tenable Nessus

My Basic Network Scan

Report generated by Nessus™ Mon, 16 Oct 2023 23:22:47 India Standard Time

Vulnerabilities by Plugin

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Vulnerabilities by Plugin

42873 (1) - 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

217.21.87.11 (tcp/21/ftp)

```
  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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     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}
```

31705 (1) - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?3a040ada

Solution

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

Risk Factor

Low

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

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	28482
CVE	CVE-2007-1858

Plugin Information

Published: 2008/03/28, Modified: 2021/02/03

Plugin Output

217.21.87.11 (tcp/21/ftp)

```

The following is a list of SSL anonymous ciphers supported by the remote TCP server :

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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    AECDH-AES128-SHA              0xC0, 0x18       ECDH          None     AES-CBC(128)
 SHA1
    AECDH-AES256-SHA              0xC0, 0x19       ECDH          None     AES-CBC(256)
 SHA1
    AECDH-RC4-SHA                 0xC0, 0x16       ECDH          None     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 (1) - 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

4.4

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

3.7 (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

217.21.87.11 (tcp/21/ftp)

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-RC4-SHA             0xC0, 0x11       ECDH          RSA      RC4(128)
 SHA1
    AECDH-RC4-SHA                 0xC0, 0x16       ECDH          None     RC4(128)
 SHA1
    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}
```

104743 (1) - 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

217.21.87.11 (tcp/21/ftp)

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

157288 (1) - 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

217.21.87.11 (tcp/21/ftp)

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

22964 (6) - 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: 2023/07/10

Plugin Output

217.21.87.11 (tcp/21/ftp)

```
An FTP server is running on this port.
```

217.21.87.11 (tcp/80/www)

```
A web server is running on this port.
```

217.21.87.11 (tcp/443/www)

```
A TLSv1.2 server answered on this port.
```

217.21.87.11 (tcp/443/www)

```
A web server is running on this port through TLSv1.2.
```

217.21.87.11 (tcp/8443/www)

```
A TLSv1.2 server answered on this port.
```

217.21.87.11 (tcp/8443/www)

```
A web server is running on this port through TLSv1.2.
```

11219 (4) - 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: 2023/09/25

Plugin Output

217.21.87.11 (tcp/21/ftp)

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

217.21.87.11 (tcp/80/www)

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

217.21.87.11 (tcp/443/www)

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

217.21.87.11 (tcp/8443/www)

```
Port 8443/tcp was found to be open
```

10107 (3) - 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

217.21.87.11 (tcp/80/www)

```
The remote web server type is :

LiteSpeed
```

217.21.87.11 (tcp/443/www)

```
The remote web server type is :

LiteSpeed
```

217.21.87.11 (tcp/8443/www)

```
The remote web server type is :

openresty
```

10863 (3) - 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

217.21.87.11 (tcp/21/ftp)

```
Subject Name:

Common Name: *.hstgr.io

Issuer Name:

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

Serial Number: 00 90 AE EC 1F C1 50 7F 01 4C 5E 0E 29 88 BD 97 41

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 13 00:00:00 2023 GMT
Not Valid After: Aug 11 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 BB 8A D2 92 5C 05 0B B1 36 54 2F AB 65 4F A9 BA 42 61 5C
            19 55 E4 E3 02 C3 71 F3 76 6D 61 A2 75 D2 C0 6E 1F 4E 27 B5
            C4 DA 50 2D 09 42 2F 00 34 5D 6B 5E 87 F6 59 37 01 CA 03 F2
            61 8C 32 C4 91 61 34 04 32 C9 A5 FA B8 0C 9F 18 B2 58 48 EB
            CF C1 BA 78 38 1C 55 83 86 FD 4C 6C B7 34 A3 E0 C0 4A B2 6D
            BD 79 36 30 EA 0E DB F3 56 F3 4D DF 9C 2C 2D 28 4C 63 58 F3
```

```
             DF C2 B4 4C E6 D9 CA 28 73 45 92 34 B8 B3 48 BB 8F EC CD 75
             A2 E4 0A 51 80 96 01 55 69 03 CB A0 35 AE 75 BE FD 58 A1 84
             EC 30 DA 70 23 0D E1 E1 01 9E F5 C7 4D B4 95 23 F6 1E F9 14
             E4 C4 58 AD 74 F0 DD E6 92 FE 1D 77 1A E9 A0 A0 01 11 D0 90
             86 28 EB 66 9E 23 80 A8 10 00 66 31 A8 51 56 DB D0 75 37 C5
             10 23 53 05 85 9F EE 3D B1 21 E3 5E F0 50 B9 A4 BD BA 5D 23
             34 E5 A8 8B 05 DC 19 97 91 F0 61 34 75 2D 36 7D 7A 8F B4 61
             AE E9 92 3E F4 77 46 F1 D9 1B A2 B4 57 F7 CC 74 DC 76 31 74
             09 5E 71 19 93 B0 31 EF D9 AE A5 0D 32 83 0C 50 62 A9 E3 D2
             F6 1D D2 FB FE E5 FF 76 10 41 30 BF 19 F3 DE AD 3E D7 F9 BC
             44 83 96 EF E3 66 0B 24 D9 26 D8 34 DC 67 CF 60 29 BE 48 FE
             BA 63 C0 43 3D D9 81 FB C2 C1 E1 B6 6D 5A F9 9B B9 B4 61 61
             76 3D 35 B7 A0 D7 A6 DD E3 0B E6 05 C0 73 F0 57 F9 56 19 F8
             4D 8B 0E 03 14 B6 59 E2 D0 06 9A 73 59 46 C6 A9 34 A3 0A 72
             54 1A 4D 17 F8 BA AA 89 7A BD F7 65 B3 EB 3A 89 B8 15 F1 8D
             F3 01 DD  [...]
```

