The Smartbridge

Report generated by Nessus™ Wed, 28 Jun 2023 18:59:11 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.186.199.228.....4

Vulnerabilities by Host

192.186.199.228

0	5	21	27	192
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Jun 28 17:22:28 2023
End time: Wed Jun 28 18:59:11 2023

Host Information

DNS Name: 228.199.186.192.host.secureserver.net
IP: 192.186.199.228
OS: Linux Kernel 2.6

Vulnerabilities

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/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
    ADH-DES-CBC3-SHA              0x00, 0x1B        DH            None     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}
```

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/110/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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          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/143/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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          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: "c0020-7ab-5887b86c63c28"
  Inode number           : 786464
  File size              : 1963 bytes
  File modification time : May.  9, 2019 at 21:56:47 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: "c0020-7ab-5887b86c63c28"
  Inode number          : 786464
  File size             : 1963 bytes
  File modification time : May.  9, 2019 at 21:56:47 GMT
```

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

31705 - 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

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
    ----------------------        ----------        ---           ----     ---------------------   ---
    ADH-DES-CBC3-SHA              0x00, 0x1B        DH            None     3DES-CBC(168)
 SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17        ECDH          None     3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    DH-AES128-SHA256              0x00, 0xA6        DH            None     AES-GCM(128)
 SHA256
    DH-AES256-SHA384              0x00, 0xA7        DH            None     AES-GCM(256)
 SHA384
    ADH-AES128-SHA                0x00, 0x34        DH            None     AES-CBC(128)
 SHA1
    ADH-AES256-SHA                0x00, 0x3A        DH            None     AES-CBC(256)
 SHA1
    ADH-CAMELLIA128-SHA           0x00, 0x46        DH            None     Camellia-CBC(128)
 SHA1
    ADH-CAMELLIA256-SHA           0x00, 0x89        DH            None     Camellia-CBC(256)
 SHA1
    ADH-RC4-MD5                   0x00, 0x18        DH            None     RC4(128)                MD5
    ADH-SEED-SHA                  0x00, 0x9B        DH            None     SEED-CBC(128)
 SHA1
    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
    DH-AES128-SHA256              0x00, 0x6C        DH            None     AES-CBC(128)
 SHA256
    DH-AES256-SH [...]
```

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/21/ftp

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

  High Strength Ciphers (>= 112-bit key)

    Name                        Code              KEX           Auth     Encryption              MAC
    ------------------------    ----------        ---           ----     ---------------------   ---
    ADH-RC4-MD5                 0x00, 0x18        DH            None     RC4(128)                MD5
    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 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/110/pop3

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

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/143/imap

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

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/993/imap

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

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/995/pop3

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

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/2078/www

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

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/2080/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/2083/www

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

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/2096/www

```
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/110/pop3

```
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/143/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/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.
```

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/2078/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/2080/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/2083/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/2096/www

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

42085 - IMAP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

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

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

Common Name: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3
```

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

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
            11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
            EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
            70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
            7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
            6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
            8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
            F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E [...]
```

42087 - POP3 Service STLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/110/pop3

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

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

Common Name: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3
```

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

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
            11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
            EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
            70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
            7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
            6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
            8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
            F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B [...]
```

54582 - SMTP Service Cleartext Login Permitted

Synopsis

The remote mail server allows cleartext logins.

Description

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

See Also

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

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

Solution

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

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/587/smtp

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

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

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

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

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

VPR Score

2.5

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	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2018/07/30

Plugin Output

tcp/22/ssh

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

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

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

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

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/21/ftp

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/110/pop3

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/143/imap

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/443/www

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/993/imap

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/995/pop3

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/2078/www

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/2080/www

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/2083/www

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/2096/www

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

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/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
    ADH-DES-CBC3-SHA              0x00, 0x1B        DH            None     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
    ----------------------        ----------        ---           ----     ---------------------  ---
    DH-AES128-SHA256              0x00, 0xA6        DH            None     AES-GCM(128)
SHA256
    DH-AES256-SHA384              0x00, 0xA7        DH            None     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)
[...]
```

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/110/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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          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
    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
    DHE-RSA-AES128-SHA256         0x00, 0x67        DH            RSA      AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B        DH            RSA      AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDH          RSA      AES-CBC(128)
[...]
```

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/143/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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          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
    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
    DHE-RSA-AES128-SHA256         0x00, 0x67        DH            RSA      AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B        DH            RSA      AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDH          RSA      AES-CBC(128)
[...]
```

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:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E        DH            RSA      AES-CCM(128)
AEAD
    DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2        DH            RSA      AES-CCM8(128)
AEAD
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F        DH            RSA      AES-CCM(256)
AEAD
    DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3        DH            RSA      AES-CCM8(256)
AEAD
    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
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45        DH            RSA      Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88        DH            RSA      Camellia-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH    [...]
```

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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          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
    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
    DHE-RSA-AES128-SHA256         0x00, 0x67        DH            RSA      AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B        DH            RSA      AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDH          RSA      AES-CBC(128)
[...]
```

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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          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
    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
    DHE-RSA-AES128-SHA256         0x00, 0x67        DH            RSA      AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B        DH            RSA      AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDH          RSA      AES-CBC(128)
[...]
```

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/2078/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
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
SHA256

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

- 0x13,0x01 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/2080/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
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
SHA1
    AES128-SHA                    0x00, 0x2F        RSA           RSA      AES-CBC(128)
SHA1
    AES256-SHA                    0x00, 0x35        RSA           RSA      AES-CBC(256)
SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67        DH            RSA      AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B        DH            RSA      AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDH          RSA      AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
SHA384
    RSA-AES128-SHA256             0x00, 0x3C        RSA           RSA      AES-CBC(128)
SHA256
    RSA-AES256-SHA256             0x00, 0x3D        RSA           RSA      AES-CBC(256)
SHA256

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

- 0x13,0x01 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/2083/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
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F        RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35        RSA           RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67        DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B        DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C        RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D        RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

- 0x13,0x01 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/2096/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
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
SHA1
    AES128-SHA                    0x00, 0x2F        RSA           RSA      AES-CBC(128)
SHA1
    AES256-SHA                    0x00, 0x35        RSA           RSA      AES-CBC(256)
SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67        DH            RSA      AES-CBC(128)
SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B        DH            RSA      AES-CBC(256)
SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDH          RSA      AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA      AES-CBC(256)
SHA384
    RSA-AES128-SHA256             0x00, 0x3C        RSA           RSA      AES-CBC(128)
SHA256
    RSA-AES256-SHA256             0x00, 0x3D        RSA           RSA      AES-CBC(256)
SHA256

The fields above are :

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

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
http/1.1
h2
```

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://228.199.186.192.host.secureserver.net/
Version    : unknown
Source     : Server: Apache
backported : 0
```

48204 - Apache HTTP Server Version

Synopsis

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

Description

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

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

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

Plugin Output

tcp/443/www

```
URL        : https://228.199.186.192.host.secureserver.net/
Version    : unknown
Source     : Server: Apache
backported : 0
```

166602 - Asset Attribute: Fully Qualified Domain Name (FQDN)

Synopsis

Report Fully Qualified Domain Name (FQDN) for the remote host.

Description

Report Fully Qualified Domain Name (FQDN) for the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/10/27, Modified: 2022/10/27

Plugin Output

tcp/0

```
The FQDN for the remote host has been determined to be:

  FQDN       : 228.199.186.192.host.secureserver.net
  Confidence : 100
  Resolves   : True
  Method     : rDNS Lookup: IP Address

Another possible FQDN was also detected:
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

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

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

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2023/06/20

Plugin Output

tcp/0

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

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

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server -> Apache Software Foundation Apache HTTP Server
  cpe:/a:mysql:mysql:5.6.51-cll-lve -> MySQL MySQL
  cpe:/a:openbsd:openssh:5.3 -> OpenBSD OpenSSH
```

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 : unknown
Confidence level : 56
```

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---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 500 allowed.
220-Local time is now 04:58. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 15 minutes of inactivity.
```

42149 - FTP Service AUTH TLS Command Support

Synopsis

The remote directory service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/21/ftp

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/443/www

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/2078/www

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/2080/www

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/2083/www

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/2096/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 :

    /
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2078/www

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

  - HTTP methods  COPY  DELETE  GET  HEAD  LOCK  MKCOL  MOVE  OPTIONS
     PROPFIND  PROPPATCH  PUT  UNLOCK 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
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/443/www

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/2078/www

```
The remote web server type is :

cPanel
```

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/2080/www

```
The remote web server type is :

cPanel
```

85805 - HTTP/2 Cleartext Detection

Synopsis

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

Description

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

See Also

https://http2.github.io/

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

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

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
192.186.199.228 resolves as 228.199.186.192.host.secureserver.net.
```

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: Wed, 28 Jun 2023 12:55:46 GMT
  Server: Apache
  Upgrade: h2,h2c
  Connection: Upgrade, Keep-Alive
  Last-Modified: Thu, 09 May 2019 21:56:47 GMT
  ETag: "c0020-7ab-5887b86c63c28"
  Accept-Ranges: bytes
  Content-Length: 1963
  Vary: Accept-Encoding
  Cache-Control: no-cache, no-store, must-revalidate
  Pragma: no-cache
  Expires: 0
  Keep-Alive: timeout=5
  Content-Type: text/html

Response Body :

<!DOCTYPE html>
<html>
```

```
<head>
<title>Coming Soon</title>
<meta http-equiv="content-type" content="text/html; charset=utf-8" >
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<style type="text/css">
body {
  /*background: linear-gradient(90deg, white, gray);*/
  background-color: #eee;
}

body, h1, p {
  font-family: "Helvetica Neue", "Segoe UI", Segoe, Helvetica, Arial, "Lucida Grande", sans-serif;
  font-weight: normal;
  margin: 0;
  padding: 0;
  text-align: center;
}

.container {
  margin-left:  auto;
  margin-right:  auto;
  margin-top: 177px;
  max-width: 1170px;
  padding-right: 15px;
  padding-left: 15px;
}

.row:before, .row:after {
  display: table;
  content: " ";
}

h1 {
  font-size: 48px;
  font-weight: 300;
  margin: 0 0 20px 0;
}

.lead {
  font-size: 21px;
  font-weight: 200;
  margin-bottom: 20px;
}

p {
  margin: 0 0 10px;
}

a {
  color: #3282e6;
  text-decoration: none;
}
</style>
</head>

<body>
<div class="container text-center" id="error">

  <svg height="100" width="100">
    <circle cx="50" cy="50" r="31" stroke="#679b08" stroke-width="9.5" fill="none" />
    <circle cx="50" cy="50" r="6" stroke="#679b08" stroke-width="1" fill="#679b08" />
    <line x1="50" y1="50" x2="35" y2="50" style="stroke:#679b08;stroke-width:6" />
    <line x1="65" y1="35" x2="50" y2="50" style="stroke:#679b08;stroke-width:6" />
    <path d="M59 65 L83 65 L75 87 Z" fill="#679b08" />
    <rect width="20" height="9" x="70" y="56" style="fill:#eee;stroke-wi [...]
```

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: Wed, 28 Jun 2023 12:55:43 GMT
  Server: Apache
  Upgrade: h2,h2c
  Connection: Upgrade, Keep-Alive
  Last-Modified: Thu, 09 May 2019 21:56:47 GMT
  ETag: "c0020-7ab-5887b86c63c28"
  Accept-Ranges: bytes
  Content-Length: 1963
  Vary: Accept-Encoding
  Cache-Control: no-cache, no-store, must-revalidate
  Pragma: no-cache
  Expires: 0
  Keep-Alive: timeout=5
  Content-Type: text/html

Response Body :

<!DOCTYPE html>
<html>
```

```
<head>
<title>Coming Soon</title>
<meta http-equiv="content-type" content="text/html; charset=utf-8" >
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<style type="text/css">
body {
  /*background: linear-gradient(90deg, white, gray);*/
  background-color: #eee;
}

body, h1, p {
  font-family: "Helvetica Neue", "Segoe UI", Segoe, Helvetica, Arial, "Lucida Grande", sans-serif;
  font-weight: normal;
  margin: 0;
  padding: 0;
  text-align: center;
}

.container {
  margin-left:  auto;
  margin-right:  auto;
  margin-top: 177px;
  max-width: 1170px;
  padding-right: 15px;
  padding-left: 15px;
}

.row:before, .row:after {
  display: table;
  content: " ";
}

h1 {
  font-size: 48px;
  font-weight: 300;
  margin: 0 0 20px 0;
}

.lead {
  font-size: 21px;
  font-weight: 200;
  margin-bottom: 20px;
}

p {
  margin: 0 0 10px;
}

a {
  color: #3282e6;
  text-decoration: none;
}
</style>
</head>

<body>
<div class="container text-center" id="error">

  <svg height="100" width="100">
    <circle cx="50" cy="50" r="31" stroke="#679b08" stroke-width="9.5" fill="none" />
    <circle cx="50" cy="50" r="6" stroke="#679b08" stroke-width="1" fill="#679b08" />
    <line x1="50" y1="50" x2="35" y2="50" style="stroke:#679b08;stroke-width:6" />
    <line x1="65" y1="35" x2="50" y2="50" style="stroke:#679b08;stroke-width:6" />
    <path d="M59 65 L83 65 L75 87 Z" fill="#679b08" />
    <rect width="20" height="9" x="70" y="56" style="fill:#eee;stroke-w [...]
```

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/2078/www

```
Response Code : HTTP/1.1 401 Unauthorized

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

  Date: Wed, 28 Jun 2023 12:55:52 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: 228.199.186.192.host.secureserver.net:2078
  Cache-Control: no-cache, no-store, must-revalidate, private
  Connection: close
  Vary: Accept-Encoding
  WWW-Authenticate: Basic realm="Restricted Area"
  Content-Length: 35
  Content-Type: text/html; charset="utf-8"
  Expires: Fri, 01 Jan 1990 00:00:00 GMT

Response Body :

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

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive 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/2080/www

```
Response Code : HTTP/1.1 401 Unauthorized

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

  Date: Wed, 28 Jun 2023 12:55:58 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: 228.199.186.192.host.secureserver.net:2080
  Cache-Control: no-cache, no-store, must-revalidate, private
  Connection: close
  Vary: Accept-Encoding
  WWW-Authenticate: Basic realm="Horde DAV Server"
  Content-Length: 35
  Content-Type: text/html; charset="utf-8"
  Expires: Fri, 01 Jan 1990 00:00:00 GMT

Response Body :

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

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive 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/2083/www

```
Response Code : HTTP/1.1 200 OK

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

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Wed, 28 Jun 2023 12:56:07 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: cpsession=%3ah4tflWS_aMc5vXGr%2c74ceebfd53c2f61a1797b826ce92307f; HttpOnly; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=228.199.186.192.host.secureserver.net;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.228.199.186.192.host.secureserver.net; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.228.199.186.192.host.secureserver.net;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
```

```
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2083; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=228.199.186.192.host.secureserver.net; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.228.199.186.192.host.secureserver.net; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2083
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.228.199.186.192.host.secureserver.net;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083
  Cache-Control: no-cache, no-store, must-revalidate, private
  Content-Length: 38276

Response Body :


<!DOCTYPE html>
<html lang="en" dir="ltr">
<hea [...]
```

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/2096/www

```
Response Code : HTTP/1.1 200 OK

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

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Wed, 28 Jun 2023 12:55:38 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: webmailsession=%3aXaFJZ0IbD80tFnBK%2c71188b4ac5a5105848ee23a03cccc08a; HttpOnly;
 path=/; port=2096; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2096; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=228.199.186.192.host.secureserver.net;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.228.199.186.192.host.secureserver.net; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.228.199.186.192.host.secureserver.net;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
```

```
 Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
port=2096; secure
 Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
secure
 Set-Cookie: imp_key=expired; HttpOnly; domain=228.199.186.192.host.secureserver.net; expires=Thu,
01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
 Set-Cookie: Horde=expired; HttpOnly; domain=.228.199.186.192.host.secureserver.net; expires=Thu,
01-Jan-1970 00:00:01 GMT; path=/; port=2096
 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.228.199.186.192.host.secureserver.net;
expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096
 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Thu, 27-Jun-2024 12:55:38 GMT; path=/;
port=2096; secure
 Cache-Control: no-cache, n [...]
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

```
The remote imap server banner is :

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

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/993/imap

```
The remote imap server banner is :

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

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0802

Plugin Information

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

Plugin Output

tcp/3306/mysql

```
Version  : 5.6.51-cll-lve
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_PASSWORD (new more secure passwords)
  CLIENT_FOUND_ROWS (Found instead of affected rows)
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_NO_SCHEMA (Don't allow database.table.column)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_ODBC (ODBC client)
  CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
  CLIENT_IGNORE_SPACE (Ignore spaces before "(")
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_INTERACTIVE (This is an interactive client)
  CLIENT_SIGPIPE (IGNORE sigpipes)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_RESERVED (Old flag for 4.1 protocol)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

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: 2023/05/31

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: 2023/05/31

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: 2023/05/31

Plugin Output

tcp/110/pop3

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

Plugin Output

tcp/143/imap

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

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: 2023/05/31

Plugin Output

tcp/465/smtp

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

Plugin Output

tcp/587/smtp

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

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: 2023/05/31

Plugin Output

tcp/995/pop3

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

Plugin Output

tcp/2077

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

Plugin Output

tcp/2078/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

Plugin Output

tcp/2080/www

```
Port 2080/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: 2023/05/31

Plugin Output

tcp/2082

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

Plugin Output

tcp/2083/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

Plugin Output

tcp/2095

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

Plugin Output

tcp/2096/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/05/31

Plugin Output

tcp/3306/mysql

```
Port 3306/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 : 202306280805
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : The Smartbridge
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.1.4
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 266.589 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 : 2023/6/28 17:22 India Standard Time
Scan duration : 5777 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 2.6
Confidence level : 56
Method : MLSinFP

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_5.3
SinFP:
   P1:B10013:F0x12:W14600:O0204ffff:M1420:
   P2:B10013:F0x12:W14480:O0204ffff0402080affffffff4445414401030309:M1420:
   P3:B00000:F0x00:W0:O0:M0
   P4:190502_7_p=443R
HTTP:!:Server: Apache

SMTP:!:220-p3plcpnl0049.prod.phx3.secureserver.net ESMTP Exim 4.95 #2 Wed, 28 Jun 2023 04:57:30
 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
500 unrecognized command
500 unrecognized command
SSLcert:!:i/CN:Starfield Secure Certificate Authority - G2i/O:Starfield Technologies, Inc.i/
OU:http://certs.starfieldtech.com/repository/s/CN:*.prod.phx3.secureserver.net
0c09249976cc8a4a6a6360d31151eaf6d98682bf
```

```
i/CN:Starfield Secure Certificate Authority - G2i/O:Starfield Technologies, Inc.i/OU:http://
certs.starfieldtech.com/repository/s/CN:*.prod.phx3.secureserver.net
0c09249976cc8a4a6a6360d31151eaf6d98682bf



The remote host is running Linux Kernel 2.6
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

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

This does not necessarily indicate a problem with the scan.

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

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

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

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

Plugin Output

tcp/0

```
The following issues were reported :

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

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

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

There are several possible reasons for this :

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

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

This might be an availability problem related to the following :

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

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

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

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

Solution

Steps to resolve this issue include :

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

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

Plugin Output

tcp/0

```
Port 465 was detected as being open but is now closed
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/110/pop3

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/993/imap

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/995/pop3

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2078/www

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2080/www

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2083/www

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2096/www

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

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

See Also

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

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/110/pop3

```
Remote POP server banner :

+OK Dovecot ready.
```

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

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

See Also

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

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/995/pop3

```
Remote POP server banner :

+OK Dovecot ready.
```

54580 - SMTP Authentication Methods

Synopsis

The remote mail server supports authentication.

Description

The remote SMTP server advertises that it supports authentication.

See Also

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/587/smtp

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

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

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

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

Solution

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

Risk Factor

None

References

XREF IAVT:0001-T-0932

Plugin Information

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

Plugin Output

tcp/465/smtp

```
Remote SMTP server banner :

220-p3plcpnl0049.prod.phx3.secureserver.net ESMTP Exim 4.95 #2 Wed, 28 Jun 2023 04:57:30 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
500 unrecognized command
500 unrecognized command
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

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

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

Solution

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

Risk Factor

None

References

XREF IAVT:0001-T-0932

Plugin Information

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

Plugin Output

tcp/587/smtp

```
Remote SMTP server banner :

220-p3plcpnl0049.prod.phx3.secureserver.net ESMTP Exim 4.95 #2 Wed, 28 Jun 2023 04:54:56 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

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

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-dss-cert-v01@openssh.com
  ssh-rsa
  ssh-rsa-cert-v01@openssh.com

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
```

```
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

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-sha2-512
  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-sha2-512
  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
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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_5.3
SSH supported authentication : publickey,password
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/21/ftp

```
The host name known by Nessus is :

  228.199.186.192.host.secureserver.net

The Common Name in the certificate is :

  *.prod.phx3.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.phx3.secureserver.net
  prod.phx3.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/110/pop3

```
The host name known by Nessus is :

  228.199.186.192.host.secureserver.net

The Common Name in the certificate is :

  *.prod.phx3.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.phx3.secureserver.net
  prod.phx3.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/143/imap

```
The host name known by Nessus is :

  228.199.186.192.host.secureserver.net

The Common Name in the certificate is :

  *.prod.phx3.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.phx3.secureserver.net
  prod.phx3.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/443/www

```
The host name known by Nessus is :

  228.199.186.192.host.secureserver.net

The Common Name in the certificate is :

  *.prod.phx3.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.phx3.secureserver.net
  prod.phx3.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/465/smtp

```
The host name known by Nessus is :

  228.199.186.192.host.secureserver.net

The Common Name in the certificate is :

  *.prod.phx3.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.phx3.secureserver.net
  prod.phx3.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/993/imap

```
The host name known by Nessus is :

  228.199.186.192.host.secureserver.net

The Common Name in the certificate is :

  *.prod.phx3.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.phx3.secureserver.net
  prod.phx3.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/995/pop3

```
The host name known by Nessus is :

  228.199.186.192.host.secureserver.net

The Common Name in the certificate is :

  *.prod.phx3.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.phx3.secureserver.net
  prod.phx3.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/2078/www

```
The host name known by Nessus is :

  228.199.186.192.host.secureserver.net

The Common Name in the certificate is :

  *.prod.phx3.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.phx3.secureserver.net
  prod.phx3.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/2080/www

```
The host name known by Nessus is :

  228.199.186.192.host.secureserver.net

The Common Name in the certificate is :

  *.prod.phx3.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.phx3.secureserver.net
  prod.phx3.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/2083/www

```
The host name known by Nessus is :

  228.199.186.192.host.secureserver.net

The Common Name in the certificate is :

  *.prod.phx3.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.phx3.secureserver.net
  prod.phx3.secureserver.net
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/2096/www

```
The host name known by Nessus is :

  228.199.186.192.host.secureserver.net

The Common Name in the certificate is :

  *.prod.phx3.secureserver.net

The Subject Alternate Names in the certificate are :

  *.prod.phx3.secureserver.net
  prod.phx3.secureserver.net
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/21/ftp

```
Subject Name:

Common Name: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
```

```
             11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
             EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
             70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
             7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
             6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
             8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
             F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B AE C8 A3 5A 15 95 81 50 56 27 B9 78
           77 C3 89 65 C2 89 6C 1E 0A 3A 00 DD 67 C9 99 0D D2 6C 0E 28
           BE 5F 77 F5 6C 3A B2 09 1E 73 29 EF 55 96 8B C1 E6 87 3 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/110/pop3

```
Subject Name:

Common Name: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
```

```
             11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
             EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
             70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
             7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
             6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
             8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
             F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B AE C8 A3 5A 15 95 81 50 56 27 B9 78
           77 C3 89 65 C2 89 6C 1E 0A 3A 00 DD 67 C9 99 0D D2 6C 0E 28
           BE 5F 77 F5 6C 3A B2 09 1E 73 29 EF 55 96 8B C1 E6 87 3 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

```
Subject Name:

Common Name: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
```

```
             11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
             EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
             70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
             7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
             6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
             8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
             F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B AE C8 A3 5A 15 95 81 50 56 27 B9 78
           77 C3 89 65 C2 89 6C 1E 0A 3A 00 DD 67 C9 99 0D D2 6C 0E 28
           BE 5F 77 F5 6C 3A B2 09 1E 73 29 EF 55 96 8B C1 E6 87 3 [...]
```

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: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
```

```
             11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
             EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
             70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
             7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
             6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
             8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
             F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B AE C8 A3 5A 15 95 81 50 56 27 B9 78
           77 C3 89 65 C2 89 6C 1E 0A 3A 00 DD 67 C9 99 0D D2 6C 0E 28
           BE 5F 77 F5 6C 3A B2 09 1E 73 29 EF 55 96 8B C1 E6 87 3 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/465/smtp

```
Subject Name:

Common Name: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
```

```
             11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
             EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
             70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
             7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
             6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
             8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
             F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B AE C8 A3 5A 15 95 81 50 56 27 B9 78
           77 C3 89 65 C2 89 6C 1E 0A 3A 00 DD 67 C9 99 0D D2 6C 0E 28
           BE 5F 77 F5 6C 3A B2 09 1E 73 29 EF 55 96 8B C1 E6 87 3 [...]
```

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: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
```

```
            11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
            EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
            70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
            7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
            6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
            8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
            F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B AE C8 A3 5A 15 95 81 50 56 27 B9 78
           77 C3 89 65 C2 89 6C 1E 0A 3A 00 DD 67 C9 99 0D D2 6C 0E 28
           BE 5F 77 F5 6C 3A B2 09 1E 73 29 EF 55 96 8B C1 E6 87 3 [...]
```

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: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
```

```
             11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
             EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
             70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
             7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
             6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
             8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
             F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B AE C8 A3 5A 15 95 81 50 56 27 B9 78
           77 C3 89 65 C2 89 6C 1E 0A 3A 00 DD 67 C9 99 0D D2 6C 0E 28
           BE 5F 77 F5 6C 3A B2 09 1E 73 29 EF 55 96 8B C1 E6 87 3 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2078/www

```
Subject Name:

Common Name: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
```

```
             11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
             EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
             70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
             7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
             6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
             8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
             F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B AE C8 A3 5A 15 95 81 50 56 27 B9 78
           77 C3 89 65 C2 89 6C 1E 0A 3A 00 DD 67 C9 99 0D D2 6C 0E 28
           BE 5F 77 F5 6C 3A B2 09 1E 73 29 EF 55 96 8B C1 E6 87 3 [...]
```

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/2080/www

```
Subject Name:

Common Name: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
```

```
             11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
             EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
             70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
             7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
             6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
             8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
             F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B AE C8 A3 5A 15 95 81 50 56 27 B9 78
           77 C3 89 65 C2 89 6C 1E 0A 3A 00 DD 67 C9 99 0D D2 6C 0E 28
           BE 5F 77 F5 6C 3A B2 09 1E 73 29 EF 55 96 8B C1 E6 87 3 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2083/www

```
Subject Name:

Common Name: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
```

```
             11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
             EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
             70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
             7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
             6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
             8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
             F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B AE C8 A3 5A 15 95 81 50 56 27 B9 78
           77 C3 89 65 C2 89 6C 1E 0A 3A 00 DD 67 C9 99 0D D2 6C 0E 28
           BE 5F 77 F5 6C 3A B2 09 1E 73 29 EF 55 96 8B C1 E6 87 3 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2096/www

```
Subject Name:

Common Name: *.prod.phx3.secureserver.net

Issuer Name:

Country: US
State/Province: Arizona
Locality: Scottsdale
Organization: Starfield Technologies, Inc.
Organization Unit: http://certs.starfieldtech.com/repository/
Common Name: Starfield Secure Certificate Authority - G2

Serial Number: 44 47 F7 EF 7B E2 49 D9

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 28 23:11:15 2023 GMT
Not Valid After: Feb 29 23:11:15 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E5 72 E9 2B 6A 8E 00 FD 9A F7 83 2F 30 61 83 83 5E 76 37
            19 E8 BB FA 39 0B 49 12 AD 50 5B 21 6D A2 3E 52 7F 44 41 01
            AE 30 AB EA 41 F8 72 5D E8 6F FF C1 CF AA 10 B5 0E 1B 6D C8
            92 88 55 EE 52 2C 4E 79 03 EF 0D 23 1E 55 13 F9 F1 F3 63 9B
            A7 90 13 A7 98 14 A6 89 2B 53 B6 34 BF 4B DA 08 82 D7 31 DF
            48 59 52 17 BF B1 39 4E 06 EB CD B1 0C 5D 18 81 9F 60 32 FF
```

```
             11 54 75 49 F9 7F 22 2B FD 26 B4 8F 65 C1 91 18 C0 3A 1D D8
             EC 7F E3 C5 AA EC 78 FF E1 4F AF 06 16 22 8A 7C B1 11 F4 0E
             70 74 7A CA A9 48 6C C2 AB 77 90 EB 55 E5 B9 7F 4D F2 D4 2C
             7C AA 08 43 39 CF 59 11 95 BA A4 A4 F6 EF 3F 7D 7F 98 D6 23
             6F 6F E7 73 1C A7 05 C2 67 D8 30 CA 8B 47 49 EB 56 03 E0 1C
             8A 1C 11 D5 29 CF 21 81 65 E1 56 D1 C6 14 BF 67 61 5E 9B D7
             F1 E2 5D 5E E7 6F E7 7E D7 6B F4 6C 63 09 AA BC F1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 8D 07 A1 11 AC 0F 1A 6E 54 E1 C2 7A A3 D6 7F 65 0A 16 14
           D8 25 01 A2 84 76 5C 46 02 ED F7 3B F5 84 6E F2 7F 4D 22 62
           B9 D9 71 0C 56 76 12 3E 14 55 BC 5D 61 26 A4 24 48 02 62 BD
           B8 E3 25 AB 8A 7F C5 6B EE 76 98 BD 9C C4 1D EB 7D 44 56 33
           CA 53 68 7A 48 13 E1 8B AE C8 A3 5A 15 95 81 50 56 27 B9 78
           77 C3 89 65 C2 89 6C 1E 0A 3A 00 DD 67 C9 99 0D D2 6C 0E 28
           BE 5F 77 F5 6C 3A B2 09 1E 73 29 EF 55 96 8B C1 E6 87 3 [...]
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/21/ftp

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

Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/110/pop3

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

Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/143/imap

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

Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/465/smtp

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

Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/993/imap

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

Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/995/pop3

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

Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/2078/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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/2080/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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/2083/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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/2096/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=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jun 29 17:39:16 2004 GMT
Valid To            : Jun 29 17:39:16 2034 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIBADANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJVUzElMCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLj
+6XGmBIWtDBFk385N78gDGIc/oav7PKaf8MOh2tTYbitTkPskpD6E8J7oX+zlJ0T1KKY/
e97gKvDIr1MvnsoFAZMej2YcOadN+lq2cwQlZut3f+dZxkqZJRRU6ybH838Z1TBwj6+wRir/
resp7defqgSHo9T5iaU0X9tDkYI22WY8sbi5gv2cOj4QyDvvBmVmepsZGD3/
cVE8MC5fvj13c7JdBmzDI1aaK4UmkhynArPkPw2vCHmCuDY96pzTNbO8acr1zJ3o/
WSNF4Azbl5KXZnJHoe0nRrA1W4TNSNe35tfPe/W93bC6j67eA0cQmdrBNj41tpvi/
JEoAGrAgEDo4HFMIHCMB0GA1UdDgQWBBS/X7fRzt0fhvRbVazc1xDCDqmI5zCBkgYDVR0jBIGKMIGHgBS/
X7fRzt0fhvRbVazc1xDCDqmI56FspGowaDELMAkGA1UEBhMCVVMxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xMjAwBgNVBA
+yz3SFmH8lU+nLMPUxA2IGvd56Deruix/U0F47ZEUD0/CwqTRV/p2JdLiXTAAsgGh1o
+Re49L2L7ShZ3U0WixeDyLJlxy16paq8U4Zt3VekyvggQQto8PT7dL5WXXp59fkdheMtlb71cZBDzI0fmgAKhynpVSJYACPq4xJDKVtHCN2MQWplBq
D5fs4C8fF5Q=
-----END CERTIFICATE-----
```

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/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
    ADH-DES-CBC3-SHA              0x00, 0x1B        DH            None     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
   ADH-AES128-SHA               0x00, 0x34       DH           None     AES-CBC(128)
SHA1
   ADH-AES256-SHA               0x00, 0x3A       DH           None     AES-CBC(256)
SHA1
   ADH-CAMELLIA128-SHA          0x00, 0x46       DH           None     Camellia-CBC(128)
SHA1
   ADH-CAMELLIA256-SHA          0x00, 0x89       DH           None     Camellia-CBC(256)
SHA1
   ADH-SEED-SHA                 0x00 [...]
```

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/110/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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          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
   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
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
SHA256
   RSA-AES256-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/143/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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          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
   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
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
SHA256
   RSA-AES256-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/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-CAMELLIA-CBC-128    0xC0, 0x76        ECDH          RSA      Camellia-CBC(128)
 SHA256
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77        ECDH          RSA      Camellia-CBC(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45        DH            RSA      Camellia-CBC(128)
 SHA1
```

```
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH           RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH         RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH         RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA          RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA          RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA          RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA          RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH           RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH           RSA      AES-CBC(256)
SHA256
   DHE-RSA-CAMELLIA128-SHA256    0x00, 0xBE       DH           RSA      Camellia-CBC(128)
SHA256
   DHE-RSA-CAMELLIA256-SHA256    0x00, 0xC4       DH           RSA      Camellia-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH         RSA      AES-CBC(128)     [...]
```

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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          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
   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
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
SHA256
   RSA-AES256-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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          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
   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
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
SHA256
   RSA-AES256-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/2078/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
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F        RSA           RSA      AES-CBC(128)
 SHA1
```

```
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

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

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/2080/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
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F        RSA           RSA      AES-CBC(128)
 SHA1
```

```
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

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

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/2083/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
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F        RSA           RSA      AES-CBC(128)
 SHA1
```

```
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

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

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/2096/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
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F        RSA           RSA      AES-CBC(128)
 SHA1
```

```
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

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

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/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
    ADH-DES-CBC3-SHA             0x00, 0x1B       DH            None     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
   DH-AES128-SHA256              0x00, 0xA6      DH           None     AES-GCM(128)
SHA256
   DH-AES256-SHA384              0x00, 0xA7      DH           None     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           RS [...]
```

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/110/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
    ECDHE-RSA-DES-CBC3-SHA       0xC0, 0x12       ECDH          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
```

```
   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
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH           RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH           RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA            RSA    [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2022/07/25

Plugin Output

tcp/143/imap

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

SSL Version : TLSv12
  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
    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
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH           RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH           RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA            RSA    [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 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
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     --------------------    ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E        DH            RSA      AES-CCM(128)
 AEAD
    DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2        DH            RSA      AES-CCM8(128)
 AEAD
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F        DH            RSA      AES-CCM(256)
 AEAD
    DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3        DH            RSA      AES-CCM8(256)
 AEAD
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    DHE-RSA-CHACHA20-POLY1305     0xCC, 0xAA        DH            RSA      ChaCha20-Poly1305(256)
 SHA256
```

```
   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   [...]
```

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
    ECDHE-RSA-DES-CBC3-SHA       0xC0, 0x12       ECDH          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
```

```
   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
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH           RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH           RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA            RSA    [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 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
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          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
```

```
   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
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH           RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH           RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA            RSA    [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2022/07/25

Plugin Output

tcp/2078/www

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

SSL Version : TLSv12
  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
   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
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
SHA384
   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/2080/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
    ----------------------       ----------        ---           ----     --------------------   ---
    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
   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
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
SHA384
   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/2083/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
    ----------------------       ----------        ---           ----     --------------------   ---
    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
   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
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
SHA384
   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/2096/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
    ----------------------       ----------        ---           ----     --------------------   ---
    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
   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
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
SHA384
   RSA-AES128-SHA256     [...]
```

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/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      [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/110/pop3

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

  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
    ECDHE-RSA-AES128-SHA           0xC0, 0x13       ECDH           RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA           0xC0, 0x14       ECDH           RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256          0x00, 0x67       DH             RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256          0x00, 0x6B       DH             RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256        0xC0, 0x27       ECDH           RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384        0xC0, 0x28       ECDH           RSA      AES-CBC(256)
 SHA384

The fields above are  [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/143/imap

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

  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
    ECDHE-RSA-AES128-SHA           0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA           0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256          0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256          0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256        0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384        0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are  [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/443/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E        DH            RSA      AES-CCM(128)
 AEAD
    DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2        DH            RSA      AES-CCM8(128)
 AEAD
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F        DH            RSA      AES-CCM(256)
 AEAD
    DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3        DH            RSA      AES-CCM8(256)
 AEAD
```

```
   DHE-RSA-AES256-SHA384         0x00, 0x9F      DH           RSA      AES-GCM(256)
SHA384
   DHE-RSA-CHACHA20-POLY1305     0xCC, 0xAA      DH           RSA      ChaCha20-Poly1305(256)
SHA256
   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
   DHE-RSA-AES128-SHA            0x00, 0x33      DH           RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39      DH           RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45      DH           RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88      DH           RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13      ECDH         RSA      AES-CBC(128) [...]
```

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
    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
    ECDHE-RSA-AES128-SHA           0xC0, 0x13       ECDH           RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA           0xC0, 0x14       ECDH           RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256          0x00, 0x67       DH             RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256          0x00, 0x6B       DH             RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256        0xC0, 0x27       ECDH           RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384        0xC0, 0x28       ECDH           RSA      AES-CBC(256)
 SHA384

The fields above are  [...]
```

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
    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
    ECDHE-RSA-AES128-SHA           0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA           0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256          0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256          0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256        0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384        0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are  [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/2078/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ----------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
```

```
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/2080/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
```

```
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/2083/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
```

```
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/2096/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
```

```
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    DHE-RSA-AES128-SHA256         0x00, 0x67       DH            RSA      AES-CBC(128)
 SHA256
    DHE-RSA-AES256-SHA256         0x00, 0x6B       DH            RSA      AES-CBC(256)
 SHA256
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

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

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/21/ftp

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

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/110/pop3

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

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

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

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/465/smtp

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

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/993/imap

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

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/995/pop3

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

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2078/www

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

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2080/www

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

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2083/www

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

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2096/www

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

|-Subject             : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Issuer              : C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification
 Authority
|-Valid From          : Jun 29 17:39:16 2004 GMT
|-Valid To            : Jun 29 17:39:16 2034 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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/110/pop3

```
A POP3 server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/03/29

Plugin Output

tcp/143/imap

```
An IMAP 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 TLSv1.2 server answered on this port.
```

tcp/443/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/03/29

Plugin Output

tcp/465/smtp

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

tcp/465/smtp

```
An SMTP server is running on this port through TLSv1.2.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/03/29

Plugin Output

tcp/587/smtp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 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.
```

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/2078/www

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

tcp/2078/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/03/29

Plugin Output

tcp/2080/www

```
A TLSv1.1 server answered on this port.
```

tcp/2080/www

```
A web server is running on this port through TLSv1.1.
```

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/2083/www

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

tcp/2083/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/03/29

Plugin Output

tcp/2096/www

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

tcp/2096/www

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

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/11/26

Plugin Output

tcp/3306/mysql

```
A MySQL server is running 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/110/pop3

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

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/143/imap

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

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/993/imap

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

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/995/pop3

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

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/2078/www

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

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/2080/www

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

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/2083/www

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

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/2096/www

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/21/ftp

```
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/110/pop3

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/143/imap

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/443/www

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/993/imap

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/995/pop3

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2078/www

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2080/www

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2083/www

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2096/www

```
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 192.168.1.4 to 192.186.199.228 :
192.168.1.4
192.168.1.1
117.245.48.1
218.248.57.242
?
182.73.147.245
116.119.73.117
62.115.42.118
62.115.124.54
62.115.112.242
62.115.125.128
62.115.116.212
62.115.125.55
62.115.61.31
148.72.32.65
?
192.186.199.228

Hop Count: 18
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/2083/www

```
The following string will be used :
TYPE="password"
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/2096/www

```
The following string will be used :
TYPE="password"
```

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/2078/www