



Basic Network Scan

Report generated by Tenable Nessus™

Sun, 17 Nov 2024 17:20:45 CST

TABLE OF CONTENTS

Vulnerabilities by Host

• 10.12.0.89.....	4
• 10.12.0.136.....	100
• 10.12.0.161.....	173
• 10.12.0.203.....	245

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

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

Remediations

• Suggested Remediations.....	406
-------------------------------	-----

Vulnerabilities by Host

10.12.0.89



Scan Information

Start time: Sun Nov 17 17:10:59 2024

End time: Sun Nov 17 17:17:21 2024

Host Information

IP: 10.12.0.89

MAC Address: 00:50:56:A1:A8:BE

OS: Linux Kernel 2.6

Vulnerabilities

10704 - Apache Multiviews Arbitrary Directory Listing

Synopsis

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

Description

The Apache web server running on the remote host is affected by an information disclosure vulnerability. An unauthenticated, remote attacker can exploit this, by sending a crafted request, to display a listing of a remote directory, even if a valid index file exists in the directory.

For Apache web server later than 1.3.22, review listing directory configuration to avoid disclosing sensitive information

See Also

<http://www.nessus.org/u?f39e976b>

<http://www.nessus.org/u?a96611bc>

<http://www.nessus.org/u?c1c382bc>

Solution

Upgrade to Apache version 1.3.22 or later. Alternatively, as a workaround, disable Multiviews.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.9652

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	3009
CVE	CVE-2001-0731
XREF	OWASP:OWASP-CM-004
XREF	EDB-ID:21002

Plugin Information

Published: 2016/02/16, Modified: 2020/10/21

Plugin Output

tcp/80/www

Nessus was able to exploit the issue using the following request :

http://10.12.0.89/?M=A

This produced the following truncated output (limited to 10 lines) :

----- snip -----

```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of </title>
</head>
<body>
<h1>Index of </h1>
<table>
<tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr>
[...]
```

----- snip -----

187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

Synopsis

The remote SSH server is vulnerable to a mitm prefix truncation attack.

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

See Also

<https://terrapin-attack.com/>

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.1

EPSS Score

0.9629

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

```
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha1-etm@openssh.com
Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha1-etm@openssh.com
```


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=Europa
| -Issuer  : CN=Europa
```

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=Europa
| -Issuer   : CN=Europa
```

57582 - SSL Self-Signed Certificate

Synopsis

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

Description

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/143/imap

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

```
| -Subject : CN=Europa
```

57582 - SSL Self-Signed Certificate

Synopsis

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

Description

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/993/imap

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

```
| -Subject : CN=Europa
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/143/imap

TLsv1 is enabled and the server supports at least one cipher.

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/993/imap

TLsv1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

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: 2024/05/14

Plugin Output

tcp/143/imap

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

157288 - TLS Version 1.1 Deprecated Protocol

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: 2024/05/14

Plugin Output

tcp/993/imap

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

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

Low

VPR Score

4.2

EPSS Score

0.8808

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

The difference between the local and remote clocks is -9 seconds.

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/www

```
URL      : http://10.12.0.89/
Version  : 2.4.99
Source   : Server: Apache/2.4.38 (Debian)
backported : 1
os       : ConvertedDebian
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

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: 2024/11/12

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:2.4.38 -> Apache Software Foundation Apache HTTP Server
```

```
cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
```

```
cpe:/a:openbsd:openssh:7.9 -> OpenBSD OpenSSH
```

```
cpe:/a:openbsd:openssh:7.9p1 -> OpenBSD OpenSSH
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
00:50:56:A1:A8:BE : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 00:50:56:A1:A8:BE
```

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/80/www

```
The remote web server type is :  
Apache/2.4.38 (Debian)
```

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 is 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: 2024/02/26

Plugin Output

tcp/80/www

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : yes

Options allowed : (Not implemented)

Headers :

Date: Sun, 17 Nov 2024 23:13:56 GMT

Server: Apache/2.4.38 (Debian)

Vary: Accept-Encoding

Content-Length: 742

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

<html>

<head>

<title>Index of </title>

</head>

<body>

<h1>Index of </h1>

```

<table>
  <tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
  <tr><th colspan="5"><hr></th></tr>
  <tr><td valign="top"></td><td><a href="html/">html</a></td><td align="right">2020-11-01 17:10 </td><td align="right"> - </td><td>&nbsp;</td></tr>
  <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.38 (Debian) Server at 10.12.0.89 Port 80</address>
</body></html>

```

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 LITERAL+ STARTTLS AUTH=PLAIN
AUTH=LOGIN] Dovecot (Debian) 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 LITERAL+ AUTH=PLAIN AUTH=LOGIN]
Dovecot (Debian) 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: Europa

Issuer Name:

Common Name: Europa

Serial Number: 04 42 FF EB D3 6A 46 97 CC E2 7E AE D6 7F AD 5C AF A2 3A 8D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 31 17:45:57 2020 GMT
Not Valid After: Oct 29 17:45:57 2030 GMT
```

Public Key Info:

Algorithm: RSA Encryption

Key Length: 2048 bits

Public Key: 00 A4 4B C8 08 9D 10 30 93 49 F5 3E 2E 43 FD B5 C3 06 71 16
26 57 BE F6 5C E4 8A 4C A8 39 14 29 9E 99 EF C6 21 80 76 F2
B7 0E 6B C9 A1 76 08 7D CA 61 AB 3A 41 87 15 D9 08 32 9D E9
D9 2B 69 0E 26 0D C0 5C 7F A2 4D C1 17 A5 2C 7A CA 0F 2D F7
3B 97 70 2E DE 8D 8F 33 08 C0 44 3A 72 BC C0 F5 26 9C 64 A3
0D 37 82 84 E3 7E 75 64 7E C8 70 93 59 3D 23 F7 B4 D8 9A D8
D0 FF 6C 35 7C E9 05 B8 D7 FF 3C 6F 29 75 9C A0 66 D8 71 18
E0 A3 B7 A6 3D 9B 92 3A 84 BD 85 3C AF C2 A4 0D BB 9D C7 94
0D 0B B5 06 21 D3 ED 4F 31 FD 34 35 92 87 98 95 FD 85 F7 FE
33 ED E3 6D 59 D5 E4 D5 27 11 FA 50 98 F7 FB F0 2E 02 98 DF
05 1A 1E 35 2B 69 A4 EA 69 43 84 AC 38 C3 47 80 F0 9F 85 1F
23 23 C5 7D 1F 59 7A 3B 75 90 20 56 21 4E 8B 50 F5 BB 7D 91
86 A6 8E 5C C6 44 FE 05 E2 6E F5 5D 49 A9 0B 62 97