217.21.87.11 (tcp/443/www)

```
Subject Name:

Common Name: *.hstgr.io

Issuer Name:

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

Serial Number: 00 90 AE EC 1F C1 50 7F 01 4C 5E 0E 29 88 BD 97 41

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 13 00:00:00 2023 GMT
Not Valid After: Aug 11 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 BB 8A D2 92 5C 05 0B B1 36 54 2F AB 65 4F A9 BA 42 61 5C
            19 55 E4 E3 02 C3 71 F3 76 6D 61 A2 75 D2 C0 6E 1F 4E 27 B5
            C4 DA 50 2D 09 42 2F 00 34 5D 6B 5E 87 F6 59 37 01 CA 03 F2
            61 8C 32 C4 91 61 34 04 32 C9 A5 FA B8 0C 9F 18 B2 58 48 EB
            CF C1 BA 78 38 1C 55 83 86 FD 4C 6C B7 34 A3 E0 C0 4A B2 6D
            BD 79 36 30 EA 0E DB F3 56 F3 4D DF 9C 2C 2D 28 4C 63 58 F3
            DF C2 B4 4C E6 D9 CA 28 73 45 92 34 B8 B3 48 BB 8F EC CD 75
            A2 E4 0A 51 80 96 01 55 69 03 CB A0 35 AE 75 BE FD 58 A1 84
            EC 30 DA 70 23 0D E1 E1 01 9E F5 C7 4D B4 95 23 F6 1E F9 14
            E4 C4 58 AD 74 F0 DD E6 92 FE 1D 77 1A E9 A0 A0 01 11 D0 90
            86 28 EB 66 9E 23 80 A8 10 00 66 31 A8 51 56 DB D0 75 37 C5
            10 23 53 05 85 9F EE 3D B1 21 E3 5E F0 50 B9 A4 BD BA 5D 23
            34 E5 A8 8B 05 DC 19 97 91 F0 61 34 75 2D 36 7D 7A 8F B4 61
            AE E9 92 3E F4 77 46 F1 D9 1B A2 B4 57 F7 CC 74 DC 76 31 74
            09 5E 71 19 93 B0 31 EF D9 AE A5 0D 32 83 0C 50 62 A9 E3 D2
            F6 1D D2 FB FE E5 FF 76 10 41 30 BF 19 F3 DE AD 3E D7 F9 BC
            44 83 96 EF E3 66 0B 24 D9 26 D8 34 DC 67 CF 60 29 BE 48 FE
            BA 63 C0 43 3D D9 81 FB C2 C1 E1 B6 6D 5A F9 9B B9 B4 61 61
            76 3D 35 B7 A0 D7 A6 DD E3 0B E6 05 C0 73 F0 57 F9 56 19 F8
            4D 8B 0E 03 14 B6 59 E2 D0 06 9A 73 59 46 C6 A9 34 A3 0A 72
            54 1A 4D 17 F8 BA AA 89 7A BD F7 65 B3 EB 3A 89 B8 15 F1 8D
            F3 01 DD  [...]
```

