ssuedu

Report generated by Nessus™ Wed, 13 Oct 2021 13:10:06 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

141.8.192.214

0	2	8	4	83
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Oct 13 12:44:37 2021

End time: Wed Oct 13 13:10:06 2021

Host Information

DNS Name: onar.from.sh

IP: 141.8.192.214

OS: CISCO PIX 7.0

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)

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)

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}
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/110/pop3

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Not After : Sep 30 14:01:15 2021 GMT
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/143/imap

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Not After : Sep 30 14:01:15 2021 GMT
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/993/imap

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Not After : Sep 30 14:01:15 2021 GMT
```

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)

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/110/pop3

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
    ECDHE-RSA-RC4-SHA             0xC0, 0x11        ECDH          RSA      RC4(128)
 SHA1
    RC4-MD5                       0x00, 0x04        RSA           RSA      RC4(128)               MD5
    RC4-SHA                       0x00, 0x05        RSA           RSA      RC4(128)
 SHA1

The fields above are :

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

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

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

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

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

See Also

https://www.rc4nomore.com/

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

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

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

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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/143/imap

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-RC4-SHA             0xC0, 0x11        ECDH          RSA      RC4(128)
 SHA1
    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)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

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)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

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)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/993/imap

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

15855 - POP3 Cleartext Logins Permitted

Synopsis

The remote POP3 daemon allows credentials to be transmitted in cleartext.

Description

The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.

See Also

https://tools.ietf.org/html/rfc2222

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

Solution

Contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.

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: 2004/11/30, Modified: 2017/06/12

Plugin Output

tcp/110/pop3

```
The following cleartext methods are supported :
USER
SASL PLAIN
```

54582 - SMTP Service Cleartext Login Permitted

Synopsis

The remote mail server allows cleartext logins.

Description

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

See Also

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

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

Solution

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

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/25/smtp

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

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

54582 - SMTP Service Cleartext Login Permitted

Synopsis

The remote mail server allows cleartext logins.

Description

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

See Also

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

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

Solution

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

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/587/smtp

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

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

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

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

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

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
```

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: 2021/07/22

Plugin Output

tcp/0

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

  cpe:/o:cisco:pix_firewall:7.0

Following application CPE's matched on the remote system :

  cpe:/a:mysql:mysql:5.7.31-34
  cpe:/a:openbsd:openssh:7.4 -> OpenBSD OpenSSH 7.4
```

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: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : firewall
Confidence level : 70
```

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 3 of 50 allowed.
220-Local time is now 19:48. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 5 minutes of inactivity.
```

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 :

openresty
```

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

```
141.8.192.214 resolves as onar.from.sh.
```

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

42085 - IMAP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

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

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

Common Name: from.sh

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R3

Serial Number: 03 3B 71 C0 83 B9 A4 D8 A8 95 F3 10 39 D5 E3 87 92 4A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Aug 30 21:04:37 2021 GMT
```