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 47 64 04 FF 5B 10 4D CD 3F 30 DA 64 59 AB F2 D4 5B 7C 67
B2 CD 60 8D CE 59 98 F4 81 E2 9D 80 C2 B7 0B DC D9 08 94 70
F1 D7 D2 63 0E E3 AC DF 5C DE 4E 50 73 8E 68 64 E9 A2 D3 6E
C4 32 5A 6F 38 CC 64 9D AF E9 40 89 5A 56 69 91 1C 44 F1 86
CD 2B 26 8D EE BF 68 67 74 BB 22 B6 3A 90 B5 F0 03 81 79 22
5C 27 B7 9C 1F B3 8C CF 18 2C A3 F5 F5 1C DE D2 A9 B3 C1 7C
E2 2D 59 7E 35 2F 69 A3 75 98 35 D6 59 EC 59 DB C3 F1 92 C5 [...]

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: 2024/05/20

Plugin Output

tcp/22/ssh

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

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: 2024/05/20

Plugin Output

tcp/25/smtp

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

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: 2024/05/20

Plugin Output

tcp/80/www

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

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: 2024/05/20

Plugin Output

tcp/143/imap

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

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: 2024/05/20

Plugin Output

tcp/993/imap

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

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: 2024/05/20

Plugin Output

tcp/3306

```
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: 2024/10/04

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202411171908
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 10.12.0.25
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 130.502 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
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 : 2024/11/17 17:11 CST
Scan duration : 378 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: 2024/10/14

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 that these signatures would help us improve OS fingerprinting, please submit them by visiting <https://www.tenable.com/research/submitsignatures>.

```
SSH:!:SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
```

```
SinFP:
```

```
P1:B10113:F0x12:W64240:00204ffff:M1460:
```

```
P2:B10113:F0x12:W65160:00204ffff0402080affffff4445414401030306:M1460:
```

```
P3:B00000:F0x00:W0:00:M0
```

```
P4:191003_7_p=143
```

```
HTTP:!:Server: Apache/2.4.38 (Debian)
```

```
SMTP:!:220-Exim 4.84 FLAG: CSEC-0007-SMTP
```

```
220 HINT: Find a way to login to the webmail portal.
```

```
SSLcert:!:i/CN:Europas/CN:Europa
```

```
12a5a947326466321d086b143fede65cf2e016a3
```

```
i/CN:Europas/CN:Europa
```

```
12a5a947326466321d086b143fede65cf2e016a3
```

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.
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

<https://www.openssh.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2024/11/12

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 7.9p1
Banner  : SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

<https://www.openssl.org/>

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

<https://www.openssl.org/>

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/993/imap

Synopsis

The remote host is missing several patches.

Description

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

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/11/12

Plugin Output

tcp/0

```
. You need to take the following action :
```

```
[ SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) (187315) ]
```

```
+ Action to take : Contact the vendor for an update with the strict key exchange countermeasures or  
  disable the affected algorithms.
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

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

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

Solution

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

Risk Factor

None

References

XREF IAVT:0001-T-0932

Plugin Information

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

Plugin Output

tcp/25/smtp

```
Remote SMTP server banner :
```

```
220-Exim 4.84 FLAG: CSEC-0007-SMTP
220 HINT: Find a way to login to the webmail portal.
```

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-sha256
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 :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
```



```
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

The server supports the following options for `encryption_algorithms_server_to_client` :

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
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_client` :

```
none
zlib@openssh.com
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

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: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
SSH supported authentication : publickey
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 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/993/imap

```
This port supports TLSv1.3/TLSv1.0/TLSv1.1/TLSv1.2.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

```
Subject Name:

Common Name: Europa

Issuer Name:

Common Name: Europa

Serial Number: 04 42 FF EB D3 6A 46 97 CC E2 7E AE D6 7F AD 5C AF A2 3A 8D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 31 17:45:57 2020 GMT
Not Valid After: Oct 29 17:45:57 2030 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 4B C8 08 9D 10 30 93 49 F5 3E 2E 43 FD B5 C3 06 71 16
             26 57 BE F6 5C E4 8A 4C A8 39 14 29 9E 99 EF C6 21 80 76 F2
             B7 0E 6B C9 A1 76 08 7D CA 61 AB 3A 41 87 15 D9 08 32 9D E9
             D9 2B 69 0E 26 0D C0 5C 7F A2 4D C1 17 A5 2C 7A CA 0F 2D F7
             3B 97 70 2E DE 8D 8F 33 08 C0 44 3A 72 BC C0 F5 26 9C 64 A3
             0D 37 82 84 E3 7E 75 64 7E C8 70 93 59 3D 23 F7 B4 D8 9A D8
             D0 FF 6C 35 7C E9 05 B8 D7 FF 3C 6F 29 75 9C A0 66 D8 71 18
             E0 A3 B7 A6 3D 9B 92 3A 84 BD 85 3C AF C2 A4 0D BB 9D C7 94
             0D 0B B5 06 21 D3 ED 4F 31 FD 34 35 92 87 98 95 FD 85 F7 FE
             33 ED E3 6D 59 D5 E4 D5 27 11 FA 50 98 F7 FB F0 2E 02 98 DF
             05 1A 1E 35 2B 69 A4 EA 69 43 84 AC 38 C3 47 80 F0 9F 85 1F
```

```
23 23 C5 7D 1F 59 7A 3B 75 90 20 56 21 4E 8B 50 F5 BB 7D 91
86 A6 8E 5C C6 44 FE 05 E2 6E F5 5D 49 A9 0B 62 97
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 47 64 04 FF 5B 10 4D CD 3F 30 DA 64 59 AB F2 D4 5B 7C 67
           B2 CD 60 8D CE 59 98 F4 81 E2 9D 80 C2 B7 0B DC D9 08 94 70
           F1 D7 D2 63 0E E3 AC DF 5C DE 4E 50 73 8E 68 64 E9 A2 D3 6E
           C4 32 5A 6F 38 CC 64 9D AF E9 40 89 5A 56 69 91 1C 44 F1 86
           CD 2B 26 8D EE BF 68 67 74 BB 22 B6 3A 90 B5 F0 03 81 79 22
           5C 27 B7 9C 1F B3 8C CF 18 2C A3 F5 F5 1C DE D2 A9 B3 C1 7C
           E2 2D 59 7E 35 2F 69 A3 75 98 35 D6 59 EC 59 DB C3 F1 92 C5
           A8 3D A5 11 93 9E 6B 6E AD 7F 04 83 F3 5D 2C 9C 98 CA 4A 28
           78 F7 31 24 3E FC DF 15 99 AD AD B4 BE 69 24 04 99 AE FF 66
           41 2A E4 A9 D1 78 2F B8 [...]
```


