)
SHA1
    DHE-RSA-AES128-SHA256        0x00, 0x67    DH      RSA    AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256        0x00, 0x6B    DH      RSA    AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256      0xC0, 0x27    ECDH    RSA    AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384      0xC0, 0x28    ECDH    RSA    AES-CBC(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/2087/www

```
 Here is the list of SSL PFS ciphers supported by the remote server :

   High Strength Ciphers (>= 112-bit key)

     Name                        Code          KEX        Auth     Encryption            MAC
     --------------------        ----------    ---        ----     --------------------  ---
     DHE-RSA-AES128-SHA256       0x00, 0x9E    DH         RSA      AES-GCM(128)
   SHA256
     DHE-RSA-AES256-SHA384       0x00, 0x9F    DH         RSA      AES-GCM(256)
   SHA384
     ECDHE-RSA-AES128-SHA256     0xC0, 0x2F    ECDH       RSA      AES-GCM(128)
   SHA256
     ECDHE-RSA-AES256-SHA384     0xC0, 0x30    ECDH       RSA      AES-GCM(256)
   SHA384
     DHE-RSA-AES128-SHA          0x00, 0x33    DH         RSA      AES-CBC(128)
   SHA1
```

```
    DHE-RSA-AES256-SHA            0x00, 0x39      DH        RSA       AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45      DH        RSA       Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88      DH        RSA       Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13      ECDH      RSA       AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14      ECDH      RSA       AES-CBC(256)
SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67      DH        RSA       AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B      DH        RSA       AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27      ECDH      RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28      ECDH      RSA       AES-CBC(256)
SHA384


The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/2096/www

```
 Here is the list of SSL PFS ciphers supported by the remote server :

   High Strength Ciphers (>= 112-bit key)

     Name                        Code         KEX       Auth     Encryption             MAC
     --------------------        ----------   ---       ----     --------------------   ---
     DHE-RSA-AES128-SHA256       0x00, 0x9E   DH        RSA      AES-GCM(128)
  SHA256
     DHE-RSA-AES256-SHA384       0x00, 0x9F   DH        RSA      AES-GCM(256)
  SHA384
     ECDHE-RSA-AES128-SHA256     0xC0, 0x2F   ECDH      RSA      AES-GCM(128)
  SHA256
     ECDHE-RSA-AES256-SHA384     0xC0, 0x30   ECDH      RSA      AES-GCM(256)
  SHA384
     DHE-RSA-AES128-SHA          0x00, 0x33   DH        RSA      AES-CBC(128)
  SHA1
```

```
    DHE-RSA-AES256-SHA           0x00, 0x39      DH        RSA      AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA      0x00, 0x45      DH        RSA      Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA      0x00, 0x88      DH        RSA      Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA         0xC0, 0x13      ECDH      RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA         0xC0, 0x14      ECDH      RSA      AES-CBC(256)
SHA1
    DHE-RSA-AES128-SHA256        0x00, 0x67      DH        RSA      AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256        0x00, 0x6B      DH        RSA      AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256      0xC0, 0x27      ECDH      RSA      AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384      0xC0, 0x28      ECDH      RSA      AES-CBC(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/21/ftp

```
 The following root Certification Authority certificate was found :

 |-Subject            : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
  Services
 |-Issuer             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
  Services
 |-Valid From         : Jan 01 00:00:00 2004 GMT
 |-Valid To           : Dec 31 23:59:59 2028 GMT
 |-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/110/pop3

```
  The following root Certification Authority certificate was found :

 |-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
  Services
 |-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
  Services
 |-Valid From          : Jan 01 00:00:00 2004 GMT
 |-Valid To            : Dec 31 23:59:59 2028 GMT
 |-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/143/imap

```
The following root Certification Authority certificate was found :

|-Subject            : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From         : Jan 01 00:00:00 2004 GMT
|-Valid To           : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/465/smtp

```
 The following root Certification Authority certificate was found :

 |-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
  Services
 |-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
  Services
 |-Valid From          : Jan 01 00:00:00 2004 GMT
 |-Valid To            : Dec 31 23:59:59 2028 GMT
 |-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/993/imap

```
The following root Certification Authority certificate was found :

|-Subject            : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From         : Jan 01 00:00:00 2004 GMT
|-Valid To           : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/995/pop3

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/2078/www

