sona

Report generated by Nessus™ Thu, 24 Aug 2023 19:19:49 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

162.215.219.65

0	0	22	2	211
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Aug 24 17:26:51 2023
End time:	Thu Aug 24 19:19:49 2023

Host Information

DNS Name:	server.cbw.pmj.mybluehostin.me
IP:	162.215.219.65
OS:	Linux Kernel 2.6

Vulnerabilities

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

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

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2020/11/17, Modified: 2023/06/08

Plugin Output

tcp/443/www

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

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

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

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2020/11/17, Modified: 2023/06/08

Plugin Output

tcp/2078/www

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

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

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

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2020/11/17, Modified: 2023/06/08

Plugin Output

tcp/2080/www

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

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

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

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2020/11/17, Modified: 2023/06/08

Plugin Output

tcp/2083/www

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

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

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

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2020/11/17, Modified: 2023/06/08

Plugin Output

tcp/2087/www

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

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

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

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2020/11/17, Modified: 2023/06/08

Plugin Output

tcp/2096/www

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

52609 - IMAP Service STARTTLS Plaintext Command Injection

Synopsis

The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

Description

The remote IMAP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.

Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

See Also

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

https://www.securityfocus.com/archive/1/516901/30/0/threaded

Solution

Contact the vendor to see if an update is available.

Risk Factor

Medium

VPR Score

6.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	46767
BID	58171
CVE	CVE-2011-0411
CVE	CVE-2011-1926
XREF	CERT:555316

Plugin Information

Published: 2011/03/10, Modified: 2021/02/24

Plugin Output

tcp/143/imap

```
Nessus sent the following two commands in a single packet :

  nessus1 STARTTLS\r\nnessus2 CAPABILITY\r\n

And the server sent the following two responses :

  nessus1 OK Begin TLS negotiation now.
  nessus2 OK Pre-login capabilities listed, post-login capabilities have more.
```

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

|-Subject : CN=server.cbw.pmj.mybluehostin.me
|-Issuer  : OU=generated by AVG Antivirus for untrusted server certificates/O=AVG Web/Mail Shield/
CN=AVG Web/Mail Shield Untrusted Root
```

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

|-Subject : CN=server.cbw.pmj.mybluehostin.me
|-Issuer  : OU=generated by AVG Antivirus for untrusted server certificates/O=AVG Web/Mail Shield/
CN=AVG Web/Mail Shield Untrusted Root
```

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/465/smtp

```

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

|-Subject : CN=server.cbw.pmj.mybluehostin.me
|-Issuer  : OU=generated by AVG Antivirus for untrusted server certificates/O=AVG Web/Mail Shield/
CN=AVG Web/Mail Shield Untrusted Root
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/993/imap

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

|-Subject : CN=server.cbw.pmj.mybluehostin.me
|-Issuer  : OU=generated by AVG Antivirus for untrusted server certificates/O=AVG Web/Mail Shield/
CN=AVG Web/Mail Shield Untrusted Root
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/995/pop3

```

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

|-Subject : CN=server.cbw.pmj.mybluehostin.me
|-Issuer  : OU=generated by AVG Antivirus for untrusted server certificates/O=AVG Web/Mail Shield/
CN=AVG Web/Mail Shield Untrusted Root
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

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

Plugin Output

tcp/110/pop3

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

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

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

Plugin Output

tcp/143/imap

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

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

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

Plugin Output

tcp/465/smtp

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

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

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

Plugin Output

tcp/993/imap

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

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

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

Plugin Output

tcp/995/pop3

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

157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

tcp/110/pop3

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

157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

tcp/143/imap

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

157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

tcp/465/smtp

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

157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

tcp/993/imap

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

157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

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

Description

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

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

See Also

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

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2023/04/19

Plugin Output

tcp/995/pop3

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

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

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

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

Solution

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

Risk Factor

Low

VPR Score

2.5

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

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

Plugin Output

tcp/22/ssh

```

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

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

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

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

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

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

Description

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

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

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

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

See Also

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

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

Solution

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

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/22/ssh

```

The following weak key exchange algorithms are enabled :

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

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

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

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - mail.cbw.pmj.mybluehostin.me
```

48204 - Apache HTTP Server Version

Synopsis

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

Description

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

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/80/http_proxy

```
URL        : http://server.cbw.pmj.mybluehostin.me/
Version    : unknown
Source     : Server: Apache
backported : 0
```

48204 - Apache HTTP Server Version

Synopsis

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

Description

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

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/443/www

```
URL        : https://server.cbw.pmj.mybluehostin.me/
Version    : unknown
Source     : Server: Apache
backported : 0
```

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

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

  FQDN       : server.cbw.pmj.mybluehostin.me
  Confidence : 100
  Resolves   : True
  Method     : rDNS Lookup: IP Address

Another possible FQDN was also detected:
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

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

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

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2023/07/27

Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

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

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server -> Apache Software Foundation Apache HTTP Server
  cpe:/a:mysql:mysql -> MySQL MySQL
  cpe:/a:openbsd:openssh:7.4 -> OpenBSD OpenSSH
```

31658 - DNS Sender Policy Framework (SPF) Enabled

Synopsis

The remote domain publishes SPF records.

Description

The remote domain publishes SPF records. SPF (Sender Policy Framework) is a mechanism to let an organization specify their mail sending policy, such as which mail servers are authorized to send mail on its behalf.

See Also

http://www.openspf.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/03/26, Modified: 2011/05/24

Plugin Output

udp/53/dns

```
The following SPF records could be extracted for cbw.pmj.mybluehostin.me:

v=spf1 +a +mx +ip4:162.215.219.65 ~all
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/53/dns

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

udp/53/dns

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

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

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

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

Solution

n/a

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/21/ftp

```

The remote FTP banner is :

220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 05:58. 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 15 minutes of inactivity.
```

42149 - FTP Service AUTH TLS Command Support

Synopsis

The remote directory service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/21/ftp

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2078/www

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2080/www

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2083/www

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2087/www

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2096/www

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

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/http_proxy

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

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2078/www

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

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

    /
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/80/http_proxy

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/443/www

```
The remote web server type is :

Apache
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/2078/www

```
The remote web server type is :

cPanel
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/2080/www

```
The remote web server type is :

cPanel
```

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

```
162.215.219.65 resolves as server.cbw.pmj.mybluehostin.me.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/http_proxy

```

Response Code : HTTP/1.1 200 OK

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

  Date: Thu, 24 Aug 2023 13:06:15 GMT
  Server: Apache
  Last-Modified: Tue, 11 Jul 2023 17:58:54 GMT
  Accept-Ranges: none
  Content-Length: 163
  Cache-Control: no-cache, no-store, must-revalidate
  Pragma: no-cache
  Expires: 0
  Keep-Alive: timeout=5, max=100
  Content-Type: text/html
  Via: HTTP/1.1 forward.http.proxy:3128
  Connection: keep-alive

Response Body :

<html><head><META HTTP-EQUIV="Cache-control" CONTENT="no-cache"><META HTTP-EQUIV="refresh"
 CONTENT="0;URL=/cgi-sys/defaultwebpage.cgi"></head><body></body></html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/443/www

```

Response Code : HTTP/1.1 200 OK

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

  Date: Thu, 24 Aug 2023 13:06:13 GMT
  Server: Apache
  Last-Modified: Tue, 11 Jul 2023 17:58:54 GMT
  Accept-Ranges: bytes
  Content-Length: 163
  Cache-Control: no-cache, no-store, must-revalidate
  Pragma: no-cache
  Expires: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html><head><META HTTP-EQUIV="Cache-control" CONTENT="no-cache"><META HTTP-EQUIV="refresh"
 CONTENT="0;URL=/cgi-sys/defaultwebpage.cgi"></head><body></body></html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2078/www

```

Response Code : HTTP/1.1 401 Unauthorized

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

  Date: Thu, 24 Aug 2023 13:06:21 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: server.cbw.pmj.mybluehostin.me:2078
  Cache-Control: no-cache, no-store, must-revalidate, private
  Connection: close
  Vary: Accept-Encoding
  WWW-Authenticate: Basic realm="Restricted Area"
  Content-Length: 35
  Content-Type: text/html; charset="utf-8"
  Expires: Fri, 01 Jan 1990 00:00:00 GMT

Response Body :

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

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2080/www

```

Response Code : HTTP/1.1 401 Unauthorized

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

  Date: Thu, 24 Aug 2023 13:06:28 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: server.cbw.pmj.mybluehostin.me:2080
  Cache-Control: no-cache, no-store, must-revalidate, private
  Connection: close
  Vary: Accept-Encoding
  WWW-Authenticate: Basic realm="Horde DAV Server"
  Content-Length: 35
  Content-Type: text/html; charset="utf-8"
  Expires: Fri, 01 Jan 1990 00:00:00 GMT

Response Body :

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

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2083/www

```

Response Code : HTTP/1.1 200 OK

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

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Thu, 24 Aug 2023 13:06:47 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: cpsession=%3aYdjqGx946JcVgcvc%2c81a3e9ccbaa14e49d51aaf4dc1490103; HttpOnly; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=server.cbw.pmj.mybluehostin.me;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
```

```
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2083; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=server.cbw.pmj.mybluehostin.me; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083
  Cache-Control: no-cache, no-store, must-revalidate, private
  X-Frame-Options: SAMEORIGIN
  X-Content-Type-Options: nosniff
  Content-Length: 38076

Response Body :


<!DOCTYPE html>
<html lan [...]
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2087/www