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: Europa

Issuer Name:

Common Name: Europa

Serial Number: 04 42 FF EB D3 6A 46 97 CC E2 7E AE D6 7F AD 5C AF A2 3A 8D

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 31 17:45:57 2020 GMT
Not Valid After: Oct 29 17:45:57 2030 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 4B C8 08 9D 10 30 93 49 F5 3E 2E 43 FD B5 C3 06 71 16
             26 57 BE F6 5C E4 8A 4C A8 39 14 29 9E 99 EF C6 21 80 76 F2
             B7 0E 6B C9 A1 76 08 7D CA 61 AB 3A 41 87 15 D9 08 32 9D E9
             D9 2B 69 0E 26 0D C0 5C 7F A2 4D C1 17 A5 2C 7A CA 0F 2D F7
             3B 97 70 2E DE 8D 8F 33 08 C0 44 3A 72 BC C0 F5 26 9C 64 A3
             0D 37 82 84 E3 7E 75 64 7E C8 70 93 59 3D 23 F7 B4 D8 9A D8
             D0 FF 6C 35 7C E9 05 B8 D7 FF 3C 6F 29 75 9C A0 66 D8 71 18
             E0 A3 B7 A6 3D 9B 92 3A 84 BD 85 3C AF C2 A4 0D BB 9D C7 94
             0D 0B B5 06 21 D3 ED 4F 31 FD 34 35 92 87 98 95 FD 85 F7 FE
             33 ED E3 6D 59 D5 E4 D5 27 11 FA 50 98 F7 FB F0 2E 02 98 DF
             05 1A 1E 35 2B 69 A4 EA 69 43 84 AC 38 C3 47 80 F0 9F 85 1F
```