217.21.87.11 (tcp/8443/www)

```
Subject Name:

Common Name: *.hstgr.io

Issuer Name:

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

Serial Number: 00 90 AE EC 1F C1 50 7F 01 4C 5E 0E 29 88 BD 97 41

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 13 00:00:00 2023 GMT
Not Valid After: Aug 11 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 BB 8A D2 92 5C 05 0B B1 36 54 2F AB 65 4F A9 BA 42 61 5C
            19 55 E4 E3 02 C3 71 F3 76 6D 61 A2 75 D2 C0 6E 1F 4E 27 B5
            C4 DA 50 2D 09 42 2F 00 34 5D 6B 5E 87 F6 59 37 01 CA 03 F2
            61 8C 32 C4 91 61 34 04 32 C9 A5 FA B8 0C 9F 18 B2 58 48 EB
            CF C1 BA 78 38 1C 55 83 86 FD 4C 6C B7 34 A3 E0 C0 4A B2 6D
            BD 79 36 30 EA 0E DB F3 56 F3 4D DF 9C 2C 2D 28 4C 63 58 F3
            DF C2 B4 4C E6 D9 CA 28 73 45 92 34 B8 B3 48 BB 8F EC CD 75
            A2 E4 0A 51 80 96 01 55 69 03 CB A0 35 AE 75 BE FD 58 A1 84
            EC 30 DA 70 23 0D E1 E1 01 9E F5 C7 4D B4 95 23 F6 1E F9 14
            E4 C4 58 AD 74 F0 DD E6 92 FE 1D 77 1A E9 A0 A0 01 11 D0 90
            86 28 EB 66 9E 23 80 A8 10 00 66 31 A8 51 56 DB D0 75 37 C5
            10 23 53 05 85 9F EE 3D B1 21 E3 5E F0 50 B9 A4 BD BA 5D 23
            34 E5 A8 8B 05 DC 19 97 91 F0 61 34 75 2D 36 7D 7A 8F B4 61
            AE E9 92 3E F4 77 46 F1 D9 1B A2 B4 57 F7 CC 74 DC 76 31 74
            09 5E 71 19 93 B0 31 EF D9 AE A5 0D 32 83 0C 50 62 A9 E3 D2
            F6 1D D2 FB FE E5 FF 76 10 41 30 BF 19 F3 DE AD 3E D7 F9 BC
            44 83 96 EF E3 66 0B 24 D9 26 D8 34 DC 67 CF 60 29 BE 48 FE
            BA 63 C0 43 3D D9 81 FB C2 C1 E1 B6 6D 5A F9 9B B9 B4 61 61
            76 3D 35 B7 A0 D7 A6 DD E3 0B E6 05 C0 73 F0 57 F9 56 19 F8
            4D 8B 0E 03 14 B6 59 E2 D0 06 9A 73 59 46 C6 A9 34 A3 0A 72
            54 1A 4D 17 F8 BA AA 89 7A BD F7 65 B3 EB 3A 89 B8 15 F1 8D
            F3 01 DD  [...]
```

21643 (3) - 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: 2023/07/10

Plugin Output

217.21.87.11 (tcp/21/ftp)

```

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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     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
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
 SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA    [...]
```

217.21.87.11 (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
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1

The fields above are :

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

217.21.87.11 (tcp/8443/www)

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
```

```
 High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption             MAC
   ----------------------        ----------       ---           ----     ---------------------  ---
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76       ECDH          RSA      Camellia-CBC(128)
SHA256
   ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77       ECDH          RSA      Camellia-CBC(256)
SHA384
   ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
SHA256
   RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
AEAD
   RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
AEAD
   RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
AEAD
   RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
AEAD
   RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA             [...]
```

56984 (3) - 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: 2023/07/10

Plugin Output

217.21.87.11 (tcp/21/ftp)

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

217.21.87.11 (tcp/443/www)

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

217.21.87.11 (tcp/8443/www)

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

57041 (3) - 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

217.21.87.11 (tcp/21/ftp)

```

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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    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
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-RC4-SHA             0xC0, 0x11       ECDH          RSA      RC4(128)
 SHA1
    DHE-RSA-AES128-SHA256      [...]
```

217.21.87.11 (tcp/443/www)

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1

The fields above are :

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

217.21.87.11 (tcp/8443/www)

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
```

```
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76       ECDH          RSA      Camellia-CBC(128)
 SHA256
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77       ECDH          RSA      Camellia-CBC(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

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

70544 (3) - 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

217.21.87.11 (tcp/21/ftp)