```

Response Code : HTTP/1.1 200 OK

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

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Thu, 24 Aug 2023 13:06:37 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2087; secure
  Set-Cookie: whostmgrsession=%3a17TDjDUmD37jqi3P%2c2ed454903590944efa13683b01d16ce0; HttpOnly;
 path=/; port=2087; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2087; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=server.cbw.pmj.mybluehostin.me;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2087; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;
 secure
```

```
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2087; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=server.cbw.pmj.mybluehostin.me; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2087; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2087
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087
  Cache-Control: no-cache, no-store, must-revalidate, private
  X-Frame-Options: SAMEORIGIN
  X-Content-Type-Options: nosniff
  Content-Length: 37743

Response Body :


<!DOCTYPE htm [...]
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2096/www

```

Response Code : HTTP/1.1 200 OK

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

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Thu, 24 Aug 2023 13:06:09 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: webmailsession=%3a_hUdevhBUMCFIbHY%2c2b5088a67466a989c1f0e63821e6da02; HttpOnly;
 path=/; port=2096; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2096; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=server.cbw.pmj.mybluehostin.me;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
```

```
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2096; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=server.cbw.pmj.mybluehostin.me; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.server.cbw.pmj.mybluehostin.me;
 expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096
  Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Fri, 23-Aug-2024 13:06:09 GMT; path=/;
 port=2096; secure
  Cache-Control: no-cache, no-store, must-revalidate, private
  X-Fram [...]
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

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

Description

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

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

Solution

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

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

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

Plugin Output

icmp/0

```
The difference between the local and remote clocks is 156 seconds.
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

```
The remote imap server banner is :

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

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/993/imap

```
The remote imap server banner is :

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

42085 - IMAP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

```

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

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

Common Name: server.cbw.pmj.mybluehostin.me

Issuer Name:

Organization Unit: generated by AVG Antivirus for untrusted server certificates
Organization: AVG Web/Mail Shield
Common Name: AVG Web/Mail Shield Untrusted Root

Serial Number: 1A DD A0 8D 89 10 FD 46 AA BF 33 9D 7E 88 32 53

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BA 49 52 25 68 92 A4 7D E5 E1 42 A6 41 E0 77 16 5B E5 DA
            DE 02 0C 35 A6 11 0A 2C 3A 2B 44 35 DB 43 E0 2F 95 70 34 67
            7E 14 1A 83 6D D8 8D EF 4D 85 9E 41 B4 28 5D 94 F7 D6 55 70
            65 8C 93 D8 1F 13 F8 51 2F 5B F1 9F 6E 92 36 BF 4A 16 6E 6D
            1A 41 EE 7C 27 DD 64 36 9A 4B 71 AD 85 B2 47 3D 36 7D DB BF
            C8 D5 0C 9F CD B9 9F 44 5E 8B 9B 02 3B A8 81 A7 35 62 E3 0B
            BF 3A 45 C5 37 26 1E 77 ED 23 AA 1F 90 6F FA 60 B2 F0 78 3B
            95 D2 CA 8E D1 72 6A C1 67 29 13 5F ED 72 C0 E4 42 FB 75 DC
            B1 4A 7C BF 52 97 3B C0 D7 FD 44 EB CC 2F 99 A4 A3 9B 0B 9C
            5E F0 C5 C9 48 55 C2 ED DF 34 70 6F E7 E0 9F B8 63 3B A8 45
            09 B5 67 47 16 B2 03 DC B9 7A AA 1E 19 BA F9 2A 15 4B 70 0E
            56 7E C4 4C 60 17 7E 57 0C BA 4C 28 58 44 06 A8 9E 59 98 32
            24 68 29 50 82 6D FA ED 3A 81 02 D0 19 97 1F E5 57
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 7F 3C 52 86 F6 01 C8 4B B7 95 00 BA D7 C4 0F EE 82 DF 35
           49 35 96 53 95 BD 20 8C D8 B5 59 9D 6B ED 0B 20 BB 42 97 96
           6E EB E6 48 7C F8 A0 24 1B 32 00 1D 84 2C FA 43 AA CE 9F 31
           F2 E8 E0 06 F3 2A 02 76 D6 CD 3E 19 B9 D8 35 55 D0 F8 6D 7F
           6B 66 F1 DB 32 9D FD 87 97 E2 24 40 CF 1F 02 EE 3E [...]
```

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0802

Plugin Information

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

Plugin Output

tcp/3306/mysql

```
The remote database access is restricted and configured to reject access
from unauthorized IPs.  Therefore it was not possible to extract its
version number.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/21/ftp

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/22/ssh

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/25

```
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: 2023/06/20

Plugin Output

tcp/53/dns

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/80/http_proxy

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/110/pop3

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/111

```
Port 111/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/143/imap

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/443/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/465/smtp

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/587/smtp

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/993/imap

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/995/pop3

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/2077

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/2078/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/2079

```
Port 2079/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/2080/www

```
Port 2080/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/2082

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/2083/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/2086

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/2087/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/2095

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/2096/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

tcp/3306/mysql

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

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.5.4
Nessus build : 20013
Plugin feed version : 202308241011
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : sona
Scan policy used : Basic Network Scan
Scanner IP : 172.16.23.12
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 274.166 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/8/24 17:27 India Standard Time
Scan duration : 6747 sec
Scan for malware : no
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
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:B10113:F0x12:W29040:O0204ffff:M1412:
   P2:B10113:F0x12:W29040:O0204ffff0101040201030307:M1412:
   P3:B00000:F0x00:W0:O0:M0
   P4:190504_7_p=443R
HTTP:!:Server: Apache

SMTP:!:220 and/or bulk e-mail.
SSLcert:!:i/CN:cPanel, Inc. Certification Authorityi/O:cPanel, Inc.s/
CN:server.cbw.pmj.mybluehostin.me
357af89834969746974f53ad3bd5412fb5122fee
i/CN:cPanel, Inc. Certification Authorityi/O:cPanel, Inc.s/CN:server.cbw.pmj.mybluehostin.me
357af89834969746974f53ad3bd5412fb5122fee
```

```
The remote host is running Linux Kernel 2.6
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

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

This does not necessarily indicate a problem with the scan.

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

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

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0515

Plugin Information

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

Plugin Output

tcp/0

```
The following issues were reported :

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

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

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

There are several possible reasons for this :

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

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

This might be an availability problem related to the following :

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

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

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

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

Solution

Steps to resolve this issue include :

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF	IAVB:0001-B-0509

Plugin Information

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

Plugin Output

tcp/0

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

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/110/pop3

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/465/smtp

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/993/imap

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/995/pop3

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

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

See Also

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

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/110/pop3

```
Remote POP server banner :

+OK Dovecot ready.
```

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

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

See Also

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

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/995/pop3

```
Remote POP server banner :

+OK Dovecot ready.
```

42087 - POP3 Service STLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/110/pop3

```

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

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

Common Name: server.cbw.pmj.mybluehostin.me

Issuer Name:

Organization Unit: generated by AVG Antivirus for untrusted server certificates
Organization: AVG Web/Mail Shield
Common Name: AVG Web/Mail Shield Untrusted Root

Serial Number: 1A DD A0 8D 89 10 FD 46 AA BF 33 9D 7E 88 32 53

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BA 49 52 25 68 92 A4 7D E5 E1 42 A6 41 E0 77 16 5B E5 DA
            DE 02 0C 35 A6 11 0A 2C 3A 2B 44 35 DB 43 E0 2F 95 70 34 67
            7E 14 1A 83 6D D8 8D EF 4D 85 9E 41 B4 28 5D 94 F7 D6 55 70
            65 8C 93 D8 1F 13 F8 51 2F 5B F1 9F 6E 92 36 BF 4A 16 6E 6D
            1A 41 EE 7C 27 DD 64 36 9A 4B 71 AD 85 B2 47 3D 36 7D DB BF
            C8 D5 0C 9F CD B9 9F 44 5E 8B 9B 02 3B A8 81 A7 35 62 E3 0B
            BF 3A 45 C5 37 26 1E 77 ED 23 AA 1F 90 6F FA 60 B2 F0 78 3B
            95 D2 CA 8E D1 72 6A C1 67 29 13 5F ED 72 C0 E4 42 FB 75 DC
            B1 4A 7C BF 52 97 3B C0 D7 FD 44 EB CC 2F 99 A4 A3 9B 0B 9C
            5E F0 C5 C9 48 55 C2 ED DF 34 70 6F E7 E0 9F B8 63 3B A8 45
            09 B5 67 47 16 B2 03 DC B9 7A AA 1E 19 BA F9 2A 15 4B 70 0E
            56 7E C4 4C 60 17 7E 57 0C BA 4C 28 58 44 06 A8 9E 59 98 32
            24 68 29 50 82 6D FA ED 3A 81 02 D0 19 97 1F E5 57
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 7F 3C 52 86 F6 01 C8 4B B7 95 00 BA D7 C4 0F EE 82 DF 35
           49 35 96 53 95 BD 20 8C D8 B5 59 9D 6B ED 0B 20 BB 42 97 96
           6E EB E6 48 7C F8 A0 24 1B 32 00 1D 84 2C FA 43 AA CE 9F 31
           F2 E8 E0 06 F3 2A 02 76 D6 CD 3E 19 B9 D8 35 55 D0 F8 6D 7F
           6B 66 F1 DB 32 9D FD 87 97 E2 24 40 CF 1F 02 EE 3E B0  [...]
```

34043 - PowerDNS Version Detection

Synopsis

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

Description

The remote host is running PowerDNS, an open source DNS server. It was possible to extract the version number of the remote installation by sending a special DNS request for the text 'version.pdns' in the domain 'chaos'.