```
23 23 C5 7D 1F 59 7A 3B 75 90 20 56 21 4E 8B 50 F5 BB 7D 91
86 A6 8E 5C C6 44 FE 05 E2 6E F5 5D 49 A9 0B 62 97
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 47 64 04 FF 5B 10 4D CD 3F 30 DA 64 59 AB F2 D4 5B 7C 67
           B2 CD 60 8D CE 59 98 F4 81 E2 9D 80 C2 B7 0B DC D9 08 94 70
           F1 D7 D2 63 0E E3 AC DF 5C DE 4E 50 73 8E 68 64 E9 A2 D3 6E
           C4 32 5A 6F 38 CC 64 9D AF E9 40 89 5A 56 69 91 1C 44 F1 86
           CD 2B 26 8D EE BF 68 67 74 BB 22 B6 3A 90 B5 F0 03 81 79 22
           5C 27 B7 9C 1F B3 8C CF 18 2C A3 F5 F5 1C DE D2 A9 B3 C1 7C
           E2 2D 59 7E 35 2F 69 A3 75 98 35 D6 59 EC 59 DB C3 F1 92 C5
           A8 3D A5 11 93 9E 6B 6E AD 7F 04 83 F3 5D 2C 9C 98 CA 4A 28
           78 F7 31 24 3E FC DF 15 99 AD AD B4 BE 69 24 04 99 AE FF 66
           41 2A E4 A9 D1 78 2F B8 [...]
```

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-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)	
ECDHE-RSA-CAMELLIA-CBC-256 SHA384	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)	
DHE-RSA-AES128-SHA SHA1	0x00, 0x33	DH	RSA	AES-CBC(128)	
DHE-RSA-AES256-SHA SHA1	0x00, 0x39	DH	RSA	AES-CBC(256)	
DHE-RSA-CAMELLIA128-SHA SHA1	0x00, 0x45	DH	RSA	Camellia-CBC(128)	

DHE-RSA-CAMELLIA256-SHA SHA1	0x00, 0x88	DH	RSA	Camellia-CBC(256)
DHE-RSA-SEED-SHA SHA1	0x00, 0x9A	DH	RSA	SEED-CBC(128)
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x67	DH	RSA	AES-CBC(128)
DHE-RSA-AES256-SHA256 SHA256	0x00, 0x6B	DH	RSA	AES-CBC(256)
DHE-RSA-CAMELLIA128-SHA256 SHA256	0x00, 0xBE	DH	RSA	Camellia-CBC(128)
DHE-RSA-CAMELLIA256-SHA256 SHA256	0x00, 0xC4	DH	RSA	Camellia-CBC(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)

The fields above are :

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

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-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)	
ECDHE-RSA-CAMELLIA-CBC-256 SHA384	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)	
DHE-RSA-AES128-SHA SHA1	0x00, 0x33	DH	RSA	AES-CBC(128)	
DHE-RSA-AES256-SHA SHA1	0x00, 0x39	DH	RSA	AES-CBC(256)	
DHE-RSA-CAMELLIA128-SHA SHA1	0x00, 0x45	DH	RSA	Camellia-CBC(128)	

DHE-RSA-CAMELLIA256-SHA SHA1	0x00, 0x88	DH	RSA	Camellia-CBC(256)
DHE-RSA-SEED-SHA SHA1	0x00, 0x9A	DH	RSA	SEED-CBC(128)
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x67	DH	RSA	AES-CBC(128)
DHE-RSA-AES256-SHA256 SHA256	0x00, 0x6B	DH	RSA	AES-CBC(256)
DHE-RSA-CAMELLIA128-SHA256 SHA256	0x00, 0xBE	DH	RSA	Camellia-CBC(128)
DHE-RSA-CAMELLIA256-SHA256 SHA256	0x00, 0xC4	DH	RSA	Camellia-CBC(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)

The fields above are :

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

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?e17ffcd>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

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
-----	-----	---	---	-----	---
DHE-RSA-AES-128-CCM-AEAD	0xC0, 0x9E	DH	RSA	AES-CCM(128)	
AEAD					

DHE-RSA-AES-128-CCM8-AEAD AEAD	0xC0, 0xA2	DH	RSA	AES-CCM8(128)
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)
DHE-RSA-AES-256-CCM-AEAD AEAD	0xC0, 0x9F	DH	RSA	AES-CCM(256)
DHE-RSA-AES-256-CCM8-AEAD AEAD	0xC0, 0xA3	DH	RSA	AES-CCM8(256)
DHE-RSA-AES256-SHA384 SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)
DHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xAA	DH	RSA	ChaCha20-Poly1305(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)
ECDHE-RSA-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)
ECDHE-RSA-CAMELLIA-CBC-256	0xC0, 0x77	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?e17ffcd>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

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
-----	-----	---	---	-----	---
DHE-RSA-AES-128-CCM-AEAD	0xC0, 0x9E	DH	RSA	AES-CCM(128)	
AEAD					

DHE-RSA-AES-128-CCM8-AEAD AEAD	0xC0, 0xA2	DH	RSA	AES-CCM8(128)
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)
DHE-RSA-AES-256-CCM-AEAD AEAD	0xC0, 0x9F	DH	RSA	AES-CCM(256)
DHE-RSA-AES-256-CCM8-AEAD AEAD	0xC0, 0xA3	DH	RSA	AES-CCM8(256)
DHE-RSA-AES256-SHA384 SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)
DHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xAA	DH	RSA	ChaCha20-Poly1305(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)
ECDHE-RSA-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)
ECDHE-RSA-CAMELLIA-CBC-256	0xC0, 0x77	ECDH	RSA	[...]

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
-----	-----	---	----	-----	---
DHE-RSA-AES-128-CCM-AEAD	0xC0, 0x9E	DH	RSA	AES-CCM(128)	
AEAD					
DHE-RSA-AES-128-CCM8-AEAD	0xC0, 0xA2	DH	RSA	AES-CCM8(128)	
AEAD					
DHE-RSA-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
DHE-RSA-AES-256-CCM-AEAD	0xC0, 0x9F	DH	RSA	AES-CCM(256)	
AEAD					
DHE-RSA-AES-256-CCM8-AEAD	0xC0, 0xA3	DH	RSA	AES-CCM8(256)	
AEAD					

DHE-RSA-AES256-SHA384 SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)
DHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xAA	DH	RSA	ChaCha20-Poly1305(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)
ECDHE-RSA-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)
ECDHE-RSA-CAMELLIA-CBC-256 SHA384	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)
ECDHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)
DHE-RSA-AES128-SHA SHA1	0x00, 0x33	DH	RSA	AES-CBC(128)
DHE-RSA-AES256-SHA SHA1	0x00, 0x39	DH	RSA	AES-CBC(256)
DHE-RSA-CAMELLIA128-SHA SHA1	0x00, 0x45	DH	RSA	Camellia-CBC(128)
DHE-RSA-CAMELLIA256-SHA SHA1	0x00, 0x88	DH	RSA	Camellia-CBC(256)
DHE-RSA-SEED-SHA	0x00, 0x9A	DH	RSA	SEED-CBC(128 [...])

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/993/imap

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

High Strength Ciphers (>= 112-bit key)

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

DHE-RSA-AES256-SHA384 SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)
DHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xAA	DH	RSA	ChaCha20-Poly1305(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)
ECDHE-RSA-CAMELLIA-CBC-128 SHA256	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)
ECDHE-RSA-CAMELLIA-CBC-256 SHA384	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)
ECDHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)
DHE-RSA-AES128-SHA SHA1	0x00, 0x33	DH	RSA	AES-CBC(128)
DHE-RSA-AES256-SHA SHA1	0x00, 0x39	DH	RSA	AES-CBC(256)
DHE-RSA-CAMELLIA128-SHA SHA1	0x00, 0x45	DH	RSA	Camellia-CBC(128)
DHE-RSA-CAMELLIA256-SHA SHA1	0x00, 0x88	DH	RSA	Camellia-CBC(256)
DHE-RSA-SEED-SHA	0x00, 0x9A	DH	RSA	SEED-CBC(128 [...])

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

- 0x13,0x01 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

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 recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

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
-----	-----	----	----	-----	----
DHE-RSA-AES-128-CCM-AEAD	0xC0, 0x9E	DH	RSA	AES-CCM(128)	
AEAD					
DHE-RSA-AES-128-CCM8-AEAD	0xC0, 0xA2	DH	RSA	AES-CCM8(128)	
AEAD					
DHE-RSA-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
DHE-RSA-AES-256-CCM-AEAD	0xC0, 0x9F	DH	RSA	AES-CCM(256)	
AEAD					
DHE-RSA-AES-256-CCM8-AEAD	0xC0, 0xA3	DH	RSA	AES-CCM8(256)	
AEAD					
DHE-RSA-AES256-SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)	
SHA384					
ECDHE-RSA-CAMELLIA-CBC-128	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)	
SHA256					
ECDHE-RSA-CAMELLIA-CBC-256	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)	
SHA384					
DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC(128)	
SHA1					
DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC(256)	
SHA1					
DHE-RSA-CAMELLIA128-SHA	0x00, 0x45	DH	RSA	Camellia-CBC(128)	
SHA1					
DHE-RSA-CAMELLIA256-SHA	0x00, 0x88	DH	RSA	Camellia-CBC(256)	
SHA1					
DHE-RSA-SEED-SHA	0x00, 0x9A	DH	RSA	SEED-CBC(128)	
SHA1					
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
SHA1					
ECDHE-RSA-AES256-SHA	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	
SHA1					
DHE-RSA-AES128-SHA256	0x00, 0x67	DH	RSA	AES-CBC(128)	
SHA256					
DHE-RSA-AES256-SHA256	0x00, 0x6B	DH	[...]		

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

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 recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

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
-----	-----	----	----	-----	----
DHE-RSA-AES-128-CCM-AEAD	0xC0, 0x9E	DH	RSA	AES-CCM(128)	
AEAD					
DHE-RSA-AES-128-CCM8-AEAD	0xC0, 0xA2	DH	RSA	AES-CCM8(128)	
AEAD					
DHE-RSA-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
DHE-RSA-AES-256-CCM-AEAD	0xC0, 0x9F	DH	RSA	AES-CCM(256)	
AEAD					
DHE-RSA-AES-256-CCM8-AEAD	0xC0, 0xA3	DH	RSA	AES-CCM8(256)	
AEAD					
DHE-RSA-AES256-SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)	
SHA384					
ECDHE-RSA-CAMELLIA-CBC-128	0xC0, 0x76	ECDH	RSA	Camellia-CBC(128)	
SHA256					
ECDHE-RSA-CAMELLIA-CBC-256	0xC0, 0x77	ECDH	RSA	Camellia-CBC(256)	
SHA384					
DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC(128)	
SHA1					
DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC(256)	
SHA1					
DHE-RSA-CAMELLIA128-SHA	0x00, 0x45	DH	RSA	Camellia-CBC(128)	
SHA1					
DHE-RSA-CAMELLIA256-SHA	0x00, 0x88	DH	RSA	Camellia-CBC(256)	
SHA1					
DHE-RSA-SEED-SHA	0x00, 0x9A	DH	RSA	SEED-CBC(128)	
SHA1					
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
SHA1					
ECDHE-RSA-AES256-SHA	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	
SHA1					
DHE-RSA-AES128-SHA256	0x00, 0x67	DH	RSA	AES-CBC(128)	
SHA256					
DHE-RSA-AES256-SHA256	0x00, 0x6B	DH	[...]		

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: 2024/03/26

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: 2024/03/26

Plugin Output

tcp/25/smtp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

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: 2024/03/26

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.
```