```
Not Valid After: Nov 28 21:04:36 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E4 A1 0A A6 A1 D2 92 25 E1 1D 04 13 A2 4C 65 15 16 F2 B0
            DE 4E 22 A6 AA B6 B7 8D 1A 9B 9C EB 38 D4 63 7C 50 B3 E7 59
            D2 02 48 57 AD C8 A7 E4 4C F7 8C C6 32 31 D2 64 68 E2 A2 2D
            F8 6E 57 81 2D 4B 5E 3F DA F7 45 E4 D5 D9 A1 A6 65 66 5E 47
            F0 79 0A B2 47 BE 1C A6 54 59 07 FB 06 EA B1 E1 38 25 7E 44
            4B 3B E9 3C 97 4B A6 1F DA D8 B9 8D 74 1A 80 DF 04 20 02 2A
            06 9D 5E F9 64 D0 12 CA CA 06 49 FD 4F DD 4C 77 64 98 09 68
            D6 B6 88 38 B2 11 C9 0B 29 B7 37 14 7B D5 F3 FD 30 AF 66 86
            62 4B 62 92 B9 28 C5 E7 D4 66 7A 85 AF 3D C1 58 5D 6D 57 06
            A9 C7 61 7D F8 D4 A3 82 08 6F 5F 6E FC 53 F2 7C 32 43 58 18
            6E 75 04 C0 71 6F 39 D8 3F 1E F3 A6 D2 D6 6B 7E 0C E8 FF F7
            6C 80 18 A3 C8 F5 C9 BF F7 81 A2 45 4D 6A 3E 3F EB CF A5 D4
            78 B6 ED 6C 77 64 16 FE 98 F6 B9 2F F8 56 4B 9E 9B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 25 E0 2E E4 F6 9E 77 FC 90 C6 EA 5A A7 1F 79 B3 91 80 FB
           0A C0 37 0A 92 42 C8 50 A7 DB 37 33 DF A4 D9 92 02 CD AC 54
           52 32 0C 0C 65 38 2D B0 10 BA 78 3F D3 81 5E 83 39 9E 99 86
           EC BD 63 C4 B9 B3 18 AB 7D 2B 9D 1C B4 B5 7C 4E B5 AF 4B CC
           DF F4 75 6D FF DB B6 7F A8 67 40 94 FC 14 B4 AB 50 10 0E 76
           05 3D D5 F3 C1 F7 A1 D2 DD 55 25 16 AA E1 7A 4B 1C FF 56 99
           CF C4 DC AE 8B 55 73 13 8C D2 [...]
```

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: 2021/05/10

Plugin Output

tcp/3306/mysql

```
Version  : 5.7.31-34
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_PASSWORD (new more secure passwords)
  CLIENT_FOUND_ROWS (Found instead of affected rows)
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_NO_SCHEMA (Don't allow database.table.column)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_ODBC (ODBC client)
  CLIENT_LOCAL_FILES (Can use LOAD DATA LOCAL)
  CLIENT_IGNORE_SPACE (Ignore spaces before "(")
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_INTERACTIVE (This is an interactive client)
  CLIENT_SSL (Switch to SSL after handshake)
  CLIENT_SIGPIPE (IGNORE sigpipes)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_RESERVED (Old flag for 4.1 protocol)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

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: 2021/09/16

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: 2021/09/16

Plugin Output

tcp/25/smtp

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

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: 2021/09/16

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: 2021/09/16

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: 2021/09/16

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: 2021/09/16

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: 2021/09/16

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: 2021/09/16

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: 2021/09/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.15.2
Nessus build : 20273
Plugin feed version : 202110130251
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86
Scan type : Normal
Scan name : ssuedu
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.73.130
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 80.374 ms
Thorough tests : no
Experimental tests : 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 : 2021/10/13 12:44 EDT
Scan duration : 1485 sec
```

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: 2021/09/27

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP

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_7.4
SinFP:
   P1:B11013:F0x12:W64240:O0204ffff:M1460:
   P2:B11013:F0x12:W64240:O0204ffff:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:181501_7_p=443R
HTTP:!:Server: openresty

SMTP:!:220 onar.from.sh
SSLcert:!:i/CN:R3i/O:Let's Encrypts/CN:from.sh
82e4e795613a8f8fcc1534a82030b2e2eefb305c
i/CN:R3i/O:Let's Encrypts/CN:from.sh
82e4e795613a8f8fcc1534a82030b2e2eefb305c
i/CN:R3i/O:Let's Encrypts/CN:from.sh
82e4e795613a8f8fcc1534a82030b2e2eefb305c
i/CN:R3i/O:Let's Encrypts/CN:from.sh
82e4e795613a8f8fcc1534a82030b2e2eefb305c
```

```
The remote host is running CISCO PIX 7.0
```