```
 The following root Certification Authority certificate was found :

 |-Subject              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
  Services
 |-Issuer               : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
  Services
 |-Valid From           : Jan 01 00:00:00 2004 GMT
 |-Valid To             : Dec 31 23:59:59 2028 GMT
 |-Signature Algorithm  : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/2083/www

```
  The following root Certification Authority certificate was found :

 |-Subject            : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
  Services
 |-Issuer             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
  Services
 |-Valid From         : Jan 01 00:00:00 2004 GMT
 |-Valid To           : Dec 31 23:59:59 2028 GMT
 |-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/2087/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/2096/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256

- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384

- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384

- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305

- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/110/pop3

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RSA-AES128-SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)	SHA256
RSA-AES256-SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	SHA384
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	SHA1
ECDHE-RSA-AES256-SHA	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	SHA1
AES128-SHA	0x00, 0x2F	RSA	RSA	AES-CBC(128)	SHA1
AES256-SHA	0x00, 0x35	RSA	RSA	AES-CBC(256)	SHA1
CAMELLIA128-SHA	0x00, 0x41	RSA	RSA	Camellia-CBC(128)	SHA1
CAMELLIA256-SHA	0x00, 0x84	RSA	RSA	Camellia-CBC(256)	SHA1
IDEA-CBC-SHA	0x00, 0x07	RSA	RSA	IDEA-CBC(128)	SHA1
SEED-SHA	0x00, 0x96	RSA	RSA	SEED-CBC(128)	SHA1
ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)	SHA256
ECDHE-RSA-AES256-SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)	SHA384
RSA-AES128-SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)	SHA256
RSA-AES256-SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)	SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256

- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384

- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384

- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305

- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/143/imap

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
below:

  High Strength Ciphers (>= 112-bit key)

    Name   Code   KEX   Auth   Encryption   MAC
    --------------------   ----------   ---   ----   --------------------   ---
    RSA-AES128-SHA256   0x00, 0x9C   RSA   RSA   AES-GCM(128)
SHA256
    RSA-AES256-SHA384   0x00, 0x9D   RSA   RSA   AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA   0xC0, 0x13   ECDH   RSA   AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA   0xC0, 0x14   ECDH   RSA   AES-CBC(256)
SHA1
    AES128-SHA   0x00, 0x2F   RSA   RSA   AES-CBC(128)
SHA1
    AES256-SHA   0x00, 0x35   RSA   RSA   AES-CBC(256)
SHA1
    CAMELLIA128-SHA   0x00, 0x41   RSA   RSA   Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA   0x00, 0x84   RSA   RSA   Camellia-CBC(256)
SHA1
    IDEA-CBC-SHA   0x00, 0x07   RSA   RSA   IDEA-CBC(128)
SHA1
    SEED-SHA   0x00, 0x96   RSA   RSA   SEED-CBC(128)
SHA1
    ECDHE-RSA-AES128-SHA256   0xC0, 0x27   ECDH   RSA   AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384   0xC0, 0x28   ECDH   RSA   AES-CBC(256)
SHA384
    RSA-AES128-SHA256   0x00, 0x3C   RSA   RSA   AES-CBC(128)
SHA256
    RSA-AES256-SHA256   0x00, 0x3D   RSA   RSA   AES-CBC(256)
SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256

- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384

- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384

- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305

- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/465/smtp

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
below:

  High Strength Ciphers (>= 112-bit key)

    Name   Code   KEX   Auth   Encryption   MAC
    ---------------------   ----------   ---   ----   -------------------- ---
    DHE-RSA-AES128-SHA   0x00, 0x33   DH   RSA   AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA   0x00, 0x39   DH   RSA   AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA   0x00, 0x45   DH   RSA   Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA   0x00, 0x88   DH   RSA   Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA   0xC0, 0x13   ECDH   RSA   AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA   0xC0, 0x14   ECDH   RSA   AES-CBC(256)
SHA1
    AES128-SHA   0x00, 0x2F   RSA   RSA   AES-CBC(128)
SHA1
    AES256-SHA   0x00, 0x35   RSA   RSA   AES-CBC(256)
SHA1
    CAMELLIA128-SHA   0x00, 0x41   RSA   RSA   Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA   0x00, 0x84   RSA   RSA   Camellia-CBC(256)
SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256

- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384

- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384

- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305

- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/993/imap

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

  High Strength Ciphers (>= 112-bit key)