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: 2023/10/17

Plugin Output

tcp/0

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/143/imap

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

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/993/imap

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/143/imap

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/993/imap

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

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

<https://tools.ietf.org/html/rfc8446>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/143/imap

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

<https://tools.ietf.org/html/rfc8446>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/993/imap

```
TLSv1.3 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: 2024/04/19

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: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.12.0.25 to 10.12.0.89 :
10.12.0.25
10.12.0.89

Hop Count: 1
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

```
Nessus was able to extract the following information :
```

```
- mDNS hostname      : Europa.local.
```

10.12.0.136



Scan Information

Start time: Sun Nov 17 17:04:07 2024

End time: Sun Nov 17 17:15:03 2024

Host Information

IP: 10.12.0.136

MAC Address: 00:50:56:A1:95:57

OS: Microsoft Windows 11

Vulnerabilities

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

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

<https://sweet32.info>

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.1

EPSS Score

0.0053

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

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

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	
SHA1					

The fields above are :

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

10043 - Chargen UDP Service Remote DoS

Synopsis

The remote host is running a 'chargen' service.

Description

When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection.

The purpose of this service was to mostly test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third-party host using this host as a relay.

An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

See Also

<http://www.nessus.org/u?f0dbdf05>

Solution

- Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen

Then launch cmd.exe and type :

```
net stop simptcp net start simptcp
```

To restart the service.

Risk Factor

Medium

VPR Score

4.4

EPSS Score

0.8755

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0103

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/11/29, Modified: 2020/06/12

Plugin Output

udp/19

10061 - Echo Service Detection

Synopsis

An echo service is running on the remote host.

Description

The remote host is running the 'echo' service. This service echoes any data which is sent to it.

This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.

Solution

Below are some examples of how to disable the echo service on some common platforms, however many services can exhibit this behavior and the list below is not exhaustive.

Consult vendor documentation for the service exhibiting the echo behavior for more information.

- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process.
- Under Ubuntu systems, comment out the 'echo' line in /etc/systemd/system.conf and retart the systemd service.

- Under Windows systems, set the following registry key to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho

Then launch cmd.exe and type :

```
net stop simptcp net start simptcp
```

To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.4

EPSS Score

0.8755

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0103

CVE CVE-1999-0635

Plugin Information

Published: 1999/06/22, Modified: 2020/06/12

Plugin Output

tcp/7/echo

10061 - Echo Service Detection

Synopsis

An echo service is running on the remote host.

Description

The remote host is running the 'echo' service. This service echoes any data which is sent to it.

This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.

Solution

Below are some examples of how to disable the echo service on some common platforms, however many services can exhibit this behavior and the list below is not exhaustive.

Consult vendor documentation for the service exhibiting the echo behavior for more information.

- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process.
- Under Ubuntu systems, comment out the 'echo' line in /etc/systemd/system.conf and retart the systemd service.

- Under Windows systems, set the following registry key to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho

Then launch cmd.exe and type :

```
net stop simptcp net start simptcp
```

To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.4

EPSS Score

0.8755

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0103

CVE CVE-1999-0635

Plugin Information

Published: 1999/06/22, Modified: 2020/06/12

Plugin Output

udp/7

10198 - Quote of the Day (QOTD) Service Detection

Synopsis

The quote service (qotd) is running on this host.

Description

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.

Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17.

When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).

An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.4

EPSS Score

0.8755

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0103

Plugin Information

Published: 1999/11/30, Modified: 2019/10/04

Plugin Output

tcp/17/qotd

10198 - Quote of the Day (QOTD) Service Detection

Synopsis

The quote service (qotd) is running on this host.

Description

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.

Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17.

When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).

An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.4

EPSS Score

0.8755

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0103

Plugin Information

Published: 1999/11/30, Modified: 2019/10/04

Plugin Output

udp/17/qotd

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/3389/msrdp

```
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=Enceladus
| -Issuer   : CN=Enceladus
```

57582 - SSL Self-Signed Certificate

Synopsis

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

Description

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/3389/msrdp

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