```
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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     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
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AECDH-AES128-SHA              0xC0, 0x18       ECDH          None     AES-CBC(128)
 SHA1
    AECDH-AES256-SHA              0xC0, 0x19       ECDH          None     AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00 [...]
```

217.21.87.11 (tcp/443/www)

```
Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1

The fields above are :

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

217.21.87.11 (tcp/8443/www)

```
Here is the list of SSL CBC ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76       ECDH          RSA      Camellia-CBC(128)
 SHA256
```

```
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77       ECDH          RSA      Camellia-CBC(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
 SHA1
    CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256
    RSA-CAMELLIA128-SHA256        0x00, 0xBA       RSA           RSA      Camellia-CBC(128)
 SHA256
    RSA-CAMELLIA256-SHA256        0x00, 0xC0       RSA           RSA      Camellia-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}
```

94761 (3) - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

217.21.87.11 (tcp/21/ftp)

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

217.21.87.11 (tcp/443/www)

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
```

```
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

217.21.87.11 (tcp/8443/www)

```


The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

95631 (3) - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

217.21.87.11 (tcp/21/ftp)

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

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgc
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

217.21.87.11 (tcp/443/www)

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

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgc
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

217.21.87.11 (tcp/8443/www)

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

```
Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgc
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

136318 (3) - 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

217.21.87.11 (tcp/21/ftp)

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

217.21.87.11 (tcp/443/www)

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

217.21.87.11 (tcp/8443/www)

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

156899 (3) - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 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: 2023/07/10

Plugin Output

217.21.87.11 (tcp/21/ftp)

```
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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     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
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-RC4-SHA             0xC0, 0x11       ECDH          RSA      RC4(128)               SH
 [...]
```

217.21.87.11 (tcp/443/www)

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
```

```
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1

The fields above are :

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

217.21.87.11 (tcp/8443/www)

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76       ECDH          RSA      Camellia-CBC(128)
 SHA256
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77       ECDH          RSA      Camellia-CBC(256)
 SHA384
    RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
 AEAD
    RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
 AEAD
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
 AEAD
    RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
 AEAD
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
 SHA1
    CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RS [...]
```

62564 (2) - TLS Next Protocols Supported

Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

https://technotes.googlecode.com/git/nextprotoneg.html

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

217.21.87.11 (tcp/21/ftp)

```

The target advertises that the following protocols are
supported over SSL / TLS:

  ftp
```

217.21.87.11 (tcp/8443/www)

```

The target advertises that the following protocols are
supported over SSL / TLS:

  h2
  http/1.1
```

84502 (2) - 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

217.21.87.11 (tcp/443/www)

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

217.21.87.11 (tcp/8443/www)

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

84821 (2) - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2023/07/10

Plugin Output

217.21.87.11 (tcp/443/www)

```
http/1.1
h2
```

217.21.87.11 (tcp/8443/www)

```
http/1.1
h2
```

87242 (2) - TLS NPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS NPN extension.

Description

The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-03.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/12/08, Modified: 2023/07/10

Plugin Output

217.21.87.11 (tcp/21/ftp)

```
NPN Supported Protocols:

  ftp
```

217.21.87.11 (tcp/8443/www)

```
NPN Supported Protocols:

  h2
  http/1.1
```

10092 (1) - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

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

Solution

n/a

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

217.21.87.11 (tcp/21/ftp)

```

The remote FTP banner is :

220 FTP Server ready.
```

10114 (1) - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

217.21.87.11 (icmp/0)

```
The difference between the local and remote clocks is -30 seconds.
```

10287 (1) - 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: 2023/06/26

Plugin Output

217.21.87.11 (udp/0)

```
For your information, here is the traceroute from 192.168.0.100 to 217.21.87.11 :
192.168.0.100

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.
192.168.0.1
10.230.192.1
?
136.232.112.109
172.16.25.116
172.16.1.220
182.79.206.229
116.119.44.224
?
217.21.87.11
?
217.21.87.11

Hop Count: 15
```

11936 (1) - 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

217.21.87.11 (tcp/0)

```

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


The remote host is running Linux Kernel 2.6
```

19506 (1) - 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: 2023/07/31

Plugin Output

217.21.87.11 (tcp/0)

```
Information about this scan :