```
    Name                      Code         KEX        Auth      Encryption             MAC
    ---------------------     ----------   ---        ----      --------------------   ---
    RSA-AES128-SHA256         0x00, 0x9C   RSA        RSA       AES-GCM(128)
SHA256
    RSA-AES256-SHA384         0x00, 0x9D   RSA        RSA       AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA      0xC0, 0x13   ECDH       RSA       AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA      0xC0, 0x14   ECDH       RSA       AES-CBC(256)
SHA1
    AES128-SHA                0x00, 0x2F   RSA        RSA       AES-CBC(128)
SHA1
    AES256-SHA                0x00, 0x35   RSA        RSA       AES-CBC(256)
SHA1
    CAMELLIA128-SHA           0x00, 0x41   RSA        RSA       Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA           0x00, 0x84   RSA        RSA       Camellia-CBC(256)
SHA1
    IDEA-CBC-SHA              0x00, 0x07   RSA        RSA       IDEA-CBC(128)
SHA1
    SEED-SHA                  0x00, 0x96   RSA        RSA       SEED-CBC(128)
SHA1
    ECDHE-RSA-AES128-SHA256   0xC0, 0x27   ECDH       RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384   0xC0, 0x28   ECDH       RSA       AES-CBC(256)
SHA384
    RSA-AES128-SHA256         0x00, 0x3C   RSA        RSA       AES-CBC(128)
SHA256
    RSA-AES256-SHA256         0x00, 0x3D   RSA        RSA       AES-CBC(256)
SHA256
```

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256

- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384

- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384

- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305

- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/995/pop3

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

  High Strength Ciphers (>= 112-bit key)