```
| -Subject : CN=Enceladus
```

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/3389/msrdp

TLsv1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

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: 2024/05/14

Plugin Output

tcp/3389/msrdp

TLsv1.1 is enabled and the server supports at least one cipher.

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: 2024/11/12

Plugin Output

tcp/0

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

```
cpe:/o:microsoft:windows_11 -> Microsoft Windows 11
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/135/epmap

The following DCERPC services are available locally :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : SidKey Local End Point

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service


```
Named pipe : lsasspirpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : lsapolicylookup

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : lsacap

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/445

The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 29770a8f-829b-4158-90a2-78cd488501f7, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\SessEnvPublicRpc
Netbios name : \\ENCELADUS

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\ENCELADUS

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\ENCELADUS

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service

Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\ENCELADUS

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\ENCELADUS

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\ENCELADUS

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\ENCELADUS

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\ENCELADUS

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, [...]

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49664/dce-rpc

The following DCERPC services are available on TCP port 49664 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49664
IP : 10.12.0.136

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49664
IP : 10.12.0.136

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
TCP Port : 49664
IP : 10.12.0.136

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191felb, version 1.0

Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49664
IP : 10.12.0.136

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49665/dce-rpc

The following DCERPC services are available on TCP port 49665 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49665
IP : 10.12.0.136

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49666/dce-rpc

The following DCERPC services are available on TCP port 49666 :

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Remote RPC service
TCP Port : 49666
IP : 10.12.0.136
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49667/dce-rpc

The following DCERPC services are available on TCP port 49667 :

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 29770a8f-829b-4158-90a2-78cd488501f7, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49667
IP : 10.12.0.136
```


10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49668/dce-rpc

The following DCERPC services are available on TCP port 49668 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 10.12.0.136

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 10.12.0.136

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49669/dce-rpc

The following DCERPC services are available on TCP port 49669 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49669
IP : 10.12.0.136

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49669
IP : 10.12.0.136

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49669
IP : 10.12.0.136

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Remote RPC service

TCP Port : 49669
IP : 10.12.0.136

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49669
IP : 10.12.0.136

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49670/dce-rpc

The following DCERPC services are available on TCP port 49670 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49670
IP : 10.12.0.136

10052 - Daytime Service Detection

Synopsis

A daytime service is running on the remote host.

Description

The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host.

In addition, if the daytime service is running on a UDP port, an attacker may link it to the echo port of a third-party host using spoofing, thus creating a possible denial of service condition between this host and the third party.

Solution

- On Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process.
- On Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime
Next, launch cmd.exe and type :
net stop simptcp net start simptcp
This will restart the service.

Risk Factor

None

Plugin Information

Published: 1999/06/22, Modified: 2014/05/09

Plugin Output

tcp/13/daytime

10052 - Daytime Service Detection

Synopsis

A daytime service is running on the remote host.

Description

The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host.

In addition, if the daytime service is running on a UDP port, an attacker may link it to the echo port of a third-party host using spoofing, thus creating a possible denial of service condition between this host and the third party.

Solution

- On Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process.
- On Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime
Next, launch cmd.exe and type :
net stop simptcp net start simptcp
This will restart the service.

Risk Factor

None

Plugin Information

Published: 1999/06/22, Modified: 2014/05/09

Plugin Output

udp/13/daytime

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 : 70
```

11367 - Discard Service Detection

Synopsis

A discard service is running on the remote host.

Description

The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives.

This service is unused these days, so it is advised that you disable it.

Solution

- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry key to 0 :

HKLM\System\CurrentControlSet\Services\SimptCP\Parameters\EnableTcpDiscard Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

None

Plugin Information

Published: 2003/03/12, Modified: 2011/03/11

Plugin Output

tcp/9/discard

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

The following card manufacturers were identified :

00:50:56:A1:95:57 : VMware, Inc.

86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 00:50:56:A1:95:57
```

53513 - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

<http://www.nessus.org/u?51eae65d>

<http://technet.microsoft.com/en-us/library/bb878128.aspx>

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2011/04/21, Modified: 2023/10/17

Plugin Output

udp/5355/llmnr

```
According to LLMNR, the name of the remote host is 'Enceladus'.
```

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: 2024/05/20

Plugin Output

tcp/7/echo

```
Port 7/tcp was found to be open
```

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: 2024/05/20

Plugin Output

tcp/9/discard

```
Port 9/tcp was found to be open
```

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: 2024/05/20

Plugin Output

tcp/13/daytime

```
Port 13/tcp was found to be open
```

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: 2024/05/20

Plugin Output

tcp/17/qotd

```
Port 17/tcp was found to be open
```

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: 2024/05/20

Plugin Output

tcp/19/chargen

```
Port 19/tcp was found to be open
```


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: 2024/05/20

Plugin Output

tcp/135/epmap

```
Port 135/tcp was found to be open
```

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: 2024/05/20

Plugin Output

tcp/3389/msrdp

```
Port 3389/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: 2024/10/04

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202411171908
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 10.12.0.25
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 144.116 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/11/17 17:04 CST
Scan duration : 649 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: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows 11
Confidence level : 70
Method : SinFP
```

```
The remote host is running Microsoft Windows 11
```

21745 - OS Security Patch Assessment Failed

Synopsis

Errors prevented OS Security Patch Assessment.

Description

OS Security Patch Assessment is not available for this host because either the credentials supplied in the scan policy did not allow Nessus to log into it or some other problem occurred.

Solution

Fix the problem(s) so that OS Security Patch Assessment is possible.