Solution

If desired, hide the version number of PowerDNS by modifying the 'version-string' option in pdns.conf or recursor.conf.

Risk Factor

None

Plugin Information

Published: 2008/08/25, Modified: 2019/11/22

Plugin Output

udp/53/dns

```
 Query method   : version.pdns
 Version source : PowerDNS Authoritative Server 4.3.1 (built Mar 10 2021 14:03:23 by
root@rpmbuild-64-centos-7.dev.cpanel.net)
 Version        : 4.3.1
 Type           : Authoritative Server
```

10223 - RPC portmapper Service Detection

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0632

Plugin Information

Published: 1999/08/19, Modified: 2019/10/04

Plugin Output

udp/111/rpc-portmapper

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

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

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

Solution

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

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

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

Plugin Output

tcp/465/smtp

```
Remote SMTP server banner :

220 and/or bulk e-mail.
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

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

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

Solution

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

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

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

Plugin Output

tcp/587/smtp

```
Remote SMTP server banner :

220 and/or bulk e-mail.
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/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: server.cbw.pmj.mybluehostin.me

Issuer Name:

Organization Unit: generated by AVG Antivirus for untrusted server certificates
Organization: AVG Web/Mail Shield
Common Name: AVG Web/Mail Shield Untrusted Root

Serial Number: 32 E5 95 34 0E BD 2E 42 84 20 40 99 3F 69 8D 6D

Version: 1

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BA 49 52 25 68 92 A4 7D E5 E1 42 A6 41 E0 77 16 5B E5 DA
            DE 02 0C 35 A6 11 0A 2C 3A 2B 44 35 DB 43 E0 2F 95 70 34 67
            7E 14 1A 83 6D D8 8D EF 4D 85 9E 41 B4 28 5D 94 F7 D6 55 70
            65 8C 93 D8 1F 13 F8 51 2F 5B F1 9F 6E 92 36 BF 4A 16 6E 6D
            1A 41 EE 7C 27 DD 64 36 9A 4B 71 AD 85 B2 47 3D 36 7D DB BF
            C8 D5 0C 9F CD B9 9F 44 5E 8B 9B 02 3B A8 81 A7 35 62 E3 0B
            BF 3A 45 C5 37 26 1E 77 ED 23 AA 1F 90 6F FA 60 B2 F0 78 3B
            95 D2 CA 8E D1 72 6A C1 67 29 13 5F ED 72 C0 E4 42 FB 75 DC
            B1 4A 7C BF 52 97 3B C0 D7 FD 44 EB CC 2F 99 A4 A3 9B 0B 9C
            5E F0 C5 C9 48 55 C2 ED DF 34 70 6F E7 E0 9F B8 63 3B A8 45
            09 B5 67 47 16 B2 03 DC B9 7A AA 1E 19 BA F9 2A 15 4B 70 0E
            56 7E C4 4C 60 17 7E 57 0C BA 4C 28 58 44 06 A8 9E 59 98 32
            24 68 29 50 82 6D FA ED 3A 81 02 D0 19 97 1F E5 57
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 33 8C 89 80 2A 80 6E AB FF 95 4C 42 0A A4 71 D0 A4 12 F5
           C8 6B BF 18 9C A7 11 33 92 95 AC 74 52 2A 9B 5A 87 3A 32 29
           E7 54 DA A9 C9 07 6E E1 14 DA 2E 69 C4 77 DF E9 0C C3 9F 32
           9F 87 8C 34 5F 9A 49 7E 89 C6 29 C7 12 8D 87 8E 42 5B 83 AB
           4D CE 1B C2 E4 3F 52 C4 01 59 47 B5 52 59 D2 C4 8 [...]
```

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_ [...]
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

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

Description

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

```

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

  hmac-sha1
  hmac-sha1-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,gssapi-keyex,gssapi-with-mic,password
```

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: 2023/07/10

Plugin Output

tcp/143/imap

```
This port supports TLSv1.3/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: 2023/07/10

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: 2023/07/10

Plugin Output

tcp/465/smtp

```
This port supports TLSv1.3/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: 2023/07/10

Plugin Output

tcp/993/imap

```
This port supports TLSv1.3/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: 2023/07/10

Plugin Output

tcp/995/pop3

```
This port supports TLSv1.3/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: 2023/07/10

Plugin Output

tcp/2078/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: 2023/07/10

Plugin Output

tcp/2080/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: 2023/07/10

Plugin Output

tcp/2083/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: 2023/07/10

Plugin Output

tcp/2087/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: 2023/07/10

Plugin Output

tcp/2096/www

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

56472 - SSL Certificate Chain Contains Unnecessary Certificates

Synopsis

The X.509 certificate chain used by this service contains certificates that aren't required to form a path to the CA.

Description

At least one of the X.509 certificates sent by the remote host is not required to form a path from the server's own certificate to the CA. This may indicate that the certificate bundle installed with the server's certificate is for certificates lower in the certificate hierarchy.

Some SSL implementations, often those found in embedded devices, cannot handle certificate chains with unused certificates.

See Also

http://www.ietf.org/rfc/rfc4346.txt

Solution

Remove unnecessary certificates from the certificate chain.

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2012/01/17

Plugin Output

tcp/110/pop3

```
The following certificates were part of the certificate chain
sent by the remote host, but are not necessary to building the
certificate chain.

|-Organization Unit: generated by AVG Antivirus for SSL/TLS scanning
|-Organization: AVG Web/Mail Shield
|-Common Name: AVG Web/Mail Shield Root
```

56472 - SSL Certificate Chain Contains Unnecessary Certificates

Synopsis

The X.509 certificate chain used by this service contains certificates that aren't required to form a path to the CA.

Description

At least one of the X.509 certificates sent by the remote host is not required to form a path from the server's own certificate to the CA. This may indicate that the certificate bundle installed with the server's certificate is for certificates lower in the certificate hierarchy.

Some SSL implementations, often those found in embedded devices, cannot handle certificate chains with unused certificates.

See Also

http://www.ietf.org/rfc/rfc4346.txt

Solution

Remove unnecessary certificates from the certificate chain.

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2012/01/17

Plugin Output

tcp/143/imap

```
The following certificates were part of the certificate chain
sent by the remote host, but are not necessary to building the
certificate chain.

|-Organization Unit: generated by AVG Antivirus for SSL/TLS scanning
|-Organization: AVG Web/Mail Shield
|-Common Name: AVG Web/Mail Shield Root
```

56472 - SSL Certificate Chain Contains Unnecessary Certificates

Synopsis

The X.509 certificate chain used by this service contains certificates that aren't required to form a path to the CA.

Description

At least one of the X.509 certificates sent by the remote host is not required to form a path from the server's own certificate to the CA. This may indicate that the certificate bundle installed with the server's certificate is for certificates lower in the certificate hierarchy.

Some SSL implementations, often those found in embedded devices, cannot handle certificate chains with unused certificates.

See Also

http://www.ietf.org/rfc/rfc4346.txt

Solution

Remove unnecessary certificates from the certificate chain.

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2012/01/17

Plugin Output

tcp/465/smtp

```
The following certificates were part of the certificate chain
sent by the remote host, but are not necessary to building the
certificate chain.

|-Organization Unit: generated by AVG Antivirus for SSL/TLS scanning
|-Organization: AVG Web/Mail Shield
|-Common Name: AVG Web/Mail Shield Root
```

56472 - SSL Certificate Chain Contains Unnecessary Certificates

Synopsis

The X.509 certificate chain used by this service contains certificates that aren't required to form a path to the CA.

Description

At least one of the X.509 certificates sent by the remote host is not required to form a path from the server's own certificate to the CA. This may indicate that the certificate bundle installed with the server's certificate is for certificates lower in the certificate hierarchy.

Some SSL implementations, often those found in embedded devices, cannot handle certificate chains with unused certificates.

See Also

http://www.ietf.org/rfc/rfc4346.txt

Solution

Remove unnecessary certificates from the certificate chain.

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2012/01/17

Plugin Output

tcp/993/imap

```
The following certificates were part of the certificate chain
sent by the remote host, but are not necessary to building the
certificate chain.

|-Organization Unit: generated by AVG Antivirus for SSL/TLS scanning
|-Organization: AVG Web/Mail Shield
|-Common Name: AVG Web/Mail Shield Root
```

56472 - SSL Certificate Chain Contains Unnecessary Certificates

Synopsis

The X.509 certificate chain used by this service contains certificates that aren't required to form a path to the CA.

Description

At least one of the X.509 certificates sent by the remote host is not required to form a path from the server's own certificate to the CA. This may indicate that the certificate bundle installed with the server's certificate is for certificates lower in the certificate hierarchy.

Some SSL implementations, often those found in embedded devices, cannot handle certificate chains with unused certificates.

See Also

http://www.ietf.org/rfc/rfc4346.txt

Solution

Remove unnecessary certificates from the certificate chain.

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2012/01/17

Plugin Output

tcp/995/pop3