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

- 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: 2021/07/23

Plugin Output

tcp/0

```
Port 110 was detected as being open but is now closed
```

```
Port 587 was detected as being open but is now unresponsive
Port 80 was detected as being open but is now unresponsive
Port 143 was detected as being open but is now closed
Port 25 was detected as being open but is now unresponsive
Port 443 was detected as being open but is now unresponsive
```

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

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.
```

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: from.sh

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R3

Serial Number: 03 3B 71 C0 83 B9 A4 D8 A8 95 F3 10 39 D5 E3 87 92 4A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Aug 30 21:04:37 2021 GMT
```

```
Not Valid After: Nov 28 21:04:36 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E4 A1 0A A6 A1 D2 92 25 E1 1D 04 13 A2 4C 65 15 16 F2 B0
            DE 4E 22 A6 AA B6 B7 8D 1A 9B 9C EB 38 D4 63 7C 50 B3 E7 59
            D2 02 48 57 AD C8 A7 E4 4C F7 8C C6 32 31 D2 64 68 E2 A2 2D
            F8 6E 57 81 2D 4B 5E 3F DA F7 45 E4 D5 D9 A1 A6 65 66 5E 47
            F0 79 0A B2 47 BE 1C A6 54 59 07 FB 06 EA B1 E1 38 25 7E 44
            4B 3B E9 3C 97 4B A6 1F DA D8 B9 8D 74 1A 80 DF 04 20 02 2A
            06 9D 5E F9 64 D0 12 CA CA 06 49 FD 4F DD 4C 77 64 98 09 68
            D6 B6 88 38 B2 11 C9 0B 29 B7 37 14 7B D5 F3 FD 30 AF 66 86
            62 4B 62 92 B9 28 C5 E7 D4 66 7A 85 AF 3D C1 58 5D 6D 57 06
            A9 C7 61 7D F8 D4 A3 82 08 6F 5F 6E FC 53 F2 7C 32 43 58 18
            6E 75 04 C0 71 6F 39 D8 3F 1E F3 A6 D2 D6 6B 7E 0C E8 FF F7
            6C 80 18 A3 C8 F5 C9 BF F7 81 A2 45 4D 6A 3E 3F EB CF A5 D4
            78 B6 ED 6C 77 64 16 FE 98 F6 B9 2F F8 56 4B 9E 9B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 25 E0 2E E4 F6 9E 77 FC 90 C6 EA 5A A7 1F 79 B3 91 80 FB
           0A C0 37 0A 92 42 C8 50 A7 DB 37 33 DF A4 D9 92 02 CD AC 54
           52 32 0C 0C 65 38 2D B0 10 BA 78 3F D3 81 5E 83 39 9E 99 86
           EC BD 63 C4 B9 B3 18 AB 7D 2B 9D 1C B4 B5 7C 4E B5 AF 4B CC
           DF F4 75 6D FF DB B6 7F A8 67 40 94 FC 14 B4 AB 50 10 0E 76
           05 3D D5 F3 C1 F7 A1 D2 DD 55 25 16 AA E1 7A 4B 1C FF 56 99
           CF C4 DC AE 8B 55 73 13 8C D2 71  [...]
```

54580 - SMTP Authentication Methods

Synopsis

The remote mail server supports authentication.

Description

The remote SMTP server advertises that it supports authentication.

See Also

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

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

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

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/25/smtp

```
Remote SMTP server banner :

220 onar.from.sh
```

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 onar.from.sh
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

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

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

Common Name: from.sh

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R3

Serial Number: 03 3B 71 C0 83 B9 A4 D8 A8 95 F3 10 39 D5 E3 87 92 4A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Aug 30 21:04:37 2021 GMT
```

```
Not Valid After: Nov 28 21:04:36 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E4 A1 0A A6 A1 D2 92 25 E1 1D 04 13 A2 4C 65 15 16 F2 B0
            DE 4E 22 A6 AA B6 B7 8D 1A 9B 9C EB 38 D4 63 7C 50 B3 E7 59
            D2 02 48 57 AD C8 A7 E4 4C F7 8C C6 32 31 D2 64 68 E2 A2 2D
            F8 6E 57 81 2D 4B 5E 3F DA F7 45 E4 D5 D9 A1 A6 65 66 5E 47
            F0 79 0A B2 47 BE 1C A6 54 59 07 FB 06 EA B1 E1 38 25 7E 44
            4B 3B E9 3C 97 4B A6 1F DA D8 B9 8D 74 1A 80 DF 04 20 02 2A
            06 9D 5E F9 64 D0 12 CA CA 06 49 FD 4F DD 4C 77 64 98 09 68
            D6 B6 88 38 B2 11 C9 0B 29 B7 37 14 7B D5 F3 FD 30 AF 66 86
            62 4B 62 92 B9 28 C5 E7 D4 66 7A 85 AF 3D C1 58 5D 6D 57 06
            A9 C7 61 7D F8 D4 A3 82 08 6F 5F 6E FC 53 F2 7C 32 43 58 18
            6E 75 04 C0 71 6F 39 D8 3F 1E F3 A6 D2 D6 6B 7E 0C E8 FF F7
            6C 80 18 A3 C8 F5 C9 BF F7 81 A2 45 4D 6A 3E 3F EB CF A5 D4
            78 B6 ED 6C 77 64 16 FE 98 F6 B9 2F F8 56 4B 9E 9B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 25 E0 2E E4 F6 9E 77 FC 90 C6 EA 5A A7 1F 79 B3 91 80 FB
           0A C0 37 0A 92 42 C8 50 A7 DB 37 33 DF A4 D9 92 02 CD AC 54
           52 32 0C 0C 65 38 2D B0 10 BA 78 3F D3 81 5E 83 39 9E 99 86
           EC BD 63 C4 B9 B3 18 AB 7D 2B 9D 1C B4 B5 7C 4E B5 AF 4B CC
           DF F4 75 6D FF DB B6 7F A8 67 40 94 FC 14 B4 AB 50 10 0E 76
           05 3D D5 F3 C1 F7 A1 D2 DD 55 25 16 AA E1 7A 4B 1C FF 56 99
           CF C4 DC AE 8B 55 73 13 8C D [...]
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/587/smtp

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

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

Common Name: from.sh

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R3

Serial Number: 03 3B 71 C0 83 B9 A4 D8 A8 95 F3 10 39 D5 E3 87 92 4A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Aug 30 21:04:37 2021 GMT
```

```
Not Valid After: Nov 28 21:04:36 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E4 A1 0A A6 A1 D2 92 25 E1 1D 04 13 A2 4C 65 15 16 F2 B0
            DE 4E 22 A6 AA B6 B7 8D 1A 9B 9C EB 38 D4 63 7C 50 B3 E7 59
            D2 02 48 57 AD C8 A7 E4 4C F7 8C C6 32 31 D2 64 68 E2 A2 2D
            F8 6E 57 81 2D 4B 5E 3F DA F7 45 E4 D5 D9 A1 A6 65 66 5E 47
            F0 79 0A B2 47 BE 1C A6 54 59 07 FB 06 EA B1 E1 38 25 7E 44
            4B 3B E9 3C 97 4B A6 1F DA D8 B9 8D 74 1A 80 DF 04 20 02 2A
            06 9D 5E F9 64 D0 12 CA CA 06 49 FD 4F DD 4C 77 64 98 09 68
            D6 B6 88 38 B2 11 C9 0B 29 B7 37 14 7B D5 F3 FD 30 AF 66 86
            62 4B 62 92 B9 28 C5 E7 D4 66 7A 85 AF 3D C1 58 5D 6D 57 06
            A9 C7 61 7D F8 D4 A3 82 08 6F 5F 6E FC 53 F2 7C 32 43 58 18
            6E 75 04 C0 71 6F 39 D8 3F 1E F3 A6 D2 D6 6B 7E 0C E8 FF F7
            6C 80 18 A3 C8 F5 C9 BF F7 81 A2 45 4D 6A 3E 3F EB CF A5 D4
            78 B6 ED 6C 77 64 16 FE 98 F6 B9 2F F8 56 4B 9E 9B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 25 E0 2E E4 F6 9E 77 FC 90 C6 EA 5A A7 1F 79 B3 91 80 FB
           0A C0 37 0A 92 42 C8 50 A7 DB 37 33 DF A4 D9 92 02 CD AC 54
           52 32 0C 0C 65 38 2D B0 10 BA 78 3F D3 81 5E 83 39 9E 99 86
           EC BD 63 C4 B9 B3 18 AB 7D 2B 9D 1C B4 B5 7C 4E B5 AF 4B CC
           DF F4 75 6D FF DB B6 7F A8 67 40 94 FC 14 B4 AB 50 10 0E 76
           05 3D D5 F3 C1 F7 A1 D2 DD 55 25 16 AA E1 7A 4B 1C FF 56 99
           CF C4 DC AE 8B 55 73 13 8C D [...]
```

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 :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

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

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
```

```
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  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_ [...]
```

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: 2021/09/23

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-etm@openssh.com

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

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

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_7.4
SSH supported authentication : publickey
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/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.
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/110/pop3

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=from.sh
|-Not After : Nov 28 21:04:36 2021 GMT
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/143/imap

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=from.sh
|-Not After : Nov 28 21:04:36 2021 GMT
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/993/imap

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=from.sh
|-Not After : Nov 28 21:04:36 2021 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/110/pop3

```
The SSL certificate will expire within 60 days, at
Nov 28 21:04:36 2021 GMT :

  Subject          : CN=from.sh
  Issuer           : C=US, O=Let's Encrypt, CN=R3
  Not valid before : Aug 30 21:04:37 2021 GMT
  Not valid after  : Nov 28 21:04:36 2021 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/143/imap

```
The SSL certificate will expire within 60 days, at
Nov 28 21:04:36 2021 GMT :

  Subject          : CN=from.sh
  Issuer           : C=US, O=Let's Encrypt, CN=R3
  Not valid before : Aug 30 21:04:37 2021 GMT
  Not valid after  : Nov 28 21:04:36 2021 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/993/imap

```
The SSL certificate will expire within 60 days, at
Nov 28 21:04:36 2021 GMT :

  Subject          : CN=from.sh
  Issuer           : C=US, O=Let's Encrypt, CN=R3
  Not valid before : Aug 30 21:04:37 2021 GMT
  Not valid after  : Nov 28 21:04:36 2021 GMT
```

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: from.sh

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R3

Serial Number: 03 3B 71 C0 83 B9 A4 D8 A8 95 F3 10 39 D5 E3 87 92 4A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Aug 30 21:04:37 2021 GMT
Not Valid After: Nov 28 21:04:36 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E4 A1 0A A6 A1 D2 92 25 E1 1D 04 13 A2 4C 65 15 16 F2 B0
            DE 4E 22 A6 AA B6 B7 8D 1A 9B 9C EB 38 D4 63 7C 50 B3 E7 59
            D2 02 48 57 AD C8 A7 E4 4C F7 8C C6 32 31 D2 64 68 E2 A2 2D
            F8 6E 57 81 2D 4B 5E 3F DA F7 45 E4 D5 D9 A1 A6 65 66 5E 47
            F0 79 0A B2 47 BE 1C A6 54 59 07 FB 06 EA B1 E1 38 25 7E 44
            4B 3B E9 3C 97 4B A6 1F DA D8 B9 8D 74 1A 80 DF 04 20 02 2A
            06 9D 5E F9 64 D0 12 CA CA 06 49 FD 4F DD 4C 77 64 98 09 68
            D6 B6 88 38 B2 11 C9 0B 29 B7 37 14 7B D5 F3 FD 30 AF 66 86
            62 4B 62 92 B9 28 C5 E7 D4 66 7A 85 AF 3D C1 58 5D 6D 57 06
```

```
            A9 C7 61 7D F8 D4 A3 82 08 6F 5F 6E FC 53 F2 7C 32 43 58 18
            6E 75 04 C0 71 6F 39 D8 3F 1E F3 A6 D2 D6 6B 7E 0C E8 FF F7
            6C 80 18 A3 C8 F5 C9 BF F7 81 A2 45 4D 6A 3E 3F EB CF A5 D4
            78 B6 ED 6C 77 64 16 FE 98 F6 B9 2F F8 56 4B 9E 9B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 25 E0 2E E4 F6 9E 77 FC 90 C6 EA 5A A7 1F 79 B3 91 80 FB
           0A C0 37 0A 92 42 C8 50 A7 DB 37 33 DF A4 D9 92 02 CD AC 54
           52 32 0C 0C 65 38 2D B0 10 BA 78 3F D3 81 5E 83 39 9E 99 86
           EC BD 63 C4 B9 B3 18 AB 7D 2B 9D 1C B4 B5 7C 4E B5 AF 4B CC
           DF F4 75 6D FF DB B6 7F A8 67 40 94 FC 14 B4 AB 50 10 0E 76
           05 3D D5 F3 C1 F7 A1 D2 DD 55 25 16 AA E1 7A 4B 1C FF 56 99
           CF C4 DC AE 8B 55 73 13 8C D2 71 43 28 52 35 9E 63 39 92 1B
           3F 58 BB 0A 96 BC B3 C8 3B 38 CC 4F 5A 25 D7 8E E9 3F AD EE
           93 C5 6A 15 08 83 50 52 C9 1A AC 09 4B 47 39 64 99 24 2F 83
     [...]
```

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: from.sh

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R3

Serial Number: 03 3B 71 C0 83 B9 A4 D8 A8 95 F3 10 39 D5 E3 87 92 4A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Aug 30 21:04:37 2021 GMT
Not Valid After: Nov 28 21:04:36 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E4 A1 0A A6 A1 D2 92 25 E1 1D 04 13 A2 4C 65 15 16 F2 B0
            DE 4E 22 A6 AA B6 B7 8D 1A 9B 9C EB 38 D4 63 7C 50 B3 E7 59
            D2 02 48 57 AD C8 A7 E4 4C F7 8C C6 32 31 D2 64 68 E2 A2 2D
            F8 6E 57 81 2D 4B 5E 3F DA F7 45 E4 D5 D9 A1 A6 65 66 5E 47
            F0 79 0A B2 47 BE 1C A6 54 59 07 FB 06 EA B1 E1 38 25 7E 44
            4B 3B E9 3C 97 4B A6 1F DA D8 B9 8D 74 1A 80 DF 04 20 02 2A
            06 9D 5E F9 64 D0 12 CA CA 06 49 FD 4F DD 4C 77 64 98 09 68
            D6 B6 88 38 B2 11 C9 0B 29 B7 37 14 7B D5 F3 FD 30 AF 66 86
            62 4B 62 92 B9 28 C5 E7 D4 66 7A 85 AF 3D C1 58 5D 6D 57 06
```

```
            A9 C7 61 7D F8 D4 A3 82 08 6F 5F 6E FC 53 F2 7C 32 43 58 18
            6E 75 04 C0 71 6F 39 D8 3F 1E F3 A6 D2 D6 6B 7E 0C E8 FF F7
            6C 80 18 A3 C8 F5 C9 BF F7 81 A2 45 4D 6A 3E 3F EB CF A5 D4
            78 B6 ED 6C 77 64 16 FE 98 F6 B9 2F F8 56 4B 9E 9B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 25 E0 2E E4 F6 9E 77 FC 90 C6 EA 5A A7 1F 79 B3 91 80 FB
           0A C0 37 0A 92 42 C8 50 A7 DB 37 33 DF A4 D9 92 02 CD AC 54
           52 32 0C 0C 65 38 2D B0 10 BA 78 3F D3 81 5E 83 39 9E 99 86
           EC BD 63 C4 B9 B3 18 AB 7D 2B 9D 1C B4 B5 7C 4E B5 AF 4B CC
           DF F4 75 6D FF DB B6 7F A8 67 40 94 FC 14 B4 AB 50 10 0E 76
           05 3D D5 F3 C1 F7 A1 D2 DD 55 25 16 AA E1 7A 4B 1C FF 56 99
           CF C4 DC AE 8B 55 73 13 8C D2 71 43 28 52 35 9E 63 39 92 1B
           3F 58 BB 0A 96 BC B3 C8 3B 38 CC 4F 5A 25 D7 8E E9 3F AD EE
           93 C5 6A 15 08 83 50 52 C9 1A AC 09 4B 47 39 64 99 24 2F 83
     [...]
```

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: from.sh

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R3

Serial Number: 03 3B 71 C0 83 B9 A4 D8 A8 95 F3 10 39 D5 E3 87 92 4A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Aug 30 21:04:37 2021 GMT
Not Valid After: Nov 28 21:04:36 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E4 A1 0A A6 A1 D2 92 25 E1 1D 04 13 A2 4C 65 15 16 F2 B0
            DE 4E 22 A6 AA B6 B7 8D 1A 9B 9C EB 38 D4 63 7C 50 B3 E7 59
            D2 02 48 57 AD C8 A7 E4 4C F7 8C C6 32 31 D2 64 68 E2 A2 2D
            F8 6E 57 81 2D 4B 5E 3F DA F7 45 E4 D5 D9 A1 A6 65 66 5E 47
            F0 79 0A B2 47 BE 1C A6 54 59 07 FB 06 EA B1 E1 38 25 7E 44
            4B 3B E9 3C 97 4B A6 1F DA D8 B9 8D 74 1A 80 DF 04 20 02 2A
            06 9D 5E F9 64 D0 12 CA CA 06 49 FD 4F DD 4C 77 64 98 09 68
            D6 B6 88 38 B2 11 C9 0B 29 B7 37 14 7B D5 F3 FD 30 AF 66 86
            62 4B 62 92 B9 28 C5 E7 D4 66 7A 85 AF 3D C1 58 5D 6D 57 06
```

```
            A9 C7 61 7D F8 D4 A3 82 08 6F 5F 6E FC 53 F2 7C 32 43 58 18
            6E 75 04 C0 71 6F 39 D8 3F 1E F3 A6 D2 D6 6B 7E 0C E8 FF F7
            6C 80 18 A3 C8 F5 C9 BF F7 81 A2 45 4D 6A 3E 3F EB CF A5 D4
            78 B6 ED 6C 77 64 16 FE 98 F6 B9 2F F8 56 4B 9E 9B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 25 E0 2E E4 F6 9E 77 FC 90 C6 EA 5A A7 1F 79 B3 91 80 FB
           0A C0 37 0A 92 42 C8 50 A7 DB 37 33 DF A4 D9 92 02 CD AC 54
           52 32 0C 0C 65 38 2D B0 10 BA 78 3F D3 81 5E 83 39 9E 99 86
           EC BD 63 C4 B9 B3 18 AB 7D 2B 9D 1C B4 B5 7C 4E B5 AF 4B CC
           DF F4 75 6D FF DB B6 7F A8 67 40 94 FC 14 B4 AB 50 10 0E 76
           05 3D D5 F3 C1 F7 A1 D2 DD 55 25 16 AA E1 7A 4B 1C FF 56 99
           CF C4 DC AE 8B 55 73 13 8C D2 71 43 28 52 35 9E 63 39 92 1B
           3F 58 BB 0A 96 BC B3 C8 3B 38 CC 4F 5A 25 D7 8E E9 3F AD EE
           93 C5 6A 15 08 83 50 52 C9 1A AC 09 4B 47 39 64 99 24 2F 83
     [...]
```

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. 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.

See Also

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

https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2008/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

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

Plugin Information

Published: 2016/12/08, Modified: 2019/11/26

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             : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Sep 30 21:12:19 2000 GMT
|-Valid To            : Sep 30 14:01:15 2021 GMT
```

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. 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.

See Also

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

https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2008/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

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

Plugin Information

Published: 2016/12/08, Modified: 2019/11/26

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             : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Sep 30 21:12:19 2000 GMT
|-Valid To            : Sep 30 14:01:15 2021 GMT
```

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. 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.

See Also

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

https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2008/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

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

Plugin Information

Published: 2016/12/08, Modified: 2019/11/26

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             : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Sep 30 21:12:19 2000 GMT
|-Valid To            : Sep 30 14:01:15 2021 GMT
```

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
   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
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
   IDEA-CBC-SHA                  0x00 [...]
```

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
   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
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
   IDEA-CBC-SHA                  0x00 [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/993/imap

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    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}
```

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/man1.1.0/apps/ciphers.html

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

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
   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    [...]
```

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/man1.1.0/apps/ciphers.html

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

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
   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    [...]
```

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/man1.1.0/apps/ciphers.html

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/993/imap

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

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                         Code             KEX           Auth     Encryption             MAC
    ----------------------       ----------       ---           ----     --------------------   ---
    ECDHE-RSA-AES128-SHA256      0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384      0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES256-SHA         0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES256-SHA384      0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384


SSL Version : TLSv11
  High Strength Ciphers (>= 112-bit key)

    Name                         Code             KEX           Auth     Encryption             MAC
    ----------------------       ----------       ---           ----     --------------------   ---
```

```
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1


SSL Version : TLSv1
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1

The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/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
   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/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
   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/993/imap

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

  High Strength Ciphers (>= 112-bit key)

    Name                         Code             KEX           Auth     Encryption             MAC
    ----------------------       ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256      0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384      0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES256-SHA         0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    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/110/pop3

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

|-Subject             : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Issuer              : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Valid From          : Sep 30 21:12:19 2000 GMT
|-Valid To            : Sep 30 14:01:15 2021 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             : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Issuer              : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Valid From          : Sep 30 21:12:19 2000 GMT
|-Valid To            : Sep 30 14:01:15 2021 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             : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Issuer              : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Valid From          : Sep 30 21:12:19 2000 GMT
|-Valid To            : Sep 30 14:01:15 2021 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: 2021/04/14

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: 2021/04/14

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: 2021/04/14

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: 2021/04/14

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: 2021/04/14

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: 2021/04/14

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: 2021/04/14

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.
```

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.
```

14773 - Service Detection: 3 ASCII Digit Code Responses

Synopsis

This plugin performs service detection.

Description

This plugin is a complement of find_service1.nasl. It attempts to identify services that return 3 ASCII digits codes (ie: FTP, SMTP, NNTP, ...)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/09/17, Modified: 2011/08/16

Plugin Output

tcp/25/smtp

```
A SMTP server is running on this port
```

14773 - Service Detection: 3 ASCII Digit Code Responses

Synopsis

This plugin performs service detection.

Description

This plugin is a complement of find_service1.nasl. It attempts to identify services that return 3 ASCII digits codes (ie: FTP, SMTP, NNTP, ...)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/09/17, Modified: 2011/08/16

Plugin Output

tcp/587/smtp

```
A SMTP server is running on this port
```

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

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

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

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

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

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/993/imap

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/110/pop3

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/143/imap

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/993/imap

```
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: 2021/08/30

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```