Risk Factor

None

References

XREF IAVB:0001-B-0501

Plugin Information

Published: 2006/06/23, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following service errors were logged :  
- It was not possible to log into the remote host via smb (unable to create a socket).
```

10940 - Remote Desktop Protocol Service Detection

Synopsis

The remote host has an remote desktop protocol service enabled.

Description

The Remote Desktop Protocol allows a user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable the service if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2023/08/21

Plugin Output

tcp/3389/msrdp

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/3389/msrdp

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


10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: Enceladus

Issuer Name:

Common Name: Enceladus

Serial Number: 6C D6 8F 91 5A 0F 21 8F 44 1F 76 B2 A3 13 37 F4

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 16 20:56:06 2024 GMT
Not Valid After: May 18 20:56:06 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 9E D0 5A C7 43 5C 0A 6C B4 F8 F4 59 28 96 29 94 94 55 C8
             2E 2A 65 39 55 50 27 FF 66 BB 9A FB 62 F2 A9 E0 6F 48 E2 43
             23 3D 41 A2 50 F2 1B F8 C8 68 DF 9E E0 1C D2 86 A2 B1 3A 32
             91 F1 95 12 E8 22 6A 84 F2 BA 44 E5 E1 08 B2 AF 3B 43 75 21
             5F 0C 4B FB 51 B0 20 DC 1C CA 5E 8B A7 4E 1A 67 6F F9 CB 51
             2D C7 4E CA D0 98 B1 31 9C EB CA 10 E8 A6 AC 4A 78 5A D6 A2
             66 38 64 8A 2E 46 D9 5C F9 ED 93 0A 7D 78 F7 53 50 56 67 95
             45 76 CC BF 31 7D 08 46 82 5B DE 53 75 C2 C5 0A BC F5 BE 8D
             00 55 13 37 FE 90 29 05 0F 92 FB BE C4 D4 A3 7B A9 B3 44 D4
             DC 31 DD C0 9C 1E A3 5B 66 5F D8 0A 60 0D CA 17 C1 96 11 D1
             E5 1F B3 DA A4 C5 2D CF 58 23 DD 83 91 78 85 81 E2 41 2F C7
```

```
CF 2A 34 69 9F 42 28 33 9D 2B 41 51 3B 5C D8 60 1E F9 47 F4
7E 1F 47 54 5F 11 BC F6 84 F5 04 A3 A6 6A 1B B5 05
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 69 0C 8E AC BA B4 D4 1B 71 04 98 FB BB 26 86 36 76 B8 D5
82 1E CB B3 0B 85 A2 EF 85 66 71 FB 7B 81 3F 09 C9 7D E9 2C
62 B3 A9 52 44 47 79 48 0F 43 CB CF 7E E2 72 99 74 EE A4 B6
E0 41 16 5F DF B5 C7 A0 DD FD 92 61 46 3A E6 4D F7 37 E9 CA
BC 89 50 55 9F 0A FF E1 85 DC DC 2C 84 D6 79 15 B8 B9 BB B4
1C B4 5C 1D 81 37 D6 28 B9 08 45 C6 FB 52 44 21 1B 23 1D 9F
7F EC 61 C6 0D D6 26 17 94 F6 5E B3 0F DF 9C 4C 38 70 DD 9C
A3 E6 AC FD 8B 8A E3 FD 75 3A F2 7A 35 13 95 84 DB E5 20 BB
91 64 13 CD 32 16 52 30 3E F0 38 A3 98 EF AC 23 92 AE 35 6B
4D 59 65 F9 BE 72 90 6E 16 30 [...]
```

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/3389/msrdp

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

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

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	

SHA1

High Strength Ciphers (>= 112-bit key)

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

SHA1

AES128-SHA SHA1	0x00, 0x2F	RSA	RSA	AES-CBC(128)
AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)
RSA-AES128-SHA256 SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)
RSA-AES256-SHA256 SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)

The fields above are :

```

{Tenable ciphertype}
{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?e17ffcd>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/3389/msrdp

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

```
SSL Version : TLSv12
```

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

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	

```
SHA1
```

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

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

RSA-AES128-SHA256 SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)
RSA-AES256-SHA384 SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)
AES128-SHA SHA1	0x00, 0x2F	RSA	RSA	AES-CBC(128)
AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)
RSA-AES128-SHA256	0x00, 0x3C	RSA	RS [...]	

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/3389/msrdp

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-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
SHA1					

ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)

The fields above are :

```
{Tenable ciphertype}
{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

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 recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/3389/msrdp

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

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
DES-CBC3-SHA SHA1	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
DHE-RSA-AES256-SHA384 SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)	
RSA-AES128-SHA256 SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)	
RSA-AES256-SHA384 SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	
AES128-SHA SHA1	0x00, 0x2F	RSA	RSA	AES-CBC(128)	
AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)	
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)	
RSA-AES128-SHA256 SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)	
RSA-AES256-SHA256 SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)	

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange} [...]
```

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: 2024/03/26

Plugin Output

tcp/7/echo

```
An echo 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: 2024/03/26

Plugin Output

tcp/19/chargen

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

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/11/26

Plugin Output

tcp/13/daytime

```
Daytime 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: 2023/10/17

Plugin Output

tcp/0

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/3389/msrdp

```
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/3389/msrdp

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


64814 - Terminal Services Use SSL/TLS

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/22, Modified: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: Enceladus

Issuer Name:

Common Name: Enceladus

Serial Number: 6C D6 8F 91 5A 0F 21 8F 44 1F 76 B2 A3 13 37 F4

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 16 20:56:06 2024 GMT
Not Valid After: May 18 20:56:06 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 9E D0 5A C7 43 5C 0A 6C B4 F8 F4 59 28 96 29 94 94 55 C8
             2E 2A 65 39 55 50 27 FF 66 BB 9A FB 62 F2 A9 E0 6F 48 E2 43
             23 3D 41 A2 50 F2 1B F8 C8 68 DF 9E E0 1C D2 86 A2 B1 3A 32
             91 F1 95 12 E8 22 6A 84 F2 BA 44 E5 E1 08 B2 AF 3B 43 75 21
             5F 0C 4B FB 51 B0 20 DC 1C CA 5E 8B A7 4E 1A 67 6F F9 CB 51
             2D C7 4E CA D0 98 B1 31 9C EB CA 10 E8 A6 AC 4A 78 5A D6 A2
             66 38 64 8A 2E 46 D9 5C F9 ED 93 0A 7D 78 F7 53 50 56 67 95
             45 76 CC BF 31 7D 08 46 82 5B DE 53 75 C2 C5 0A BC F5 BE 8D
             00 55 13 37 FE 90 29 05 0F 92 FB BE C4 D4 A3 7B A9 B3 44 D4
             DC 31 DD C0 9C 1E A3 5B 66 5F D8 0A 60 0D CA 17 C1 96 11 D1
             E5 1F B3 DA A4 C5 2D CF 58 23 DD 83 91 78 85 81 E2 41 2F C7
```