```

The following certificates were part of the certificate chain
sent by the remote host, but are not necessary to building the
certificate chain.

|-Organization Unit: generated by AVG Antivirus for SSL/TLS scanning
|-Organization: AVG Web/Mail Shield
|-Common Name: AVG Web/Mail Shield Root
```

56471 - SSL Certificate Chain Not Sorted

Synopsis

The X.509 certificate chain used by this service contains certificates that aren't in order.

Description

At least one of the X.509 certificates sent by the remote host is not in order. Some certificate authorities publish certificate bundles that are in descending instead of ascending order, which is incorrect according to RFC 4346, Section 7.4.2.

Some SSL implementations, often those found in embedded devices, cannot handle unordered certificate chains.

See Also

http://www.ietf.org/rfc/rfc4346.txt

Solution

Reorder the certificates in the certificate chain.

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2012/01/17

Plugin Output

tcp/110/pop3

```
The certificate chain sent by the remote host is not in order :

|-Subject : OU=generated by AVG Antivirus for SSL/TLS scanning/O=AVG Web/Mail Shield/CN=AVG Web/Mail
 Shield Root
|-Issuer  : OU=generated by AVG Antivirus for SSL/TLS scanning/O=AVG Web/Mail Shield/CN=AVG Web/Mail
 Shield Root
|
|--Subject : CN=server.cbw.pmj.mybluehostin.me
|--Issuer  : OU=generated by AVG Antivirus for untrusted server certificates/O=AVG Web/Mail Shield/
CN=AVG Web/Mail Shield Untrusted Root
```

56471 - SSL Certificate Chain Not Sorted

Synopsis

The X.509 certificate chain used by this service contains certificates that aren't in order.

Description

At least one of the X.509 certificates sent by the remote host is not in order. Some certificate authorities publish certificate bundles that are in descending instead of ascending order, which is incorrect according to RFC 4346, Section 7.4.2.

Some SSL implementations, often those found in embedded devices, cannot handle unordered certificate chains.

See Also

http://www.ietf.org/rfc/rfc4346.txt

Solution

Reorder the certificates in the certificate chain.

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2012/01/17

Plugin Output

tcp/143/imap

```
The certificate chain sent by the remote host is not in order :

|-Subject : OU=generated by AVG Antivirus for SSL/TLS scanning/O=AVG Web/Mail Shield/CN=AVG Web/Mail
 Shield Root
|-Issuer  : OU=generated by AVG Antivirus for SSL/TLS scanning/O=AVG Web/Mail Shield/CN=AVG Web/Mail
 Shield Root
|
|--Subject : CN=server.cbw.pmj.mybluehostin.me
|--Issuer  : OU=generated by AVG Antivirus for untrusted server certificates/O=AVG Web/Mail Shield/
CN=AVG Web/Mail Shield Untrusted Root
```

56471 - SSL Certificate Chain Not Sorted

Synopsis

The X.509 certificate chain used by this service contains certificates that aren't in order.

Description

At least one of the X.509 certificates sent by the remote host is not in order. Some certificate authorities publish certificate bundles that are in descending instead of ascending order, which is incorrect according to RFC 4346, Section 7.4.2.

Some SSL implementations, often those found in embedded devices, cannot handle unordered certificate chains.

See Also

http://www.ietf.org/rfc/rfc4346.txt

Solution

Reorder the certificates in the certificate chain.

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2012/01/17

Plugin Output

tcp/465/smtp

```
The certificate chain sent by the remote host is not in order :

|-Subject : OU=generated by AVG Antivirus for SSL/TLS scanning/O=AVG Web/Mail Shield/CN=AVG Web/Mail
 Shield Root
|-Issuer  : OU=generated by AVG Antivirus for SSL/TLS scanning/O=AVG Web/Mail Shield/CN=AVG Web/Mail
 Shield Root
|
|--Subject : CN=server.cbw.pmj.mybluehostin.me
|--Issuer  : OU=generated by AVG Antivirus for untrusted server certificates/O=AVG Web/Mail Shield/
CN=AVG Web/Mail Shield Untrusted Root
```

56471 - SSL Certificate Chain Not Sorted

Synopsis

The X.509 certificate chain used by this service contains certificates that aren't in order.

Description

At least one of the X.509 certificates sent by the remote host is not in order. Some certificate authorities publish certificate bundles that are in descending instead of ascending order, which is incorrect according to RFC 4346, Section 7.4.2.

Some SSL implementations, often those found in embedded devices, cannot handle unordered certificate chains.

See Also

http://www.ietf.org/rfc/rfc4346.txt

Solution

Reorder the certificates in the certificate chain.

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2012/01/17

Plugin Output

tcp/993/imap

```

The certificate chain sent by the remote host is not in order :

|-Subject : OU=generated by AVG Antivirus for SSL/TLS scanning/O=AVG Web/Mail Shield/CN=AVG Web/Mail
 Shield Root
|-Issuer  : OU=generated by AVG Antivirus for SSL/TLS scanning/O=AVG Web/Mail Shield/CN=AVG Web/Mail
 Shield Root
|
|--Subject : CN=server.cbw.pmj.mybluehostin.me
|--Issuer  : OU=generated by AVG Antivirus for untrusted server certificates/O=AVG Web/Mail Shield/
CN=AVG Web/Mail Shield Untrusted Root
```

56471 - SSL Certificate Chain Not Sorted

Synopsis

The X.509 certificate chain used by this service contains certificates that aren't in order.

Description

At least one of the X.509 certificates sent by the remote host is not in order. Some certificate authorities publish certificate bundles that are in descending instead of ascending order, which is incorrect according to RFC 4346, Section 7.4.2.

Some SSL implementations, often those found in embedded devices, cannot handle unordered certificate chains.

See Also

http://www.ietf.org/rfc/rfc4346.txt

Solution

Reorder the certificates in the certificate chain.

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2012/01/17

Plugin Output

tcp/995/pop3

```
The certificate chain sent by the remote host is not in order :

|-Subject : OU=generated by AVG Antivirus for SSL/TLS scanning/O=AVG Web/Mail Shield/CN=AVG Web/Mail
 Shield Root
|-Issuer  : OU=generated by AVG Antivirus for SSL/TLS scanning/O=AVG Web/Mail Shield/CN=AVG Web/Mail
 Shield Root
|
|--Subject : CN=server.cbw.pmj.mybluehostin.me
|--Issuer  : OU=generated by AVG Antivirus for untrusted server certificates/O=AVG Web/Mail Shield/
CN=AVG Web/Mail Shield Untrusted Root
```

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: server.cbw.pmj.mybluehostin.me

Issuer Name:

Organization Unit: generated by AVG Antivirus for untrusted server certificates
Organization: AVG Web/Mail Shield
Common Name: AVG Web/Mail Shield Untrusted Root

Serial Number: 1A DD A0 8D 89 10 FD 46 AA BF 33 9D 7E 88 32 53

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BA 49 52 25 68 92 A4 7D E5 E1 42 A6 41 E0 77 16 5B E5 DA
            DE 02 0C 35 A6 11 0A 2C 3A 2B 44 35 DB 43 E0 2F 95 70 34 67
            7E 14 1A 83 6D D8 8D EF 4D 85 9E 41 B4 28 5D 94 F7 D6 55 70
            65 8C 93 D8 1F 13 F8 51 2F 5B F1 9F 6E 92 36 BF 4A 16 6E 6D
            1A 41 EE 7C 27 DD 64 36 9A 4B 71 AD 85 B2 47 3D 36 7D DB BF
            C8 D5 0C 9F CD B9 9F 44 5E 8B 9B 02 3B A8 81 A7 35 62 E3 0B
            BF 3A 45 C5 37 26 1E 77 ED 23 AA 1F 90 6F FA 60 B2 F0 78 3B
            95 D2 CA 8E D1 72 6A C1 67 29 13 5F ED 72 C0 E4 42 FB 75 DC
            B1 4A 7C BF 52 97 3B C0 D7 FD 44 EB CC 2F 99 A4 A3 9B 0B 9C
```

```
             5E F0 C5 C9 48 55 C2 ED DF 34 70 6F E7 E0 9F B8 63 3B A8 45
             09 B5 67 47 16 B2 03 DC B9 7A AA 1E 19 BA F9 2A 15 4B 70 0E
             56 7E C4 4C 60 17 7E 57 0C BA 4C 28 58 44 06 A8 9E 59 98 32
             24 68 29 50 82 6D FA ED 3A 81 02 D0 19 97 1F E5 57
 Exponent: 01 00 01

 Signature Length: 256 bytes / 2048 bits
 Signature: 00 7F 3C 52 86 F6 01 C8 4B B7 95 00 BA D7 C4 0F EE 82 DF 35
            49 35 96 53 95 BD 20 8C D8 B5 59 9D 6B ED 0B 20 BB 42 97 96
            6E EB E6 48 7C F8 A0 24 1B 32 00 1D 84 2C FA 43 AA CE 9F 31
            F2 E8 E0 06 F3 2A 02 76 D6 CD 3E 19 B9 D8 35 55 D0 F8 6D 7F
            6B 66 F1 DB 32 9D FD 87 97 E2 24 40 CF 1F 02 EE 3E B0 BB C3
            DD 20 71 DC F9 B6 59 C0 2A 97 1E B4 E1 32 3A CC 90 26 50 63
            00 FD 7F 3F 15 F4 A5 99 55 85 A3 15 B6 0E 7E 6E 0B 18 31 F6
            68 52 88 95 4B [...]
```