Nessus version : 10.6.1
Nessus build : 20021
Plugin feed version : 202310161413
Scanner edition used : Nessus
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.0.100
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 139.717 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 : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/10/16 23:01 India Standard Time
Scan duration : 1264 sec
Scan for malware : no
```

24260 (1) - 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

217.21.87.11 (tcp/8443/www)

```

Response Code : HTTP/1.1 200 OK

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

  Server: openresty
  Date: Mon, 16 Oct 2023 17:38:56 GMT
  Content-Type: text/html
  Content-Length: 649
  Last-Modified: Thu, 16 May 2019 23:47:35 GMT
  Connection: keep-alive
  ETag: "5cddf697-289"
  Accept-Ranges: bytes

Response Body :

<!DOCTYPE html>
<html>
<head>
<title>Welcome to OpenResty!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to OpenResty!</h1>
<p>If you see this page, the OpenResty web platform is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="https://openresty.org/">openresty.org</a>.<br/>
Commercial support is available at
<a href="https://openresty.com/">openresty.com</a>.</p>

<p><em>Thank you for flying OpenResty.</em></p>
</body>
</html>
```

25220 (1) - 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

217.21.87.11 (tcp/0)

42149 (1) - FTP Service AUTH TLS Command Support

Synopsis

The remote directory service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/15, Modified: 2022/02/11

Plugin Output

217.21.87.11 (tcp/21/ftp)

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

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

Common Name: *.hstgr.io

Issuer Name:

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

Serial Number: 00 90 AE EC 1F C1 50 7F 01 4C 5E 0E 29 88 BD 97 41

Version: 3
```

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

Not Valid Before: Jul 13 00:00:00 2023 GMT
Not Valid After: Aug 11 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 BB 8A D2 92 5C 05 0B B1 36 54 2F AB 65 4F A9 BA 42 61 5C
            19 55 E4 E3 02 C3 71 F3 76 6D 61 A2 75 D2 C0 6E 1F 4E 27 B5
            C4 DA 50 2D 09 42 2F 00 34 5D 6B 5E 87 F6 59 37 01 CA 03 F2
            61 8C 32 C4 91 61 34 04 32 C9 A5 FA B8 0C 9F 18 B2 58 48 EB
            CF C1 BA 78 38 1C 55 83 86 FD 4C 6C B7 34 A3 E0 C0 4A B2 6D
            BD 79 36 30 EA 0E DB F3 56 F3 4D DF 9C 2C 2D 28 4C 63 58 F3
            DF C2 B4 4C E6 D9 CA 28 73 45 92 34 B8 B3 48 BB 8F EC CD 75
            A2 E4 0A 51 80 96 01 55 69 03 CB A0 35 AE 75 BE FD 58 A1 84
            EC 30 DA 70 23 0D E1 E1 01 9E F5 C7 4D B4 95 23 F6 1E F9 14
            E4 C4 58 AD 74 F0 DD E6 92 FE 1D 77 1A E9 A0 A0 01 11 D0 90
            86 28 EB 66 9E 23 80 A8 10 00 66 31 A8 51 56 DB D0 75 37 C5
            10 23 53 05 85 9F EE 3D B1 21 E3 5E F0 50 B9 A4 BD BA 5D 23
            34 E5 A8 8B 05 DC 19 97 91 F0 61 34 75 2D 36 7D 7A 8F B4 61
            AE E9 92 3E F4 77 46 F1 D9 1B A2 B4 57 F7 CC 74 DC 76 31 74
            09 5E 71 19 93 B0 31 EF D9 AE A5 0D 32 83 0C 50 62 A9 E3 D2
            F6 1D D2 FB FE E5 FF 76 10 41 30 BF 19 F3 DE AD 3E D7 F9 BC
            44 83 96 EF E3 66 0B 24 D9 26 D8 34 DC 67 CF 60 29 BE 48 FE
            BA 63 C0 43 3D D9 81 FB C2 C1 E1 B6 6D 5A F9 9B B9 B4 61 61
            76 3D 35 B7 A0 D7 A6 DD E3 0B E6 05 C0 73 F0 57 F [...]
```

45590 (1) - 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: 2023/09/25

Plugin Output

217.21.87.11 (tcp/0)

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

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

50845 (1) - 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

217.21.87.11 (tcp/21/ftp)

54615 (1) - 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

217.21.87.11 (tcp/0)

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

121010 (1) - 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

217.21.87.11 (tcp/21/ftp)

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

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations