De-ICE

Report generated by Nessus™ Thu, 01 Jun 2023 10:54:31 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

10.0.2.4

5	9	23	2	79
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	10.0.2.4
MAC Address:	08:00:27:64:FE:E2
OS:	Linux Kernel 3.0 on Ubuntu 12.04 (precise)

Vulnerabilities

84215 - ProFTPD mod_copy Information Disclosure

Synopsis

The remote host is running a ProFTPD module that is affected by an information disclosure vulnerability.

Description

The remote host is running a version of ProFTPD that is affected by an information disclosure vulnerability in the mod_copy module due to the SITE CPFR and SITE CPTO commands being available to unauthenticated clients. An unauthenticated, remote attacker can exploit this flaw to read and write to arbitrary files on any web accessible path on the host.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=4169

Solution

Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.1 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	74238
CVE	CVE-2015-3306
XREF	EDB-ID:36742
XREF	EDB-ID:36803

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2015/06/16, Modified: 2020/03/27

Plugin Output

tcp/21/ftp

```
Nessus received a 350 response from sending the following unauthenticated request :

SITE CPFR /etc/passwd
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/443/www

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


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

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    EDH-RSA-DES-CBC3-SHA                            DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                    RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    DHE-RSA-AES128-SHA                              DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA                              DH            RSA      AES-CBC(256)
 SHA1
    DHE-RSA-CAMELLIA128-SHA                         DH            RSA      Camellia-CBC(128)
 SHA1
    DHE-RSA-CAMELLIA256-SHA                         DH            RSA      Camellia-CBC(256)
 SHA1
    DHE-RSA-SEED-SHA                                DH            RSA      SEED-CBC(128)
 SHA1
    AES128-SHA                                      RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                                      RSA           RSA      AES-CBC(256)
 SHA1
    CAMELLIA128-SHA                                 RSA           RSA      Camellia-CBC(128)
 SHA1
    CAMELLIA256-SHA                                 RSA           RSA      Camellia-CBC(256)
 SHA1
    RC4-SHA                                         RSA           RSA      RC4(128)
 SHA1
    SEED-SHA                                        RSA           RSA      SEED-CBC(128)
 SHA1
    DHE-RSA-AES128-SHA256                           DH            RSA      [...]
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/993/imap

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


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

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    EDH-RSA-DES-CBC3-SHA                            DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                    RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    DHE-RSA-AES128-SHA                              DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA                              DH            RSA      AES-CBC(256)
 SHA1
    DHE-RSA-CAMELLIA128-SHA                         DH            RSA      Camellia-CBC(128)
 SHA1
    DHE-RSA-CAMELLIA256-SHA                         DH            RSA      Camellia-CBC(256)
 SHA1
    DHE-RSA-SEED-SHA                                DH            RSA      SEED-CBC(128)
 SHA1
    AES128-SHA                                      RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                                      RSA           RSA      AES-CBC(256)
 SHA1
    CAMELLIA128-SHA                                 RSA           RSA      Camellia-CBC(128)
 SHA1
    CAMELLIA256-SHA                                 RSA           RSA      Camellia-CBC(256)
 SHA1
    RC4-MD5                                         RSA           RSA      RC4(128)                MD5
    RC4-SHA                                         RSA           RSA      RC4(128)
 SHA1
    SEED-SHA                                        RSA           RSA       [...]
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/995/pop3

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


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

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    EDH-RSA-DES-CBC3-SHA                            DH            RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                    RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    DHE-RSA-AES128-SHA                              DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA                              DH            RSA      AES-CBC(256)
 SHA1
    DHE-RSA-CAMELLIA128-SHA                         DH            RSA      Camellia-CBC(128)
 SHA1
    DHE-RSA-CAMELLIA256-SHA                         DH            RSA      Camellia-CBC(256)
 SHA1
    DHE-RSA-SEED-SHA                                DH            RSA      SEED-CBC(128)
 SHA1
    AES128-SHA                                      RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                                      RSA           RSA      AES-CBC(256)
 SHA1
    CAMELLIA128-SHA                                 RSA           RSA      Camellia-CBC(128)
 SHA1
    CAMELLIA256-SHA                                 RSA           RSA      Camellia-CBC(256)
 SHA1
    RC4-MD5                                         RSA           RSA      RC4(128)                MD5
    RC4-SHA                                         RSA           RSA      RC4(128)
 SHA1
    SEED-SHA                                        RSA           RSA       [...]
```

33850 - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	IAVA:0001-A-0502
XREF	IAVA:0001-A-0648

Plugin Information

Published: 2008/08/08, Modified: 2023/05/18

Plugin Output

tcp/0

```
Ubuntu 12.04 support ended on 2017-04-30.
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.

For more information, see : https://wiki.ubuntu.com/Releases
```

73412 - OpenSSL Heartbeat Information Disclosure (Heartbleed)

Synopsis

The remote service is affected by an information disclosure vulnerability.

Description

Based on its response to a TLS request with a specially crafted heartbeat message (RFC 6520), the remote service appears to be affected by an out-of-bounds read flaw.

This flaw could allow a remote attacker to read the contents of up to 64KB of server memory, potentially exposing passwords, private keys, and other sensitive data.

See Also

http://heartbleed.com/

http://eprint.iacr.org/2014/140

http://www.openssl.org/news/vulnerabilities.html#2014-0160

https://www.openssl.org/news/secadv/20140407.txt

Solution

Upgrade to OpenSSL 1.0.1g or later.

Alternatively, recompile OpenSSL with the '-DOPENSSL_NO_HEARTBEATS'
flag to disable the vulnerable functionality.

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)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

6.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

References

BID	66690
CVE	CVE-2014-0160
XREF	CERT:720951
XREF	EDB-ID:32745
XREF	EDB-ID:32764
XREF	EDB-ID:32791
XREF	EDB-ID:32998
XREF	CISA-KNOWN-EXPLOITED:2022/05/25

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2014/04/08, Modified: 2023/04/25

Plugin Output

tcp/443/www

```
Nessus was able to read the following memory from the remote service:

0x0000:  50 50 61 00 02 48 00 1D 00 1C FE FF FF E0 FE FE    PPa..H..........
0x0010:  FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7    ................
0x0020:  00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2    ................
0x0030:  00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4    .........|.}....
0x0040:  00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6    ...........~....
0x0050:  00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF    ...........+....
0x0060:  C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B    .,.r...s........
0x0070:  CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8    .../.0.v...w....
0x0080:  C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32    .-...t...u...1.2
0x0090:  C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8    .x...y..........
0x00A0:  00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F    ................
0x00B0:  CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE    ................
0x00C0:  C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B    .............z.{
0x00D0:  00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87    .c.e.....2.8.D..
0x00E0:  00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14    ...f............
0x00F0:  00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B    ...3.9.E........
0x0100:  00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E    ...0.6.B........
0x0110:  00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19    ...1.7.C........
0x0120:  00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18    .....4.:.F......
0x0130:  00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13    ................
0x0140:  C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02    ................
0x0150:  C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18    ................
0x0160:  C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28    .....).&.*.'.+.(
0x0170:  00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20    .#..."...%.!.$.
0x0180:  00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60    ...........b.a.`
0x0190:  00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 [...]
```

73412 - OpenSSL Heartbeat Information Disclosure (Heartbleed)

Synopsis

The remote service is affected by an information disclosure vulnerability.

Description

Based on its response to a TLS request with a specially crafted heartbeat message (RFC 6520), the remote service appears to be affected by an out-of-bounds read flaw.

This flaw could allow a remote attacker to read the contents of up to 64KB of server memory, potentially exposing passwords, private keys, and other sensitive data.

See Also

http://heartbleed.com/

http://eprint.iacr.org/2014/140

http://www.openssl.org/news/vulnerabilities.html#2014-0160

https://www.openssl.org/news/secadv/20140407.txt

Solution

Upgrade to OpenSSL 1.0.1g or later.

Alternatively, recompile OpenSSL with the '-DOPENSSL_NO_HEARTBEATS'
flag to disable the vulnerable functionality.

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)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

6.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

References

BID	66690
CVE	CVE-2014-0160
XREF	CERT:720951
XREF	EDB-ID:32745
XREF	EDB-ID:32764
XREF	EDB-ID:32791
XREF	EDB-ID:32998
XREF	CISA-KNOWN-EXPLOITED:2022/05/25

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2014/04/08, Modified: 2023/04/25

Plugin Output

tcp/993/imap

```
Nessus was able to read the following memory from the remote service:

0x0000:  30 42 53 00 02 48 00 1D 00 1C FE FF FF E0 FE FE    0BS..H..........
0x0010:  FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7    ................
0x0020:  00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2    ................
0x0030:  00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4    .........|.}....
0x0040:  00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6    ...........~....
0x0050:  00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF    ...........+....
0x0060:  C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B    .,.r...s........
0x0070:  CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8    .../.0.v...w....
0x0080:  C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32    .-...t...u...1.2
0x0090:  C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8    .x...y..........
0x00A0:  00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F    ................
0x00B0:  CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE    ................
0x00C0:  C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B    .............z.{
0x00D0:  00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87    .c.e.....2.8.D..
0x00E0:  00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14    ...f............
0x00F0:  00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B    ...3.9.E........
0x0100:  00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E    ...0.6.B........
0x0110:  00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19    ...1.7.C........
0x0120:  00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18    .....4.:.F......
0x0130:  00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13    ................
0x0140:  C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02    ................
0x0150:  C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18    ................
0x0160:  C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28    .....).&.*.'.+.(
0x0170:  00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20    .#..."...%.!.$.
0x0180:  00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60    ...........b.a.`
0x0190:  00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 [...]
```

73412 - OpenSSL Heartbeat Information Disclosure (Heartbleed)

Synopsis

The remote service is affected by an information disclosure vulnerability.

Description

Based on its response to a TLS request with a specially crafted heartbeat message (RFC 6520), the remote service appears to be affected by an out-of-bounds read flaw.

This flaw could allow a remote attacker to read the contents of up to 64KB of server memory, potentially exposing passwords, private keys, and other sensitive data.

See Also

http://heartbleed.com/

http://eprint.iacr.org/2014/140

http://www.openssl.org/news/vulnerabilities.html#2014-0160

https://www.openssl.org/news/secadv/20140407.txt

Solution

Upgrade to OpenSSL 1.0.1g or later.

Alternatively, recompile OpenSSL with the '-DOPENSSL_NO_HEARTBEATS'
flag to disable the vulnerable functionality.

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)

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

6.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

References

BID	66690
CVE	CVE-2014-0160
XREF	CERT:720951
XREF	EDB-ID:32745
XREF	EDB-ID:32764
XREF	EDB-ID:32791
XREF	EDB-ID:32998
XREF	CISA-KNOWN-EXPLOITED:2022/05/25

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2014/04/08, Modified: 2023/04/25

Plugin Output

tcp/995/pop3

```
Nessus was able to read the following memory from the remote service:

0x0000:  33 58 63 00 02 48 00 1D 00 1C FE FF FF E0 FE FE    3Xc..H..........
0x0010:  FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7    ................
0x0020:  00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2    ................
0x0030:  00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4    .........|.}....
0x0040:  00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6    ...........~....
0x0050:  00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF    ...........+....
0x0060:  C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B    .,.r...s........
0x0070:  CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8    .../.0.v...w....
0x0080:  C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32    .-...t...u...1.2
0x0090:  C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8    .x...y..........
0x00A0:  00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F    ................
0x00B0:  CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE    ................
0x00C0:  C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B    .............z.{
0x00D0:  00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87    .c.e.....2.8.D..
0x00E0:  00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14    ...f............
0x00F0:  00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B    ...3.9.E........
0x0100:  00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E    ...0.6.B........
0x0110:  00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19    ...1.7.C........
0x0120:  00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18    .....4.:.F......
0x0130:  00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13    ................
0x0140:  C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02    ................
0x0150:  C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18    ................
0x0160:  C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28    .....).&.*.'.+.(
0x0170:  00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20    .#..."...%.!.$.
0x0180:  00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60    ...........b.a.`
0x0190:  00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 [...]
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an 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. An attacker can exploit this to generate another certificate with the same digital signature, allowing an 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 certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?e120eea1

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

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:H/A:N)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2022/01/14

Plugin Output

tcp/443/www

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

Subject             : CN=webhost
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 01 08:25:15 2023 GMT
Valid To            : May 29 08:25:15 2033 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIICoDCCAYgCCQCn3S0UIfeGAzANBgkqhkiG9w0BAQUFADASMRAwDgYDVQQDEwd3ZWJob3N0MB4XDTIzMDYwMTA4MjUxNVoXDTMzMDUyOTA4MjUxNV
+MaRw1nmRQmRMTgQCARAffQzsJiZSgXe9pSnJShBT6p3k7uST8CEXkk2FNUjbFXpN0VDGbH5rwTq8AKeR+Ivv0GTMTqUON6+/
lhyhrCcuEq6++SAkRPYJ7GJgu5ThAjD9tDi0jpO/2OAv6wcb+0k6Ikqy3Xzhc33rkMMLGt/9zNlesH8RNpm9kP0/
FXx9cRhB+xj62sXZ/L0M8jIsmCko4rJmtX/DcoJmCa5aoog2hUN0gR7orINoH
+quprHj1d0CAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAJ0uP3+6tJ8nQfWqlncREl6s3p+ghkKQ1hC2s6U2kmo77CCB
+8li5DKn4dMdZvx79DHMX1H+0HxAQr8XQITCwStvTpm4gT+TqBXYv9vXseTE0AmEGNZ1tuP2NiScPoe1VjL1+JChPSXR
+YtfwaB3P4QtwRtzghICAyvfwxAuRag3G5+m8NOrqlOQtcRZ7KBIIUVV1UEUY4fLkSEqcHzOTcZuez1qpYRz7DYmUw6cvqoRDfbvuxVmdygmRiIWqW
+jtG6SPVwng16qZlwrgRyFqQg==
-----END CERTIFICATE-----
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an 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. An attacker can exploit this to generate another certificate with the same digital signature, allowing an 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 certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?e120eea1

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

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:H/A:N)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2022/01/14

Plugin Output

tcp/993/imap

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

Subject             : CN=webhost
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 01 08:25:15 2023 GMT
Valid To            : May 29 08:25:15 2033 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIICoDCCAYgCCQCn3S0UIfeGAzANBgkqhkiG9w0BAQUFADASMRAwDgYDVQQDEwd3ZWJob3N0MB4XDTIzMDYwMTA4MjUxNVoXDTMzMDUyOTA4MjUxNV
+MaRw1nmRQmRMTgQCARAffQzsJiZSgXe9pSnJShBT6p3k7uST8CEXkk2FNUjbFXpN0VDGbH5rwTq8AKeR+Ivv0GTMTqUON6+/
lhyhrCcuEq6++SAkRPYJ7GJgu5ThAjD9tDi0jpO/2OAv6wcb+0k6Ikqy3Xzhc33rkMMLGt/9zNlesH8RNpm9kP0/
FXx9cRhB+xj62sXZ/L0M8jIsmCko4rJmtX/DcoJmCa5aoog2hUN0gR7orINoH
+quprHj1d0CAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAJ0uP3+6tJ8nQfWqlncREl6s3p+ghkKQ1hC2s6U2kmo77CCB
+8li5DKn4dMdZvx79DHMX1H+0HxAQr8XQITCwStvTpm4gT+TqBXYv9vXseTE0AmEGNZ1tuP2NiScPoe1VjL1+JChPSXR
+YtfwaB3P4QtwRtzghICAyvfwxAuRag3G5+m8NOrqlOQtcRZ7KBIIUVV1UEUY4fLkSEqcHzOTcZuez1qpYRz7DYmUw6cvqoRDfbvuxVmdygmRiIWqW
+jtG6SPVwng16qZlwrgRyFqQg==
-----END CERTIFICATE-----
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an 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. An attacker can exploit this to generate another certificate with the same digital signature, allowing an 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 certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?e120eea1

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

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:H/A:N)

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.9 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2022/01/14

Plugin Output

tcp/995/pop3

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

Subject              : CN=webhost
Signature Algorithm : SHA-1 With RSA Encryption
Valid From           : Jun 01 08:25:15 2023 GMT
Valid To             : May 29 08:25:15 2033 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIICoDCCAYgCCQCn3S0UIfeGAzANBgkqhkiG9w0BAQUFADASMRAwDgYDVQQDEwd3ZWJob3N0MB4XDTIzMDYwMTA4MjUxNVoXDTMzMDUyOTA4MjUxNV
+MaRw1nmRQmRMTgQCARAffQzsJiZSgXe9pSnJShBT6p3k7uST8CEXkk2FNUjbFXpN0VDGbH5rwTq8AKeR+Ivv0GTMTqUON6+/
lhyhrCcuEq6++SAkRPYJ7GJgu5ThAjD9tDi0jpO/2OAv6wcb+0k6Ikqy3Xzhc33rkMMLGt/9zNlesH8RNpm9kP0/
FXx9cRhB+xj62sXZ/L0M8jIsmCko4rJmtX/DcoJmCa5aoog2hUN0gR7orINoH
+quprHj1d0CAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAJ0uP3+6tJ8nQfWqlncREl6s3p+ghkKQ1hC2s6U2kmo77CCB
+8li5DKn4dMdZvx79DHMX1H+0HxAQr8XQITCwStvTpm4gT+TqBXYv9vXseTE0AmEGNZ1tuP2NiScPoe1VjL1+JChPSXR
+YtfwaB3P4QtwRtzghICAyvfwxAuRag3G5+m8NOrqlOQtcRZ7KBIIUVV1UEUY4fLkSEqcHzOTcZuez1qpYRz7DYmUw6cvqoRDfbvuxVmdygmRiIWqW
+jtG6SPVwng16qZlwrgRyFqQg==
-----END CERTIFICATE-----
```

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

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

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

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: 2021/02/03

Plugin Output

tcp/443/www

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

    Name                          Code              KEX           Auth      Encryption              MAC
    ----------------------        ----------        ---           ----      --------------------    ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA       3DES-CBC(168)
 SHA1
    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

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

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

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: 2021/02/03

Plugin Output

tcp/993/imap

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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    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

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

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

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: 2021/02/03

Plugin Output

tcp/995/pop3

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

    Name                          Code              KEX           Auth      Encryption              MAC
    ----------------------        ----------        ---           ----      --------------------    ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA       3DES-CBC(168)
 SHA1
    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}
```

88098 - Apache Server ETag Header Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

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 v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	6939
CVE	CVE-2003-1418

XREF CWE:200

Plugin Information

Published: 2016/01/22, Modified: 2020/04/27

Plugin Output

tcp/80/www

```
Nessus was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                : ETag: "2edc-6f6-4da1930e20900"
  Inode number          : 11996
  File size             : 1782 bytes
  File modification time : Apr. 11, 2013 at 17:33:56 GMT
```

88098 - Apache Server ETag Header Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

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 v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

1.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	6939
CVE	CVE-2003-1418

XREF CWE:200

Plugin Information

Published: 2016/01/22, Modified: 2020/04/27

Plugin Output

tcp/443/www

```
Nessus was able to determine that the Apache Server listening on
port 443 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                : ETag: "2edc-6f6-4da1930e20900"
  Inode number          : 11996
  File size             : 1782 bytes
  File modification time : Apr. 11, 2013 at 17:33:56 GMT
```

77200 - OpenSSL 'ChangeCipherSpec' MiTM Vulnerability

Synopsis

The remote host is affected by a vulnerability that could allow sensitive data to be decrypted.

Description

The OpenSSL service on the remote host is vulnerable to a man-in-the-middle (MiTM) attack, based on its acceptance of a specially crafted handshake.

This flaw could allow a MiTM attacker to decrypt or forge SSL messages by telling the service to begin encrypted communications before key material has been exchanged, which causes predictable keys to be used to secure future traffic.

Note that Nessus has only tested for an SSL/TLS MiTM vulnerability (CVE-2014-0224). However, Nessus has inferred that the OpenSSL service on the remote host is also affected by six additional vulnerabilities that were disclosed in OpenSSL's June 5th, 2014 security advisory :

- An error exists in the 'ssl3_read_bytes' function that permits data to be injected into other sessions or allows denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2010-5298)

- An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that allows nonce disclosure via the 'FLUSH+RELOAD' cache side-channel attack. (CVE-2014-0076)

- A buffer overflow error exists related to invalid DTLS fragment handling that permits the execution of arbitrary code or allows denial of service attacks.

Note that this issue only affects OpenSSL when used as a DTLS client or server. (CVE-2014-0195)

- An error exists in the 'do_ssl3_write' function that permits a NULL pointer to be dereferenced, which could allow denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2014-0198)

- An error exists related to DTLS handshake handling that could allow denial of service attacks. Note that this issue only affects OpenSSL when used as a DTLS client.

(CVE-2014-0221)

- An error exists in the 'dtls1_get_message_fragment'

function related to anonymous ECDH cipher suites. This could allow denial of service attacks. Note that this issue only affects OpenSSL TLS clients. (CVE-2014-3470)

OpenSSL did not release individual patches for these vulnerabilities, instead they were all patched under a single version release. Note that the service will remain vulnerable after patching until the service or host is restarted.

See Also

http://www.nessus.org/u?d5709faa

https://www.imperialviolet.org/2014/06/05/earlyccs.html

https://www.openssl.org/news/secadv/20140605.txt

Solution

OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

8.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:C)

References

BID	66363
BID	66801
BID	67193
BID	67898
BID	67899
BID	67900
BID	67901
CVE	CVE-2010-5298
CVE	CVE-2014-0076
CVE	CVE-2014-0195
CVE	CVE-2014-0198
CVE	CVE-2014-0221
CVE	CVE-2014-0224
CVE	CVE-2014-3470
XREF	CERT:978508

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/08/14, Modified: 2021/03/11

Plugin Output

tcp/443/www

```
The remote service on port 443 accepted an early ChangeCipherSpec message, which caused
the MAC and encryption keys to be derived entirely from public information. The entire SSL
handshake was completed, with the server accepting and producing messages encrypted and
authenticated using these weak keys.
```

77200 - OpenSSL 'ChangeCipherSpec' MiTM Vulnerability

Synopsis

The remote host is affected by a vulnerability that could allow sensitive data to be decrypted.

Description

The OpenSSL service on the remote host is vulnerable to a man-in-the-middle (MiTM) attack, based on its acceptance of a specially crafted handshake.

This flaw could allow a MiTM attacker to decrypt or forge SSL messages by telling the service to begin encrypted communications before key material has been exchanged, which causes predictable keys to be used to secure future traffic.

Note that Nessus has only tested for an SSL/TLS MiTM vulnerability (CVE-2014-0224). However, Nessus has inferred that the OpenSSL service on the remote host is also affected by six additional vulnerabilities that were disclosed in OpenSSL's June 5th, 2014 security advisory :

- An error exists in the 'ssl3_read_bytes' function that permits data to be injected into other sessions or allows denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2010-5298)

- An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that allows nonce disclosure via the 'FLUSH+RELOAD' cache side-channel attack. (CVE-2014-0076)

- A buffer overflow error exists related to invalid DTLS fragment handling that permits the execution of arbitrary code or allows denial of service attacks.

Note that this issue only affects OpenSSL when used as a DTLS client or server. (CVE-2014-0195)

- An error exists in the 'do_ssl3_write' function that permits a NULL pointer to be dereferenced, which could allow denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2014-0198)

- An error exists related to DTLS handshake handling that could allow denial of service attacks. Note that this issue only affects OpenSSL when used as a DTLS client.

(CVE-2014-0221)

- An error exists in the 'dtls1_get_message_fragment'

function related to anonymous ECDH cipher suites. This could allow denial of service attacks. Note that this issue only affects OpenSSL TLS clients. (CVE-2014-3470)

OpenSSL did not release individual patches for these vulnerabilities, instead they were all patched under a single version release. Note that the service will remain vulnerable after patching until the service or host is restarted.

See Also

http://www.nessus.org/u?d5709faa

https://www.imperialviolet.org/2014/06/05/earlyccs.html

https://www.openssl.org/news/secadv/20140605.txt

Solution

OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

8.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:C)

References

BID	66363
BID	66801
BID	67193
BID	67898
BID	67899
BID	67900
BID	67901
CVE	CVE-2010-5298
CVE	CVE-2014-0076
CVE	CVE-2014-0195
CVE	CVE-2014-0198
CVE	CVE-2014-0221
CVE	CVE-2014-0224
CVE	CVE-2014-3470
XREF	CERT:978508

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/08/14, Modified: 2021/03/11

Plugin Output

tcp/993/imap

```
The remote service on port 993 accepted an early ChangeCipherSpec message, which caused
the MAC and encryption keys to be derived entirely from public information. The entire SSL
handshake was completed, with the server accepting and producing messages encrypted and
authenticated using these weak keys.
```

77200 - OpenSSL 'ChangeCipherSpec' MiTM Vulnerability

Synopsis

The remote host is affected by a vulnerability that could allow sensitive data to be decrypted.

Description

The OpenSSL service on the remote host is vulnerable to a man-in-the-middle (MiTM) attack, based on its acceptance of a specially crafted handshake.

This flaw could allow a MiTM attacker to decrypt or forge SSL messages by telling the service to begin encrypted communications before key material has been exchanged, which causes predictable keys to be used to secure future traffic.

Note that Nessus has only tested for an SSL/TLS MiTM vulnerability (CVE-2014-0224). However, Nessus has inferred that the OpenSSL service on the remote host is also affected by six additional vulnerabilities that were disclosed in OpenSSL's June 5th, 2014 security advisory :

- An error exists in the 'ssl3_read_bytes' function that permits data to be injected into other sessions or allows denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2010-5298)

- An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that allows nonce disclosure via the 'FLUSH+RELOAD' cache side-channel attack. (CVE-2014-0076)

- A buffer overflow error exists related to invalid DTLS fragment handling that permits the execution of arbitrary code or allows denial of service attacks.

Note that this issue only affects OpenSSL when used as a DTLS client or server. (CVE-2014-0195)

- An error exists in the 'do_ssl3_write' function that permits a NULL pointer to be dereferenced, which could allow denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2014-0198)

- An error exists related to DTLS handshake handling that could allow denial of service attacks. Note that this issue only affects OpenSSL when used as a DTLS client.

(CVE-2014-0221)

- An error exists in the 'dtls1_get_message_fragment'

function related to anonymous ECDH cipher suites. This could allow denial of service attacks. Note that this issue only affects OpenSSL TLS clients. (CVE-2014-3470)

OpenSSL did not release individual patches for these vulnerabilities, instead they were all patched under a single version release. Note that the service will remain vulnerable after patching until the service or host is restarted.

See Also

http://www.nessus.org/u?d5709faa

https://www.imperialviolet.org/2014/06/05/earlyccs.html

https://www.openssl.org/news/secadv/20140605.txt

Solution

OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

8.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:C)

References

BID	66363
BID	66801
BID	67193
BID	67898
BID	67899
BID	67900
BID	67901
CVE	CVE-2010-5298
CVE	CVE-2014-0076
CVE	CVE-2014-0195
CVE	CVE-2014-0198
CVE	CVE-2014-0221
CVE	CVE-2014-0224
CVE	CVE-2014-3470
XREF	CERT:978508

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/08/14, Modified: 2021/03/11

Plugin Output

tcp/995/pop3

```
The remote service on port 995 accepted an early ChangeCipherSpec message, which caused
the MAC and encryption keys to be derived entirely from public information. The entire SSL
handshake was completed, with the server accepting and producing messages encrypted and
authenticated using these weak keys.
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

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

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/443/www

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=webhost
|-Issuer  : CN=webhost
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

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

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/993/imap

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=webhost
|-Issuer  : CN=webhost
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

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

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/995/pop3

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=webhost
|-Issuer  : CN=webhost
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                        Code              KEX           Auth      Encryption              MAC
    ----------------------      ----------        ---           ----      ----------------------  ---
    RC4-SHA                     0x00, 0x05        RSA           RSA       RC4(128)
 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}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/993/imap

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                        Code              KEX           Auth      Encryption              MAC
    ----------------------      ----------        ---           ----      ---------------------   ---
    RC4-MD5                     0x00, 0x04        RSA           RSA       RC4(128)                MD5
    RC4-SHA                     0x00, 0x05        RSA           RSA       RC4(128)
 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}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/995/pop3

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                        Code              KEX           Auth      Encryption              MAC
    ----------------------      ----------        ---           ----      ---------------------   ---
    RC4-MD5                     0x00, 0x04        RSA           RSA       RC4(128)                MD5
    RC4-SHA                     0x00, 0x05        RSA           RSA       RC4(128)
 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}
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

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

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/443/www

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=webhost
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

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

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/993/imap

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=webhost
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

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

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/995/pop3

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=webhost
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/443/www

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/993/imap

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/995/pop3

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

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/443/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/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.
```

157288 - TLS Version 1.1 Protocol Deprecated

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: 2023/04/19

Plugin Output

tcp/443/www

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

157288 - TLS Version 1.1 Protocol Deprecated

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: 2023/04/19

Plugin Output

tcp/993/imap

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

157288 - TLS Version 1.1 Protocol Deprecated

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: 2023/04/19

Plugin Output

tcp/995/pop3

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

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

http://www.nessus.org/u?b02d91cd

https://datatracker.ietf.org/doc/html/rfc8732

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/10/13, Modified: 2021/10/13

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

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: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
  hmac-sha2-256-96
  hmac-sha2-512-96

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
  hmac-sha2-256-96
  hmac-sha2-512-96
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2022/03/21

Plugin Output

tcp/0

```
The Linux distribution detected was :
 - Ubuntu 12.04 (precise)
 - Ubuntu 12.10 (quantal)
 - Ubuntu 13.04 (raring)
```

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-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL        : http://10.0.2.4/
Version    : 2.2.99
Source     : Server: Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
backported : 1
modules    : mod_ssl/2.2.22 OpenSSL/1.0.1
os         : ConvertedUbuntu
```

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-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/05/24

Plugin Output

tcp/443/www

```
URL        : https://10.0.2.4/
Version    : 2.2.99
Source     : Server: Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
backported : 1
modules    : mod_ssl/2.2.22 OpenSSL/1.0.1
os         : ConvertedUbuntu
```

39519 - Backported Security Patch Detection (FTP)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote FTP 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/21/ftp

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

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.
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/80/www

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP 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/443/www

```
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: 2023/05/03

Plugin Output

tcp/0

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

  cpe:/o:canonical:ubuntu_linux:12.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:http_server:2.2.99 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:modssl:mod_ssl:2.2.22 -> mod_ssl
  cpe:/a:openbsd:openssh:5.9 -> OpenBSD OpenSSH
  cpe:/a:openssl:openssl:1.0.1 -> OpenSSL Project OpenSSL
```

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: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

08:00:27:64:FE:E2 : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:64:FE:E2
```

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

Plugin Information

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

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220 ProFTPD 1.3.4a Server (LazyAdmin corp.) [10.0.2.4]
```

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: 2021/05/19

Plugin Output

tcp/443/www

```
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/80/www

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

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

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/443/www

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

  - HTTP methods GET HEAD OPTIONS POST 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/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
```

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/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
```

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 and HTTP pipelining are 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: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Thu, 01 Jun 2023 08:39:35 GMT
  Server: Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
  Last-Modified: Thu, 11 Apr 2013 17:33:56 GMT
  ETag: "2edc-6f6-4da1930e20900"
  Accept-Ranges: bytes
  Content-Length: 1782
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html>
<title>Lazy Admin Corp.</title>
<style type="text/css">
table {
border-width: 1px;
border-spacing: 10px;
```

```
border-style: dashed;
border-color: gray;
border-collapse: separate;
background-color: #0d0d0d;
}
font {
font-family: Verdana;
color: #aaaaaa;
}
font.hidden {
font-family: Verdana;
color: #0d0d0d;
}
font.credit {
font-family: Arial;
color: #303030;
font-size: small;
}
</style>
<body bgcolor=#202020><br><br><center><table><td><br>
<font><center><big><b>Welcome to<br>
<big><big>Lazy Admin Corp.<br></big>
HackingLab!</b></big></big></h1></center><br><br><br>
You are employed by the management of LazyAdmin corp. to PenTest their Network.<br>
At this point you have managed to successfully break into the network.<br>
The goal is now to find and extract sensitive information.<br>
<br>
<br>
<div align=right>"I choose a lazy person to do a hard job.<br>
Because a lazy person will find an easy way to do it."<br>
~ <i>Bill Gates</i></div>
<br>
<br>
Below you can find some hints how to get the sensitive information<br>
(just mark the lines to see the hints):<br>
<br><br></font>
```

```
<font class="hidden">
1. Have you seen our new cool forum yet?<br><br>
2. Do not post sensitive information to public!<br><br>
3. Different passwords for different services. What is that for?!<br><br>
4. What if you are able to break out of your cell and manage to enter another one?<br><br>
5. Some things change from time to time, others don't.<br><br>
6. Sor [...]
```

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 and HTTP pipelining are 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: 2019/11/22

Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Thu, 01 Jun 2023 08:39:35 GMT
  Server: Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
  Last-Modified: Thu, 11 Apr 2013 17:33:56 GMT
  ETag: "2edc-6f6-4da1930e20900"
  Accept-Ranges: bytes
  Content-Length: 1782
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html>
<title>Lazy Admin Corp.</title>
<style type="text/css">
table {
border-width: 1px;
border-spacing: 10px;
```

```
border-style: dashed;
border-color: gray;
border-collapse: separate;
background-color: #0d0d0d;
}
font {
font-family: Verdana;
color: #aaaaaa;
}
font.hidden {
font-family: Verdana;
color: #0d0d0d;
}
font.credit {
font-family: Arial;
color: #303030;
font-size: small;
}
</style>
<body bgcolor=#202020><br><br><center><table><td><br>
<font><center><big><b>Welcome to<br>
<big><big>Lazy Admin Corp.<br></big>
HackingLab!</b></big></big></h1></center><br><br><br>
You are employed by the management of LazyAdmin corp. to PenTest their Network.<br>
At this point you have managed to successfully break into the network.<br>
The goal is now to find and extract sensitive information.<br>
<br>
<br>
<div align=right>"I choose a lazy person to do a hard job.<br>
Because a lazy person will find an easy way to do it."<br>
~ <i>Bill Gates</i></div>
<br>
<br>
Below you can find some hints how to get the sensitive information<br>
(just mark the lines to see the hints):<br>
<br><br></font>
```

```
<font class="hidden">
1. Have you seen our new cool forum yet?<br><br>
2. Do not post sensitive information to public!<br><br>
3. Different passwords for different services. What is that for?!<br><br>
4. What if you are able to break out of your cell and manage to enter another one?<br><br>
5. Some things change from time to time, others don't.<br><br>
6. So [...]
```

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 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN]
 Dovecot ready.
```

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: 2023/05/03

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: 2023/05/03

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: 2023/05/03

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: 2023/05/03

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: 2023/05/03

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: 2023/05/03

Plugin Output

tcp/995/pop3

```
Port 995/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: 2023/04/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.5.2
Nessus build : 20009
Plugin feed version : 202305311418
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
Scan name : De-ICE
```

```
Scan policy used : Basic Network Scan
Scanner IP : 10.0.2.15
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 205.737 ms
Thorough tests : no
Experimental tests : 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 launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Scan Start Date : 2023/6/1 10:36 CEST
Scan duration : 1077 sec
Scan for malware : no
```

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: 2022/03/09

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Confidence level : 95
Method : SSH

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SSH:SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
SinFP:!:
   P1:B10113:F0x12:W14600:O0204ffff:M1460:
   P2:B10113:F0x12:W14480:O0204ffff0402080affffffff4445414401030307:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190502_7_p=22
SSLcert:!:i/CN:webhosts/CN:webhost
5017ba435b7f37a41208bebe233f65ca1b6aed30
i/CN:webhosts/CN:webhost
5017ba435b7f37a41208bebe233f65ca1b6aed30
i/CN:webhosts/CN:webhost
5017ba435b7f37a41208bebe233f65ca1b6aed30



The remote host is running Linux Kernel 3.0 on Ubuntu 12.04 (precise)
```

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.
```

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/443/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/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

57323 - OpenSSL Version Detection

Synopsis

Nessus was able to detect the OpenSSL version.

Description

Nessus was able to extract the OpenSSL version from the web server's banner. Note that security patches in many cases are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0682

Plugin Information

Published: 2011/12/16, Modified: 2023/03/27

Plugin Output

tcp/80/www

```
Source             : Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
Reported version   : 1.0.1
Backported version : 1.0.1
```

57323 - OpenSSL Version Detection

Synopsis

Nessus was able to detect the OpenSSL version.

Description

Nessus was able to extract the OpenSSL version from the web server's banner. Note that security patches in many cases are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0682

Plugin Information

Published: 2011/12/16, Modified: 2023/03/27

Plugin Output

tcp/443/www

```
Source             : Apache/2.2.22 (Ubuntu) mod_ssl/2.2.22 OpenSSL/1.0.1
Reported version   : 1.0.1
Backported version : 1.0.1
```

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.
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2023/05/22

Plugin Output

tcp/0

```
. You need to take the following 2 actions :


[ OpenSSL 'ChangeCipherSpec' MiTM Vulnerability (77200) ]

+ Action to take : OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za.
 OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS
 users (client and/or server) should upgrade to 1.0.1h.

+Impact : Taking this action will resolve 7 different vulnerabilities (CVEs).


[ ProFTPD mod_copy Information Disclosure (84215) ]

+ Action to take : Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.
```

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: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  ssh-dss
  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 encryption_algorithms_server_to_client :

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

```
The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-256-96
  hmac-sha2-512
  hmac-sha2-512-96
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-256-96
  hmac-sha2-512
  hmac-sha2-512-96
  umac-64@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 compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96
```

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: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
SSH supported authentication : publickey
```

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: 2021/02/03

Plugin Output

tcp/443/www

```
This port supports SSLv3/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: 2021/02/03

Plugin Output

tcp/993/imap

```
This port supports SSLv3/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: 2021/02/03

Plugin Output

tcp/995/pop3

```
This port supports SSLv3/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/443/www

```
Subject Name:

Common Name: webhost

Issuer Name:

Common Name: webhost

Serial Number: 00 A7 DD 2D 14 21 F7 86 03

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jun 01 08:25:15 2023 GMT
Not Valid After: May 29 08:25:15 2033 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 FC 6F 54 C4 B9 8E DA C6 BD A6 5F 4E 7F 61 86 97 2A 37 B9
            B1 72 BC 98 3B 64 2A 3A 4C 40 5C 70 D8 AB 74 53 CE 86 E2 67
            8A C0 74 64 CD 25 39 CB EB EB EF 8F 5A 02 CE E9 FF DB 21 51
            F3 62 35 73 87 3E 31 A4 70 D6 79 91 42 64 4C 4E 04 02 01 10
            1F 7D 0C EC 26 26 52 81 77 BD A5 29 C9 4A 10 53 EA 9D E4 EE
            E4 93 F0 21 17 92 4D 85 35 48 DB 15 7A 4D D1 50 C6 6C 7E 6B
            C1 3A BC 00 A7 91 F8 8B EF D0 64 CC 4E A5 0E 37 AF BF 96 1C
            A1 AC 27 2E 12 AE BE F9 20 24 44 F6 09 EC 62 60 BB 94 E1 02
            30 FD B4 38 B4 8E 93 BF D8 E0 2F EB 07 1B FB 49 3A 22 4A B2
            DD 7C E1 73 7D EB 90 C3 0B 1A DF FD CC D9 5E B0 7F 11 36 99
            BD 90 FD 3F 15 7C 7D 71 18 41 FB 18 FA DA C5 D9 FC BD 0C F2
```

```
            32 2C 98 29 28 E2 B2 66 B5 7F C3 72 82 66 09 AE 5A A2 88 36
            85 43 74 81 1E E8 AC 83 68 1F EA AE A6 B1 E3 D5 DD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 27 4B 8F DF EE AD 27 C9 D0 7D 6A A5 9D C4 44 97 AB 37 A7
           E8 21 90 A4 35 84 2D AC E9 4D A4 9A 8E FB 08 20 7E F2 58 B9
           0C A9 F8 74 C7 59 BF 1E FD 0C 73 17 D4 7F B4 1F 10 10 AF C5
           D0 21 30 B0 4A DB D3 A6 6E 20 4F E4 EA 05 76 2F F6 F5 EC 79
           31 34 02 61 06 35 9D 6D B8 FD 8D 89 27 0F A1 ED 55 8C BD 7E
           24 28 4F 49 74 7E 62 D7 F0 68 1D CF E1 0B 70 46 DC E0 84 80
           80 CA F7 F0 C4 0B 91 6A 0D C6 E7 E9 BC 34 EA EA 94 E4 2D 71
           16 7B 28 12 08 51 55 75 50 45 18 E1 F2 E4 48 4A 9C 1F 33 93
           71 9B 9E CF 5A A9 61 1C FB 0D 89 94 C3 A7 2F AA 84 43 7D BB
           EE C5 59 9D CA 09 91 88 85 AA 59 93 F3 0A 08 71 B4 AA 26  [...]
```

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: webhost

Issuer Name:

Common Name: webhost

Serial Number: 00 A7 DD 2D 14 21 F7 86 03

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jun 01 08:25:15 2023 GMT
Not Valid After: May 29 08:25:15 2033 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 FC 6F 54 C4 B9 8E DA C6 BD A6 5F 4E 7F 61 86 97 2A 37 B9
            B1 72 BC 98 3B 64 2A 3A 4C 40 5C 70 D8 AB 74 53 CE 86 E2 67
            8A C0 74 64 CD 25 39 CB EB EB EF 8F 5A 02 CE E9 FF DB 21 51
            F3 62 35 73 87 3E 31 A4 70 D6 79 91 42 64 4C 4E 04 02 01 10
            1F 7D 0C EC 26 26 52 81 77 BD A5 29 C9 4A 10 53 EA 9D E4 EE
            E4 93 F0 21 17 92 4D 85 35 48 DB 15 7A 4D D1 50 C6 6C 7E 6B
            C1 3A BC 00 A7 91 F8 8B EF D0 64 CC 4E A5 0E 37 AF BF 96 1C
            A1 AC 27 2E 12 AE BE F9 20 24 44 F6 09 EC 62 60 BB 94 E1 02
            30 FD B4 38 B4 8E 93 BF D8 E0 2F EB 07 1B FB 49 3A 22 4A B2
            DD 7C E1 73 7D EB 90 C3 0B 1A DF FD CC D9 5E B0 7F 11 36 99
            BD 90 FD 3F 15 7C 7D 71 18 41 FB 18 FA DA C5 D9 FC BD 0C F2
```

```
            32 2C 98 29 28 E2 B2 66 B5 7F C3 72 82 66 09 AE 5A A2 88 36
            85 43 74 81 1E E8 AC 83 68 1F EA AE A6 B1 E3 D5 DD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 27 4B 8F DF EE AD 27 C9 D0 7D 6A A5 9D C4 44 97 AB 37 A7
           E8 21 90 A4 35 84 2D AC E9 4D A4 9A 8E FB 08 20 7E F2 58 B9
           0C A9 F8 74 C7 59 BF 1E FD 0C 73 17 D4 7F B4 1F 10 10 AF C5
           D0 21 30 B0 4A DB D3 A6 6E 20 4F E4 EA 05 76 2F F6 F5 EC 79
           31 34 02 61 06 35 9D 6D B8 FD 8D 89 27 0F A1 ED 55 8C BD 7E
           24 28 4F 49 74 7E 62 D7 F0 68 1D CF E1 0B 70 46 DC E0 84 80
           80 CA F7 F0 C4 0B 91 6A 0D C6 E7 E9 BC 34 EA EA 94 E4 2D 71
           16 7B 28 12 08 51 55 75 50 45 18 E1 F2 E4 48 4A 9C 1F 33 93
           71 9B 9E CF 5A A9 61 1C FB 0D 89 94 C3 A7 2F AA 84 43 7D BB
           EE C5 59 9D CA 09 91 88 85 AA 59 93 F3 0A 08 71 B4 AA 26  [...]
```

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: webhost

Issuer Name:

Common Name: webhost

Serial Number: 00 A7 DD 2D 14 21 F7 86 03

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jun 01 08:25:15 2023 GMT
Not Valid After: May 29 08:25:15 2033 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 FC 6F 54 C4 B9 8E DA C6 BD A6 5F 4E 7F 61 86 97 2A 37 B9
            B1 72 BC 98 3B 64 2A 3A 4C 40 5C 70 D8 AB 74 53 CE 86 E2 67
            8A C0 74 64 CD 25 39 CB EB EB EF 8F 5A 02 CE E9 FF DB 21 51
            F3 62 35 73 87 3E 31 A4 70 D6 79 91 42 64 4C 4E 04 02 01 10
            1F 7D 0C EC 26 26 52 81 77 BD A5 29 C9 4A 10 53 EA 9D E4 EE
            E4 93 F0 21 17 92 4D 85 35 48 DB 15 7A 4D D1 50 C6 6C 7E 6B
            C1 3A BC 00 A7 91 F8 8B EF D0 64 CC 4E A5 0E 37 AF BF 96 1C
            A1 AC 27 2E 12 AE BE F9 20 24 44 F6 09 EC 62 60 BB 94 E1 02
            30 FD B4 38 B4 8E 93 BF D8 E0 2F EB 07 1B FB 49 3A 22 4A B2
            DD 7C E1 73 7D EB 90 C3 0B 1A DF FD CC D9 5E B0 7F 11 36 99
            BD 90 FD 3F 15 7C 7D 71 18 41 FB 18 FA DA C5 D9 FC BD 0C F2
```

```
            32 2C 98 29 28 E2 B2 66 B5 7F C3 72 82 66 09 AE 5A A2 88 36
            85 43 74 81 1E E8 AC 83 68 1F EA AE A6 B1 E3 D5 DD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 27 4B 8F DF EE AD 27 C9 D0 7D 6A A5 9D C4 44 97 AB 37 A7
           E8 21 90 A4 35 84 2D AC E9 4D A4 9A 8E FB 08 20 7E F2 58 B9
           0C A9 F8 74 C7 59 BF 1E FD 0C 73 17 D4 7F B4 1F 10 10 AF C5
           D0 21 30 B0 4A DB D3 A6 6E 20 4F E4 EA 05 76 2F F6 F5 EC 79
           31 34 02 61 06 35 9D 6D B8 FD 8D 89 27 0F A1 ED 55 8C BD 7E
           24 28 4F 49 74 7E 62 D7 F0 68 1D CF E1 0B 70 46 DC E0 84 80
           80 CA F7 F0 C4 0B 91 6A 0D C6 E7 E9 BC 34 EA EA 94 E4 2D 71
           16 7B 28 12 08 51 55 75 50 45 18 E1 F2 E4 48 4A 9C 1F 33 93
           71 9B 9E CF 5A A9 61 1C FB 0D 89 94 C3 A7 2F AA 84 43 7D BB
           EE C5 59 9D CA 09 91 88 85 AA 59 93 F3 0A 08 71 B4 AA 26  [...]
```

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/443/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
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
    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
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
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
   SEED-SHA                      0x00, 0x96       RSA           RSA      SEED-CBC(128)
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
   RSA-AES128-SHA256              [...]
```

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 :

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

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
    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
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
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
   SEED-SHA                      0x00, 0x96       RSA           RSA      SEED-CBC(128)
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
   RSA-AES128-SHA256              [...]
```

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 :

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

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
    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
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
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
   SEED-SHA                      0x00, 0x96       RSA           RSA      SEED-CBC(128)
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
   RSA-AES128-SHA256              [...]
```

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: 2022/07/25

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 : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
    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
   DHE-RSA-SEED-SHA             0x00, 0x9A      DH            RSA      SEED-CBC(128)
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      C [...]
```

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: 2022/07/25

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

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
    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
   DHE-RSA-SEED-SHA             0x00, 0x9A      DH            RSA      SEED-CBC(128)
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      C [...]
```

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: 2022/07/25

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

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
 SHA1
    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
   DHE-RSA-SEED-SHA             0x00, 0x9A      DH            RSA      SEED-CBC(128)
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      C [...]
```

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

https://tools.ietf.org/html/rfc3749

https://tools.ietf.org/html/rfc3943

https://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/993/imap

```
Nessus was able to confirm that the following compression method is
supported by the target :

  DEFLATE (0x01)
```

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

https://tools.ietf.org/html/rfc3749

https://tools.ietf.org/html/rfc3943

https://tools.ietf.org/html/rfc5246

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/995/pop3

```
Nessus was able to confirm that the following compression method is
supported by the target :

  DEFLATE (0x01)
```

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 :

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

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            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
```

```
    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
    DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
 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

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 :

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

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            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
```

```
    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
    DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
 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

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 :

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

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            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
```

```
    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
    DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
 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

The fields above are :

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

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/443/www

```
This port supports resuming SSLv3 sessions.
```

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 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_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
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

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: 2022/04/06

Plugin Output

tcp/443/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
    ----------------------        ----------        ---           ----     ---------------------   ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
SHA1
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA      3DES-CBC(168)
SHA1

  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
    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
    DHE-RSA-SEED-SHA              0x00, 0x9A        DH            RSA      SEED-CBC(128)
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
    RC4-SHA                       0x00, 0x05        RSA           RSA      RC4(128)                SH
[...]
```

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 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_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
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

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: 2022/04/06

Plugin Output

tcp/993/imap

```
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
    ----------------------        ----------        ---           ----     ---------------------   ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA      3DES-CBC(168)
SHA1
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA      3DES-CBC(168)
SHA1

  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
    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
    DHE-RSA-SEED-SHA              0x00, 0x9A        DH            RSA      SEED-CBC(128)
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
    RC4-MD5                       0x00, 0x04        RSA           RSA      RC4(128)                MD
[...]
```

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 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_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
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

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: 2022/04/06

Plugin Output

tcp/995/pop3

```
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
    ----------------------        ----------       ---           ----     --------------------   ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

  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
    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
    DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
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
    RC4-MD5                       0x00, 0x04       RSA           RSA      RC4(128)               MD
[...]
```

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: 2023/03/29

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: 2023/03/29

Plugin Output

tcp/22/ssh

```
An SSH 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: 2023/03/29

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: 2023/03/29

Plugin Output

tcp/443/www

```
A TLSv1 server answered on this port.
```

tcp/443/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: 2023/03/29

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: 2023/03/29

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.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

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/443/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/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.
```

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.
```

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: 2023/02/13

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: 2023/05/03

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.0.2.15 to 10.0.2.4 :
10.0.2.15
10.0.2.4

Hop Count: 1
```