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: server.cbw.pmj.mybluehostin.me

Issuer Name:

Organization Unit: generated by AVG Antivirus for untrusted server certificates
Organization: AVG Web/Mail Shield
Common Name: AVG Web/Mail Shield Untrusted Root

Serial Number: 1A DD A0 8D 89 10 FD 46 AA BF 33 9D 7E 88 32 53

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BA 49 52 25 68 92 A4 7D E5 E1 42 A6 41 E0 77 16 5B E5 DA
            DE 02 0C 35 A6 11 0A 2C 3A 2B 44 35 DB 43 E0 2F 95 70 34 67
            7E 14 1A 83 6D D8 8D EF 4D 85 9E 41 B4 28 5D 94 F7 D6 55 70
            65 8C 93 D8 1F 13 F8 51 2F 5B F1 9F 6E 92 36 BF 4A 16 6E 6D
            1A 41 EE 7C 27 DD 64 36 9A 4B 71 AD 85 B2 47 3D 36 7D DB BF
            C8 D5 0C 9F CD B9 9F 44 5E 8B 9B 02 3B A8 81 A7 35 62 E3 0B
            BF 3A 45 C5 37 26 1E 77 ED 23 AA 1F 90 6F FA 60 B2 F0 78 3B
            95 D2 CA 8E D1 72 6A C1 67 29 13 5F ED 72 C0 E4 42 FB 75 DC
            B1 4A 7C BF 52 97 3B C0 D7 FD 44 EB CC 2F 99 A4 A3 9B 0B 9C
```

```
             5E F0 C5 C9 48 55 C2 ED DF 34 70 6F E7 E0 9F B8 63 3B A8 45
             09 B5 67 47 16 B2 03 DC B9 7A AA 1E 19 BA F9 2A 15 4B 70 0E
             56 7E C4 4C 60 17 7E 57 0C BA 4C 28 58 44 06 A8 9E 59 98 32
             24 68 29 50 82 6D FA ED 3A 81 02 D0 19 97 1F E5 57
 Exponent: 01 00 01

 Signature Length: 256 bytes / 2048 bits
 Signature: 00 7F 3C 52 86 F6 01 C8 4B B7 95 00 BA D7 C4 0F EE 82 DF 35
            49 35 96 53 95 BD 20 8C D8 B5 59 9D 6B ED 0B 20 BB 42 97 96
            6E EB E6 48 7C F8 A0 24 1B 32 00 1D 84 2C FA 43 AA CE 9F 31
            F2 E8 E0 06 F3 2A 02 76 D6 CD 3E 19 B9 D8 35 55 D0 F8 6D 7F
            6B 66 F1 DB 32 9D FD 87 97 E2 24 40 CF 1F 02 EE 3E B0 BB C3
            DD 20 71 DC F9 B6 59 C0 2A 97 1E B4 E1 32 3A CC 90 26 50 63
            00 FD 7F 3F 15 F4 A5 99 55 85 A3 15 B6 0E 7E 6E 0B 18 31 F6
            68 52 88 95 4B [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

```
Subject Name:

Common Name: server.cbw.pmj.mybluehostin.me

Issuer Name:

Country: US
State/Province: TX
Locality: Houston
Organization: cPanel, Inc.
Common Name: cPanel, Inc. Certification Authority

Serial Number: 1F BE EE 0F 82 EC 3B B7 5C 8E B9 3C 62 1C C5 86

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BE 8A 7D 99 78 74 43 97 A2 7D 3C 5B 14 97 B2 E7 55 26 9B
            B0 F2 94 C2 DB FC ED C0 B2 CC DB A7 3F 06 B2 50 3C 4A 44 12
            22 5E 1D 71 80 85 99 8E 37 C7 10 53 79 E4 50 7D 88 CF 64 BA
            40 1A 1C 76 39 37 98 67 C6 F7 A7 84 2D EC 05 E8 7B 04 4C AF
            90 89 D5 0F 04 25 7B E3 FA AD 88 50 70 AF AA 6B E5 71 1E 22
            E9 4E EB 37 E7 3C 51 00 74 D1 45 F1 4A 97 0D B8 30 EC 93 89
            F2 F7 ED B6 65 5C 13 04 DD 7B 59 CD 72 99 C1 05 7D 58 C5 00
            D7 DF A6 65 FF F1 CE D0 33 9B 19 13 CF 18 2A A0 71 9B 77 D8
            FD DE FA 12 06 72 AD D0 E7 6B 2B A0 34 D3 96 DB 31 45 E3 F8
            7E F9 25 6E 16 B3 87 F4 4A 6C 35 15 5D 26 53 83 21 98 AC 68
            38 3E 62 1F 21 8F 54 A6 C6 B2 36 A6 FE E2 A0 04 E3 BE 3D E4
            3F 14 7B 3E 55 EF 52 44 07 ED EB BC 7C 75 4C F5 93 34 2B B7
            B8 F6 31 F8 39 C8 C8 89 4F 25 8E 32 CA D2 D9 1A 7F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 F4 E6 C4 7B 5C 9C 3C 9A CA 93 E7 E3 42 57 31 7F E8 6B
           A1 A6 03 9C 8D 2B 3E D7 8E C1 46 75 E1 97 B7 51 32 7D 02 EB
           33 42 1A 8C 31 D0 41 71 0A 98 85 22 D7 2C 77 93 8A 71 2E F1
           2F 11 3D AB 88 C6 35 09 98 B3 F9 70 1D 71 C1 D1 9B EA 86 79
           25 9F B1 8A A2 4F 0C BD B3 FD 77 A7 6F 01 2C 20 66 29 86 98
           58 02 7E 97 4E 7B 1E 6B 13 23 36 DC 93 ED 48 70 7E 23 2B 11
           0C A5 73 60 53 41 B8 A1 4A 97 49 DB 97 C4 50 A0 4F 75 8C 2D
           00 45 CA 8A 3C 2E B5 64 83 C8 B1 4A 1A 54 27 C7 4D [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/465/smtp

```
Subject Name:

Common Name: server.cbw.pmj.mybluehostin.me

Issuer Name:

Organization Unit: generated by AVG Antivirus for untrusted server certificates
Organization: AVG Web/Mail Shield
Common Name: AVG Web/Mail Shield Untrusted Root

Serial Number: 32 E5 95 34 0E BD 2E 42 84 20 40 99 3F 69 8D 6D

Version: 1

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BA 49 52 25 68 92 A4 7D E5 E1 42 A6 41 E0 77 16 5B E5 DA
            DE 02 0C 35 A6 11 0A 2C 3A 2B 44 35 DB 43 E0 2F 95 70 34 67
            7E 14 1A 83 6D D8 8D EF 4D 85 9E 41 B4 28 5D 94 F7 D6 55 70
            65 8C 93 D8 1F 13 F8 51 2F 5B F1 9F 6E 92 36 BF 4A 16 6E 6D
            1A 41 EE 7C 27 DD 64 36 9A 4B 71 AD 85 B2 47 3D 36 7D DB BF
            C8 D5 0C 9F CD B9 9F 44 5E 8B 9B 02 3B A8 81 A7 35 62 E3 0B
            BF 3A 45 C5 37 26 1E 77 ED 23 AA 1F 90 6F FA 60 B2 F0 78 3B
            95 D2 CA 8E D1 72 6A C1 67 29 13 5F ED 72 C0 E4 42 FB 75 DC
            B1 4A 7C BF 52 97 3B C0 D7 FD 44 EB CC 2F 99 A4 A3 9B 0B 9C
            5E F0 C5 C9 48 55 C2 ED DF 34 70 6F E7 E0 9F B8 63 3B A8 45
            09 B5 67 47 16 B2 03 DC B9 7A AA 1E 19 BA F9 2A 15 4B 70 0E
            56 7E C4 4C 60 17 7E 57 0C BA 4C 28 58 44 06 A8 9E 59 98 32
            24 68 29 50 82 6D FA ED 3A 81 02 D0 19 97 1F E5 57
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 33 8C 89 80 2A 80 6E AB FF 95 4C 42 0A A4 71 D0 A4 12 F5
           C8 6B BF 18 9C A7 11 33 92 95 AC 74 52 2A 9B 5A 87 3A 32 29
           E7 54 DA A9 C9 07 6E E1 14 DA 2E 69 C4 77 DF E9 0C C3 9F 32
           9F 87 8C 34 5F 9A 49 7E 89 C6 29 C7 12 8D 87 8E 42 5B 83 AB
           4D CE 1B C2 E4 3F 52 C4 01 59 47 B5 52 59 D2 C4 8E 95 CE 74
           EC E6 0F D4 71 94 2A 8B 4E C2 B1 E3 82 AF 70 F9 35 39 CE 5E
           6C 4A C1 CD 7A 87 A7 AA 0C 0A A5 7A 82 A9 78 D6 D7 52 A2 50
           8C 16 D9 7A FF [...]
```

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: server.cbw.pmj.mybluehostin.me

Issuer Name:

Organization Unit: generated by AVG Antivirus for untrusted server certificates
Organization: AVG Web/Mail Shield
Common Name: AVG Web/Mail Shield Untrusted Root

Serial Number: 1A DD A0 8D 89 10 FD 46 AA BF 33 9D 7E 88 32 53

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BA 49 52 25 68 92 A4 7D E5 E1 42 A6 41 E0 77 16 5B E5 DA
            DE 02 0C 35 A6 11 0A 2C 3A 2B 44 35 DB 43 E0 2F 95 70 34 67
            7E 14 1A 83 6D D8 8D EF 4D 85 9E 41 B4 28 5D 94 F7 D6 55 70
            65 8C 93 D8 1F 13 F8 51 2F 5B F1 9F 6E 92 36 BF 4A 16 6E 6D
            1A 41 EE 7C 27 DD 64 36 9A 4B 71 AD 85 B2 47 3D 36 7D DB BF
            C8 D5 0C 9F CD B9 9F 44 5E 8B 9B 02 3B A8 81 A7 35 62 E3 0B
            BF 3A 45 C5 37 26 1E 77 ED 23 AA 1F 90 6F FA 60 B2 F0 78 3B
            95 D2 CA 8E D1 72 6A C1 67 29 13 5F ED 72 C0 E4 42 FB 75 DC
            B1 4A 7C BF 52 97 3B C0 D7 FD 44 EB CC 2F 99 A4 A3 9B 0B 9C
```

```
             5E F0 C5 C9 48 55 C2 ED DF 34 70 6F E7 E0 9F B8 63 3B A8 45
             09 B5 67 47 16 B2 03 DC B9 7A AA 1E 19 BA F9 2A 15 4B 70 0E
             56 7E C4 4C 60 17 7E 57 0C BA 4C 28 58 44 06 A8 9E 59 98 32
             24 68 29 50 82 6D FA ED 3A 81 02 D0 19 97 1F E5 57
 Exponent: 01 00 01

 Signature Length: 256 bytes / 2048 bits
 Signature: 00 7F 3C 52 86 F6 01 C8 4B B7 95 00 BA D7 C4 0F EE 82 DF 35
            49 35 96 53 95 BD 20 8C D8 B5 59 9D 6B ED 0B 20 BB 42 97 96
            6E EB E6 48 7C F8 A0 24 1B 32 00 1D 84 2C FA 43 AA CE 9F 31
            F2 E8 E0 06 F3 2A 02 76 D6 CD 3E 19 B9 D8 35 55 D0 F8 6D 7F
            6B 66 F1 DB 32 9D FD 87 97 E2 24 40 CF 1F 02 EE 3E B0 BB C3
            DD 20 71 DC F9 B6 59 C0 2A 97 1E B4 E1 32 3A CC 90 26 50 63
            00 FD 7F 3F 15 F4 A5 99 55 85 A3 15 B6 0E 7E 6E 0B 18 31 F6
            68 52 88 95 4B [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/995/pop3

```
Subject Name:

Common Name: server.cbw.pmj.mybluehostin.me

Issuer Name:

Organization Unit: generated by AVG Antivirus for untrusted server certificates
Organization: AVG Web/Mail Shield
Common Name: AVG Web/Mail Shield Untrusted Root

Serial Number: 1A DD A0 8D 89 10 FD 46 AA BF 33 9D 7E 88 32 53

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BA 49 52 25 68 92 A4 7D E5 E1 42 A6 41 E0 77 16 5B E5 DA
            DE 02 0C 35 A6 11 0A 2C 3A 2B 44 35 DB 43 E0 2F 95 70 34 67
            7E 14 1A 83 6D D8 8D EF 4D 85 9E 41 B4 28 5D 94 F7 D6 55 70
            65 8C 93 D8 1F 13 F8 51 2F 5B F1 9F 6E 92 36 BF 4A 16 6E 6D
            1A 41 EE 7C 27 DD 64 36 9A 4B 71 AD 85 B2 47 3D 36 7D DB BF
            C8 D5 0C 9F CD B9 9F 44 5E 8B 9B 02 3B A8 81 A7 35 62 E3 0B
            BF 3A 45 C5 37 26 1E 77 ED 23 AA 1F 90 6F FA 60 B2 F0 78 3B
            95 D2 CA 8E D1 72 6A C1 67 29 13 5F ED 72 C0 E4 42 FB 75 DC
            B1 4A 7C BF 52 97 3B C0 D7 FD 44 EB CC 2F 99 A4 A3 9B 0B 9C
            5E F0 C5 C9 48 55 C2 ED DF 34 70 6F E7 E0 9F B8 63 3B A8 45
            09 B5 67 47 16 B2 03 DC B9 7A AA 1E 19 BA F9 2A 15 4B 70 0E
            56 7E C4 4C 60 17 7E 57 0C BA 4C 28 58 44 06 A8 9E 59 98 32
            24 68 29 50 82 6D FA ED 3A 81 02 D0 19 97 1F E5 57
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 7F 3C 52 86 F6 01 C8 4B B7 95 00 BA D7 C4 0F EE 82 DF 35
           49 35 96 53 95 BD 20 8C D8 B5 59 9D 6B ED 0B 20 BB 42 97 96
           6E EB E6 48 7C F8 A0 24 1B 32 00 1D 84 2C FA 43 AA CE 9F 31
           F2 E8 E0 06 F3 2A 02 76 D6 CD 3E 19 B9 D8 35 55 D0 F8 6D 7F
           6B 66 F1 DB 32 9D FD 87 97 E2 24 40 CF 1F 02 EE 3E B0 BB C3
           DD 20 71 DC F9 B6 59 C0 2A 97 1E B4 E1 32 3A CC 90 26 50 63
           00 FD 7F 3F 15 F4 A5 99 55 85 A3 15 B6 0E 7E 6E 0B 18 31 F6
           68 52 88 95 4B [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2078/www

```
Subject Name:

Common Name: server.cbw.pmj.mybluehostin.me

Issuer Name:

Country: US
State/Province: TX
Locality: Houston
Organization: cPanel, Inc.
Common Name: cPanel, Inc. Certification Authority

Serial Number: 1F BE EE 0F 82 EC 3B B7 5C 8E B9 3C 62 1C C5 86

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BE 8A 7D 99 78 74 43 97 A2 7D 3C 5B 14 97 B2 E7 55 26 9B
            B0 F2 94 C2 DB FC ED C0 B2 CC DB A7 3F 06 B2 50 3C 4A 44 12
            22 5E 1D 71 80 85 99 8E 37 C7 10 53 79 E4 50 7D 88 CF 64 BA
            40 1A 1C 76 39 37 98 67 C6 F7 A7 84 2D EC 05 E8 7B 04 4C AF
            90 89 D5 0F 04 25 7B E3 FA AD 88 50 70 AF AA 6B E5 71 1E 22
            E9 4E EB 37 E7 3C 51 00 74 D1 45 F1 4A 97 0D B8 30 EC 93 89
            F2 F7 ED B6 65 5C 13 04 DD 7B 59 CD 72 99 C1 05 7D 58 C5 00
            D7 DF A6 65 FF F1 CE D0 33 9B 19 13 CF 18 2A A0 71 9B 77 D8
            FD DE FA 12 06 72 AD D0 E7 6B 2B A0 34 D3 96 DB 31 45 E3 F8
            7E F9 25 6E 16 B3 87 F4 4A 6C 35 15 5D 26 53 83 21 98 AC 68
            38 3E 62 1F 21 8F 54 A6 C6 B2 36 A6 FE E2 A0 04 E3 BE 3D E4
            3F 14 7B 3E 55 EF 52 44 07 ED EB BC 7C 75 4C F5 93 34 2B B7
            B8 F6 31 F8 39 C8 C8 89 4F 25 8E 32 CA D2 D9 1A 7F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 F4 E6 C4 7B 5C 9C 3C 9A CA 93 E7 E3 42 57 31 7F E8 6B
           A1 A6 03 9C 8D 2B 3E D7 8E C1 46 75 E1 97 B7 51 32 7D 02 EB
           33 42 1A 8C 31 D0 41 71 0A 98 85 22 D7 2C 77 93 8A 71 2E F1
           2F 11 3D AB 88 C6 35 09 98 B3 F9 70 1D 71 C1 D1 9B EA 86 79
           25 9F B1 8A A2 4F 0C BD B3 FD 77 A7 6F 01 2C 20 66 29 86 98
           58 02 7E 97 4E 7B 1E 6B 13 23 36 DC 93 ED 48 70 7E 23 2B 11
           0C A5 73 60 53 41 B8 A1 4A 97 49 DB 97 C4 50 A0 4F 75 8C 2D
           00 45 CA 8A 3C 2E B5 64 83 C8 B1 4A 1A 54 27 C7 4D [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2080/www

```
Subject Name:

Common Name: server.cbw.pmj.mybluehostin.me

Issuer Name:

Country: US
State/Province: TX
Locality: Houston
Organization: cPanel, Inc.
Common Name: cPanel, Inc. Certification Authority

Serial Number: 1F BE EE 0F 82 EC 3B B7 5C 8E B9 3C 62 1C C5 86

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BE 8A 7D 99 78 74 43 97 A2 7D 3C 5B 14 97 B2 E7 55 26 9B
            B0 F2 94 C2 DB FC ED C0 B2 CC DB A7 3F 06 B2 50 3C 4A 44 12
            22 5E 1D 71 80 85 99 8E 37 C7 10 53 79 E4 50 7D 88 CF 64 BA
            40 1A 1C 76 39 37 98 67 C6 F7 A7 84 2D EC 05 E8 7B 04 4C AF
            90 89 D5 0F 04 25 7B E3 FA AD 88 50 70 AF AA 6B E5 71 1E 22
            E9 4E EB 37 E7 3C 51 00 74 D1 45 F1 4A 97 0D B8 30 EC 93 89
            F2 F7 ED B6 65 5C 13 04 DD 7B 59 CD 72 99 C1 05 7D 58 C5 00
            D7 DF A6 65 FF F1 CE D0 33 9B 19 13 CF 18 2A A0 71 9B 77 D8
            FD DE FA 12 06 72 AD D0 E7 6B 2B A0 34 D3 96 DB 31 45 E3 F8
            7E F9 25 6E 16 B3 87 F4 4A 6C 35 15 5D 26 53 83 21 98 AC 68
            38 3E 62 1F 21 8F 54 A6 C6 B2 36 A6 FE E2 A0 04 E3 BE 3D E4
            3F 14 7B 3E 55 EF 52 44 07 ED EB BC 7C 75 4C F5 93 34 2B B7
            B8 F6 31 F8 39 C8 C8 89 4F 25 8E 32 CA D2 D9 1A 7F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 F4 E6 C4 7B 5C 9C 3C 9A CA 93 E7 E3 42 57 31 7F E8 6B
           A1 A6 03 9C 8D 2B 3E D7 8E C1 46 75 E1 97 B7 51 32 7D 02 EB
           33 42 1A 8C 31 D0 41 71 0A 98 85 22 D7 2C 77 93 8A 71 2E F1
           2F 11 3D AB 88 C6 35 09 98 B3 F9 70 1D 71 C1 D1 9B EA 86 79
           25 9F B1 8A A2 4F 0C BD B3 FD 77 A7 6F 01 2C 20 66 29 86 98
           58 02 7E 97 4E 7B 1E 6B 13 23 36 DC 93 ED 48 70 7E 23 2B 11
           0C A5 73 60 53 41 B8 A1 4A 97 49 DB 97 C4 50 A0 4F 75 8C 2D
           00 45 CA 8A 3C 2E B5 64 83 C8 B1 4A 1A 54 27 C7 4D [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2083/www

```
Subject Name:

Common Name: server.cbw.pmj.mybluehostin.me

Issuer Name:

Country: US
State/Province: TX
Locality: Houston
Organization: cPanel, Inc.
Common Name: cPanel, Inc. Certification Authority

Serial Number: 1F BE EE 0F 82 EC 3B B7 5C 8E B9 3C 62 1C C5 86

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BE 8A 7D 99 78 74 43 97 A2 7D 3C 5B 14 97 B2 E7 55 26 9B
            B0 F2 94 C2 DB FC ED C0 B2 CC DB A7 3F 06 B2 50 3C 4A 44 12
            22 5E 1D 71 80 85 99 8E 37 C7 10 53 79 E4 50 7D 88 CF 64 BA
            40 1A 1C 76 39 37 98 67 C6 F7 A7 84 2D EC 05 E8 7B 04 4C AF
            90 89 D5 0F 04 25 7B E3 FA AD 88 50 70 AF AA 6B E5 71 1E 22
            E9 4E EB 37 E7 3C 51 00 74 D1 45 F1 4A 97 0D B8 30 EC 93 89
            F2 F7 ED B6 65 5C 13 04 DD 7B 59 CD 72 99 C1 05 7D 58 C5 00
            D7 DF A6 65 FF F1 CE D0 33 9B 19 13 CF 18 2A A0 71 9B 77 D8
            FD DE FA 12 06 72 AD D0 E7 6B 2B A0 34 D3 96 DB 31 45 E3 F8
            7E F9 25 6E 16 B3 87 F4 4A 6C 35 15 5D 26 53 83 21 98 AC 68
            38 3E 62 1F 21 8F 54 A6 C6 B2 36 A6 FE E2 A0 04 E3 BE 3D E4
            3F 14 7B 3E 55 EF 52 44 07 ED EB BC 7C 75 4C F5 93 34 2B B7
            B8 F6 31 F8 39 C8 C8 89 4F 25 8E 32 CA D2 D9 1A 7F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 F4 E6 C4 7B 5C 9C 3C 9A CA 93 E7 E3 42 57 31 7F E8 6B
           A1 A6 03 9C 8D 2B 3E D7 8E C1 46 75 E1 97 B7 51 32 7D 02 EB
           33 42 1A 8C 31 D0 41 71 0A 98 85 22 D7 2C 77 93 8A 71 2E F1
           2F 11 3D AB 88 C6 35 09 98 B3 F9 70 1D 71 C1 D1 9B EA 86 79
           25 9F B1 8A A2 4F 0C BD B3 FD 77 A7 6F 01 2C 20 66 29 86 98
           58 02 7E 97 4E 7B 1E 6B 13 23 36 DC 93 ED 48 70 7E 23 2B 11
           0C A5 73 60 53 41 B8 A1 4A 97 49 DB 97 C4 50 A0 4F 75 8C 2D
           00 45 CA 8A 3C 2E B5 64 83 C8 B1 4A 1A 54 27 C7 4D [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2087/www

```
Subject Name:

Common Name: server.cbw.pmj.mybluehostin.me

Issuer Name:

Country: US
State/Province: TX
Locality: Houston
Organization: cPanel, Inc.
Common Name: cPanel, Inc. Certification Authority

Serial Number: 1F BE EE 0F 82 EC 3B B7 5C 8E B9 3C 62 1C C5 86

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BE 8A 7D 99 78 74 43 97 A2 7D 3C 5B 14 97 B2 E7 55 26 9B
            B0 F2 94 C2 DB FC ED C0 B2 CC DB A7 3F 06 B2 50 3C 4A 44 12
            22 5E 1D 71 80 85 99 8E 37 C7 10 53 79 E4 50 7D 88 CF 64 BA
            40 1A 1C 76 39 37 98 67 C6 F7 A7 84 2D EC 05 E8 7B 04 4C AF
            90 89 D5 0F 04 25 7B E3 FA AD 88 50 70 AF AA 6B E5 71 1E 22
            E9 4E EB 37 E7 3C 51 00 74 D1 45 F1 4A 97 0D B8 30 EC 93 89
            F2 F7 ED B6 65 5C 13 04 DD 7B 59 CD 72 99 C1 05 7D 58 C5 00
            D7 DF A6 65 FF F1 CE D0 33 9B 19 13 CF 18 2A A0 71 9B 77 D8
            FD DE FA 12 06 72 AD D0 E7 6B 2B A0 34 D3 96 DB 31 45 E3 F8
            7E F9 25 6E 16 B3 87 F4 4A 6C 35 15 5D 26 53 83 21 98 AC 68
            38 3E 62 1F 21 8F 54 A6 C6 B2 36 A6 FE E2 A0 04 E3 BE 3D E4
            3F 14 7B 3E 55 EF 52 44 07 ED EB BC 7C 75 4C F5 93 34 2B B7
            B8 F6 31 F8 39 C8 C8 89 4F 25 8E 32 CA D2 D9 1A 7F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 F4 E6 C4 7B 5C 9C 3C 9A CA 93 E7 E3 42 57 31 7F E8 6B
           A1 A6 03 9C 8D 2B 3E D7 8E C1 46 75 E1 97 B7 51 32 7D 02 EB
           33 42 1A 8C 31 D0 41 71 0A 98 85 22 D7 2C 77 93 8A 71 2E F1
           2F 11 3D AB 88 C6 35 09 98 B3 F9 70 1D 71 C1 D1 9B EA 86 79
           25 9F B1 8A A2 4F 0C BD B3 FD 77 A7 6F 01 2C 20 66 29 86 98
           58 02 7E 97 4E 7B 1E 6B 13 23 36 DC 93 ED 48 70 7E 23 2B 11
           0C A5 73 60 53 41 B8 A1 4A 97 49 DB 97 C4 50 A0 4F 75 8C 2D
           00 45 CA 8A 3C 2E B5 64 83 C8 B1 4A 1A 54 27 C7 4D [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2096/www

```
Subject Name:

Common Name: server.cbw.pmj.mybluehostin.me

Issuer Name:

Country: US
State/Province: TX
Locality: Houston
Organization: cPanel, Inc.
Common Name: cPanel, Inc. Certification Authority

Serial Number: 1F BE EE 0F 82 EC 3B B7 5C 8E B9 3C 62 1C C5 86

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 18 00:00:00 2023 GMT
Not Valid After: Jan 18 23:59:59 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BE 8A 7D 99 78 74 43 97 A2 7D 3C 5B 14 97 B2 E7 55 26 9B
            B0 F2 94 C2 DB FC ED C0 B2 CC DB A7 3F 06 B2 50 3C 4A 44 12
            22 5E 1D 71 80 85 99 8E 37 C7 10 53 79 E4 50 7D 88 CF 64 BA
            40 1A 1C 76 39 37 98 67 C6 F7 A7 84 2D EC 05 E8 7B 04 4C AF
            90 89 D5 0F 04 25 7B E3 FA AD 88 50 70 AF AA 6B E5 71 1E 22
            E9 4E EB 37 E7 3C 51 00 74 D1 45 F1 4A 97 0D B8 30 EC 93 89
            F2 F7 ED B6 65 5C 13 04 DD 7B 59 CD 72 99 C1 05 7D 58 C5 00
```

```
             D7 DF A6 65 FF F1 CE D0 33 9B 19 13 CF 18 2A A0 71 9B 77 D8
             FD DE FA 12 06 72 AD D0 E7 6B 2B A0 34 D3 96 DB 31 45 E3 F8
             7E F9 25 6E 16 B3 87 F4 4A 6C 35 15 5D 26 53 83 21 98 AC 68
             38 3E 62 1F 21 8F 54 A6 C6 B2 36 A6 FE E2 A0 04 E3 BE 3D E4
             3F 14 7B 3E 55 EF 52 44 07 ED EB BC 7C 75 4C F5 93 34 2B B7
             B8 F6 31 F8 39 C8 C8 89 4F 25 8E 32 CA D2 D9 1A 7F
 Exponent: 01 00 01

 Signature Length: 256 bytes / 2048 bits
 Signature: 00 50 F4 E6 C4 7B 5C 9C 3C 9A CA 93 E7 E3 42 57 31 7F E8 6B
            A1 A6 03 9C 8D 2B 3E D7 8E C1 46 75 E1 97 B7 51 32 7D 02 EB
            33 42 1A 8C 31 D0 41 71 0A 98 85 22 D7 2C 77 93 8A 71 2E F1
            2F 11 3D AB 88 C6 35 09 98 B3 F9 70 1D 71 C1 D1 9B EA 86 79
            25 9F B1 8A A2 4F 0C BD B3 FD 77 A7 6F 01 2C 20 66 29 86 98
            58 02 7E 97 4E 7B 1E 6B 13 23 36 DC 93 ED 48 70 7E 23 2B 11
            0C A5 73 60 53 41 B8 A1 4A 97 49 DB 97 C4 50 A0 4F 75 8C 2D
            00 45 CA 8A 3C 2E B5 64 83 C8 B1 4A 1A 54 27 C7 4D [...]
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/443/www

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

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

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/2078/www

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

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgo
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/2080/www

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

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgo
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/2083/www

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

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

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/2087/www

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

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgo
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

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

Synopsis

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

Description

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

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

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

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

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

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

Plugin Output

tcp/2096/www

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

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

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 :

  High Strength Ciphers (>= 112-bit key)

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

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

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
```

```
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

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

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/465/smtp

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    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
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
```

```
     ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
  SHA384
     RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
  SHA256
     RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
  SHA256

 The fields above are :

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

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/993/imap

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
```

```
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

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

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/995/pop3

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
```

```
     ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
  SHA384
     RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
  SHA256
     RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
  SHA256

 The fields above are :

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

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

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 : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01       -             -        AES-GCM(128)
 AEAD


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

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

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


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

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

The fields above are :

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

Note that this servic [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

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 : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01       -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02       -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03       -             -        ChaCha20-Poly1305(256)
 AEAD


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

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

```
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
SHA256
   RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
AEAD
   RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
AEAD
   RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
AEAD
   RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
AEAD
   RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA       [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/443/www

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

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

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-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
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
```

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

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/465/smtp

```

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01       -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02       -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03       -             -        ChaCha20-Poly1305(256)
 AEAD


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

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

```
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
SHA256
   RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
AEAD
   RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
AEAD
   RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
AEAD
   RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
AEAD
   RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA       [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

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 : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01       -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02       -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03       -             -        ChaCha20-Poly1305(256)
 AEAD


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

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

```
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
SHA256
   RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
AEAD
   RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
AEAD
   RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
AEAD
   RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
AEAD
   RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA       [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/995/pop3

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01       -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02       -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03       -             -        ChaCha20-Poly1305(256)
 AEAD


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

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

```
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
SHA256
   RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
AEAD
   RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
AEAD
   RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
AEAD
   RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
AEAD
   RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA       [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/2078/www

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

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

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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/2080/www

```

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

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

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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/2083/www

```

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

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

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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/2087/www

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

SSL Version : TLSv12
  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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/2096/www

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

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

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

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 :

  High Strength Ciphers (>= 112-bit key)

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

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
```

```
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

```

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-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
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256
```

```
  The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/465/smtp

```

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
```

```
     ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
  SHA256
     ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
  SHA384

 The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/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-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
```

```
    ECDHE-RSA-AES128-SHA256        0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384        0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/995/pop3

```

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
```

```
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2078/www

```

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

  High Strength Ciphers (>= 112-bit key)

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

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2080/www

```

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

  High Strength Ciphers (>= 112-bit key)

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

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2083/www

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

  High Strength Ciphers (>= 112-bit key)

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

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2087/www

```

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

  High Strength Ciphers (>= 112-bit key)

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

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2096/www

```

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

  High Strength Ciphers (>= 112-bit key)

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

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/443/www

```

The following root Certification Authority certificate was found :

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

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2078/www

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

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

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2080/www

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

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

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2083/www

```

The following root Certification Authority certificate was found :

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

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2087/www

```

The following root Certification Authority certificate was found :

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

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2096/www

```

The following root Certification Authority certificate was found :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

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

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2023/07/10

Plugin Output

tcp/110/pop3

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


  High Strength Ciphers (>= 112-bit key)

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

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

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

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2023/07/10

Plugin Output

tcp/143/imap

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


  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
 AEAD
    RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
 AEAD
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
 AEAD
    RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
 AEAD
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

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

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2023/07/10

Plugin Output

tcp/465/smtp

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


  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
 AEAD
    RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
 AEAD
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
 AEAD
    RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
 AEAD
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

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

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2023/07/10

Plugin Output

tcp/993/imap

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


  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
 AEAD
    RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
 AEAD
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
 AEAD
    RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
 AEAD
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

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

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2023/07/10

Plugin Output

tcp/995/pop3

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


  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    RSA-AES-128-CCM-AEAD          0xC0, 0x9C       RSA           RSA      AES-CCM(128)
 AEAD
    RSA-AES-128-CCM8-AEAD         0xC0, 0xA0       RSA           RSA      AES-CCM8(128)
 AEAD
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES-256-CCM-AEAD          0xC0, 0x9D       RSA           RSA      AES-CCM(256)
 AEAD
    RSA-AES-256-CCM8-AEAD         0xC0, 0xA1       RSA           RSA      AES-CCM8(256)
 AEAD
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/21/ftp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/22/ssh

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/80/http_proxy

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

tcp/80/http_proxy

```
An HTTP proxy is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/110/pop3

```
A POP3 server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/143/imap

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/443/www

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

tcp/443/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/465/smtp

```
A TLSv1.1 server answered on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/993/imap

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

tcp/993/imap

```
An IMAP server is running on this port through TLSv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/995/pop3

```
A POP3 server is running on this port through TLSv1.
```

tcp/995/pop3

```
A TLSv1 server answered on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/2078/www

```
A TLSv1.2 server answered on this port.
```

tcp/2078/www

```
A web server is running on this port through TLSv1.2.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/2080/www

```
A TLSv1.2 server answered on this port.
```

tcp/2080/www

```
A web server is running on this port through TLSv1.2.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/2083/www

```
A TLSv1.2 server answered on this port.
```

tcp/2083/www

```
A web server is running on this port through TLSv1.2.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/2087/www

```
A TLSv1.2 server answered on this port.
```

tcp/2087/www

```
A web server is running on this port through TLSv1.2.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/2096/www

```
A TLSv1.2 server answered on this port.
```

tcp/2096/www

```
A web server is running on this port through TLSv1.2.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

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: 2023/06/13

Plugin Output

tcp/465/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: 2023/06/13

Plugin Output

tcp/587/smtp

```
A SMTP server is running on this port
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2023/07/10

Plugin Output

tcp/443/www

```

  http/1.1
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF	CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/110/pop3

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF	CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/143/imap

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF	CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/465/smtp

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF	CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/993/imap

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF	CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/995/pop3

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/143/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/443/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/465/smtp

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/993/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/995/pop3

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2078/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2080/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2083/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2087/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2096/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2023/02/13

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/06/26

Plugin Output

udp/0

```
For your information, here is the traceroute from 172.16.23.12 to 162.215.219.65 :
172.16.23.12
162.215.219.65

Hop Count: 1
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/2083/www

```
The following string will be used :
TYPE="password"
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/2087/www

```
The following string will be used :
TYPE="password"
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/2096/www

```

The following string will be used :
TYPE="password"
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/2083/www

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/2087/www

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/2096/www

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/2078/www