```
    Name                        Code         KEX      Auth    Encryption             MAC
    ---------------------       ----------   ---      ----    --------------------   ---
    RSA-AES128-SHA256           0x00, 0x9C   RSA      RSA     AES-GCM(128)
SHA256
    RSA-AES256-SHA384           0x00, 0x9D   RSA      RSA     AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA        0xC0, 0x13   ECDH     RSA     AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14   ECDH     RSA     AES-CBC(256)
SHA1
    AES128-SHA                  0x00, 0x2F   RSA      RSA     AES-CBC(128)
SHA1
    AES256-SHA                  0x00, 0x35   RSA      RSA     AES-CBC(256)
SHA1
    CAMELLIA128-SHA             0x00, 0x41   RSA      RSA     Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA             0x00, 0x84   RSA      RSA     Camellia-CBC(256)
SHA1
    IDEA-CBC-SHA                0x00, 0x07   RSA      RSA     IDEA-CBC(128)
SHA1
    SEED-SHA                    0x00, 0x96   RSA      RSA     SEED-CBC(128)
SHA1
    ECDHE-RSA-AES128-SHA256     0xC0, 0x27   ECDH     RSA     AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384     0xC0, 0x28   ECDH     RSA     AES-CBC(256)
SHA384
    RSA-AES128-SHA256           0x00, 0x3C   RSA      RSA     AES-CBC(128)
SHA256
    RSA-AES256-SHA256           0x00, 0x3D   RSA      RSA     AES-CBC(256)
SHA256
```

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256

- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384

- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384

- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305

- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/2078/www

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
below:

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name   Code   KEX   Auth   Encryption   MAC
    --------------------   ----------   ---   ----   -------------------- ---
    DES-CBC3-SHA   0x00, 0x0A   RSA   RSA   3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name   Code   KEX   Auth   Encryption   MAC
    --------------------   ----------   ---   ----   -------------------- ---
    DHE-RSA-AES128-SHA256   0x00, 0x9E   DH   RSA   AES-GCM(128)
SHA256
    DHE-RSA-AES256-SHA384   0x00, 0x9F   DH   RSA   AES-GCM(256)
SHA384
    RSA-AES128-SHA256   0x00, 0x9C   RSA   RSA   AES-GCM(128)
SHA256
    RSA-AES256-SHA384   0x00, 0x9D   RSA   RSA   AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA   0x00, 0x33   DH   RSA   AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA   0x00, 0x39   DH   RSA   AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA 0x00, 0x45   DH   RSA   Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA 0x00, 0x88   DH   RSA   Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA   0xC0, 0x13   ECDH   RSA   AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA   0xC0, 0x14   ECDH   RSA   AES-CBC(256)
SHA1
    AES128-SHA   0x00, 0x2F   RSA   RSA   AES-CBC(128)
SHA1
    AES256-SHA   0x00, 0x35   RSA   RSA   AES-CBC(256)
SHA1
    CAMELLIA128-SHA   0x00, 0x41   RSA   RSA   Camellia-CBC(128)
[...]

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256

- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384

- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384

- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305

- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/2083/www

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
below:

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name   Code   KEX   Auth   Encryption   MAC
    --------------------   ----------   ---   ----   --------------------   ---
    DES-CBC3-SHA   0x00, 0x0A   RSA   RSA   3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name   Code   KEX   Auth   Encryption   MAC
    --------------------   ----------   ---   ----   --------------------   ---
    DHE-RSA-AES128-SHA256   0x00, 0x9E   DH   RSA   AES-GCM(128)
SHA256
    DHE-RSA-AES256-SHA384   0x00, 0x9F   DH   RSA   AES-GCM(256)
SHA384
    RSA-AES128-SHA256   0x00, 0x9C   RSA   RSA   AES-GCM(128)
SHA256
    RSA-AES256-SHA384   0x00, 0x9D   RSA   RSA   AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA   0x00, 0x33   DH   RSA   AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA   0x00, 0x39   DH   RSA   AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA   0x00, 0x45   DH   RSA   Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA   0x00, 0x88   DH   RSA   Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA   0xC0, 0x13   ECDH   RSA   AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA   0xC0, 0x14   ECDH   RSA   AES-CBC(256)
SHA1
    AES128-SHA   0x00, 0x2F   RSA   RSA   AES-CBC(128)
SHA1
    AES256-SHA   0x00, 0x35   RSA   RSA   AES-CBC(256)
SHA1
    CAMELLIA128-SHA   0x00, 0x41   RSA   RSA   Camellia-CBC(128)
  [...]

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256

- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384

- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384

- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305

- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/2087/www

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
below:

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name   Code   KEX   Auth   Encryption   MAC
    ---------------------   ----------   ---   ----   -------------------- ---
    DES-CBC3-SHA   0x00, 0x0A   RSA   RSA   3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name   Code   KEX   Auth   Encryption   MAC
    ---------------------   ----------   ---   ----   -------------------- ---
    DHE-RSA-AES128-SHA256   0x00, 0x9E   DH   RSA   AES-GCM(128)
SHA256
    DHE-RSA-AES256-SHA384   0x00, 0x9F   DH   RSA   AES-GCM(256)
SHA384
    RSA-AES128-SHA256   0x00, 0x9C   RSA   RSA   AES-GCM(128)
SHA256
    RSA-AES256-SHA384   0x00, 0x9D   RSA   RSA   AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA   0x00, 0x33   DH   RSA   AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA   0x00, 0x39   DH   RSA   AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA   0x00, 0x45   DH   RSA   Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA   0x00, 0x88   DH   RSA   Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA   0xC0, 0x13   ECDH   RSA   AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA   0xC0, 0x14   ECDH   RSA   AES-CBC(256)
SHA1
    AES128-SHA   0x00, 0x2F   RSA   RSA   AES-CBC(128)
SHA1
    AES256-SHA   0x00, 0x35   RSA   RSA   AES-CBC(256)
SHA1
    CAMELLIA128-SHA   0x00, 0x41   RSA   RSA   Camellia-CBC(128)
[...]

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256

- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384

- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384

- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305

- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/2096/www

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name   Code   KEX   Auth   Encryption   MAC
    --------------------   ----------   ---   ----   --------------------   ---
    DES-CBC3-SHA   0x00, 0x0A   RSA   RSA   3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name   Code   KEX   Auth   Encryption   MAC
    --------------------   ----------   ---   ----   --------------------   ---
    DHE-RSA-AES128-SHA256   0x00, 0x9E   DH   RSA   AES-GCM(128)
SHA256
    DHE-RSA-AES256-SHA384   0x00, 0x9F   DH   RSA   AES-GCM(256)
SHA384
    RSA-AES128-SHA256   0x00, 0x9C   RSA   RSA   AES-GCM(128)
SHA256
    RSA-AES256-SHA384   0x00, 0x9D   RSA   RSA   AES-GCM(256)
SHA384
    DHE-RSA-AES128-SHA   0x00, 0x33   DH   RSA   AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA   0x00, 0x39   DH   RSA   AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA   0x00, 0x45   DH   RSA   Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA   0x00, 0x88   DH   RSA   Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA   0xC0, 0x13   ECDH   RSA   AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA   0xC0, 0x14   ECDH   RSA   AES-CBC(256)
SHA1
    AES128-SHA   0x00, 0x2F   RSA   RSA   AES-CBC(128)
SHA1
    AES256-SHA   0x00, 0x35   RSA   RSA   AES-CBC(256)
SHA1
    CAMELLIA128-SHA   0x00, 0x41   RSA   RSA   Camellia-CBC(128)
  [...]

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/25/smtp

```
An SMTP server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/110/pop3

```
A POP3 server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/443/www

```
A TLSv1.2 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.2.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/465/smtp

```
A TLSv1 server answered on this port.
```

tcp/465/smtp

```
An SMTP server is running on this port through TLSv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/587/smtp

```
An SMTP server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/993/imap

```
A TLSv1 server answered on this port.
```

tcp/993/imap

```
An IMAP server is running on this port through TLSv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/995/pop3

```
  A POP3 server is running on this port through TLSv1.
```

tcp/995/pop3

```
  A TLSv1 server answered on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/2000

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/2078/www

```
A TLSv1 server answered on this port.
```

tcp/2078/www

```
A web server is running on this port through TLSv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/2083/www

```
A TLSv1 server answered on this port.
```

tcp/2083/www

```
A web server is running on this port through TLSv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/2087/www

```
A TLSv1 server answered on this port.
```

tcp/2087/www

```
A web server is running on this port through TLSv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/2096/www

```
A TLSv1 server answered on this port.
```

tcp/2096/www

```
A web server is running on this port through TLSv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/5060

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

Plugin Output

tcp/143/imap

```
An IMAP server is running on this port.
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

Plugin Output

tcp/3306/mysql

```
A MySQL server is running on this port.
```

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2024/09/11

Plugin Output

tcp/443/www

```
http/1.1
h2
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF   CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/110/pop3

```
  TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF   CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/143/imap

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF   CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/993/imap

```
  TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF   CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/995/pop3

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF   CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/2078/www

```
  TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF   CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/2083/www

```
 TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF   CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/2087/www

```
 TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF   CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/2096/www

```
  TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/110/pop3

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/143/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/443/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/993/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/995/pop3

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2078/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2083/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2087/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2096/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/443/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF   IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

Plugin Output

tcp/0

```
  SSH was detected on port 22 but no credentials were provided.
  SSH local checks were not enabled.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

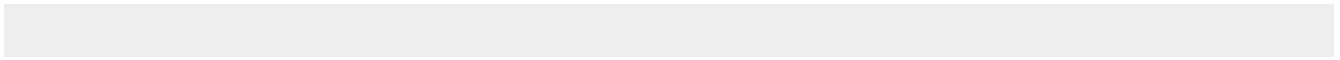Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.43.138 to 162.241.216.11 :
192.168.43.138

ttl was greater than 50 - Completing Traceroute.

192.168.43.1
10.3.255.254
192.168.58.17
192.168.34.2
192.168.34.9
223.196.21.204
182.19.123.229
182.19.125.161
223.196.40.79
112.110.250.89
112.110.250.91
182.19.106.105
195.89.101.185
62.115.175.10
62.115.135.224
62.115.135.24
62.115.139.244
?
62.115.136.107
80.239.167.103
69.195.64.105
162.144.240.135
?

Hop Count: 24

An error was detected along the way.
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/80/www

```
The following cookies are expired :

Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessauth
Path : /
Value : expired
Domain : box5331.bluehost.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/443/www

```
The following cookies are expired :

Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessauth
Path : /
Value : expired
Domain : box5331.bluehost.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/2078/www

```
The following cookies are expired :

Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessauth
Path : /
Value : expired
Domain : box5331.bluehost.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/2083/www

```
The following cookies are expired :

Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessauth
Path : /
Value : expired
Domain : box5331.bluehost.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/2087/www

```
The following cookies are expired :

Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessauth
Path : /
Value : expired
Domain : box5331.bluehost.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/2096/www

```
The following cookies are expired :

Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessauth
Path : /
Value : expired
Domain : box5331.bluehost.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

```
 CGI scanning will be disabled for this host because the host responds
 to requests for non-existent URLs with HTTP code 301
 rather than 404. The requested URL was :

    http://box5331.bluehost.com/DuRGfVaZPTFO.html
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/2083/www

```
The following string will be used :
TYPE="password"
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/2087/www

```
The following string will be used :
TYPE="password"
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/2096/www

```
  The following string will be used :
  TYPE="password"
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/2083/www

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/2087/www

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/2096/www

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.

It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/2078/www