```
CF 2A 34 69 9F 42 28 33 9D 2B 41 51 3B 5C D8 60 1E F9 47 F4
7E 1F 47 54 5F 11 BC F6 84 F5 04 A3 A6 6A 1B B5 05
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 69 0C 8E AC BA B4 D4 1B 71 04 98 FB BB 26 86 36 76 B8 D5
82 1E CB B3 0B 85 A2 EF 85 66 71 FB 7B 81 3F 09 C9 7D E9 2C
62 B3 A9 52 44 47 79 48 0F 43 CB CF 7E E2 72 99 74 EE A4 B6
E0 41 16 5F DF B5 C7 A0 DD FD 92 61 46 3A E6 4D F7 37 E9 CA
BC 89 50 55 9F 0A FF E1 85 DC DC 2C 84 D6 79 15 B8 B9 BB B4
1C B4 5C 1D 81 37 D6 28 B9 08 45 C6 FB 52 44 21 1B 23 1D 9F
7F EC 61 C6 0D D6 26 17 94 F6 5E B3 0F DF 9C 4C 38 70 DD 9C
A3 E6 AC FD 8B 8A E3 FD 75 3A F2 7A 35 13 95 84 DB E5 20 BB
91 64 13 CD 32 16 52 30 3E F0 38 A3 98 EF AC 23 92 AE 35 6B
4D 59 65 F9 BE 72 90 6E 16 30 [...]
```

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: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.12.0.25 to 10.12.0.136 :  
10.12.0.25  
10.12.0.136  
  
Hop Count: 1
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

10.12.0.161



Scan Information

Start time: Sun Nov 17 17:04:07 2024

End time: Sun Nov 17 17:11:29 2024

Host Information

IP: 10.12.0.161

MAC Address: 00:50:56:A1:E6:2A 50:50:54:50:30:30 33:50:6F:45:30:30 EA:94:20:52:41:53
00:50:56:A1:F1:9D

OS: Microsoft Windows Vista, Microsoft Windows Server 2008

Vulnerabilities

125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

Synopsis

The remote host is affected by a remote code execution vulnerability.

Description

The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

See Also

<http://www.nessus.org/u?577af692>

<http://www.nessus.org/u?8e4e0b74>

Solution

Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.5

EPSS Score

0.9748

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

References

BID	108273
CVE	CVE-2019-0708
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CEA-ID:CEA-2020-0129
XREF	CEA-ID:CEA-2019-0326
XREF	CEA-ID:CEA-2019-0700

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2019/05/22, Modified: 2024/07/17

Plugin Output

tcp/3389/msrdp

58435 - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Synopsis

The remote Windows host could allow arbitrary code execution.

Description

An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.

This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.

Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host.

See Also

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-020>

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.

Risk Factor

High

VPR Score

9.6

EPSS Score

0.7644

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

BID	52353
BID	52354
CVE	CVE-2012-0002
CVE	CVE-2012-0152
MSKB	2621440
MSKB	2667402
XREF	EDB-ID:18606
XREF	MSFT:MS12-020
XREF	IAVA:2012-A-0039

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2012/03/22, Modified: 2024/07/17

Plugin Output

tcp/3389/msrdp

10547 - Microsoft Windows LAN Manager SNMP LanMan Services Disclosure

Synopsis

The list of LanMan services running on the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of LanMan services on the remote host by sending SNMP requests with the OID 1.3.6.1.4.1.77.1.2.3.1.1

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

High

CVSS v3.0 Base Score

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

VPR Score

3.4

EPSS Score

0.0035

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0499

Plugin Information

Published: 2000/11/10, Modified: 2024/03/22

Plugin Output

udp/161/snmp

Server
IP Helper
DNS Client
DHCP Client
Workstation
SNMP Service
Windows Time
Plug and Play
Print Spooler
Task Scheduler
Windows Update
Remote Registry
Secondary Logon
Windows Firewall
COM+ Event System
Terminal Services
Windows Event Log
IPsec Policy Agent
Software Licensing
Group Policy Client
Network List Service
User Profile Service
Base Filtering Engine
TCP/IP NetBIOS Helper
Application Experience
Cryptographic Services
Diagnostic System Host
Certificate Propagation
Shell Hardware Detection
Diagnostic Policy Service
Security Accounts Manager
Network Location Awareness
SL UI Notification Service
Remote Procedure Call (RPC)
DCOM Server Process Launcher
Interactive Services Detection
Network Store Interface Service
Terminal Services Configuration
Windows Error Reporting Service
Distributed Link Tracking Client
System Event Notification Service
Windows Management Instrumentation
Distributed Transaction Coordinator
IKE and AuthIP IPsec Keying Modules
Desktop Window Manager Session Manager
Background Intelligent Transfer Service
Windows Remote Management (WS-Management)
Terminal Services UserMode Port Redirector
KtmRm for Distributed Transaction Coordinator

41028 - SNMP Agent Default Community Name (public)

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port, or change the default community string.

Risk Factor

High

VPR Score

5.2

EPSS Score

0.4545

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	2112
CVE	CVE-1999-0517

Plugin Information

Published: 2002/11/25, Modified: 2022/06/01

Plugin Output

udp/161/snmp

```
The remote SNMP server replies to the following default community  
string :
```

```
public
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

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

Description

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

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

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

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

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

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

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

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

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

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.2

EPSS Score

0.0111

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	11849
BID	33065
CVE	CVE-2004-2761
CVE	CVE-2005-4900
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2023/12/15

Plugin Output

tcp/3389/msrpd

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

```
Subject          : CN=Deimos
Signature Algorithm : SHA-1 With RSA Encryption
Valid From       : Nov 16 20:56:42 2024 GMT
Valid To        : May 18 20:56:42 2025 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIC0DCCAbigAwIBAgIQo00/
KVHzEahFG9TApCfG9zANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZEZWl1b3MwHhcNMjQxMTE2MjA1NjQyWhcNMjUwNTE4MjA1NjQyWjARMQ8wDQYDVQ
PiNhbD
+TR/3cZkmhA5BfM/7xabpTi7ErryIn7txDjhkQXA0E1xPct9OlJwYSA5Iu7FtYNrYeaUO741KmFpkALrNZ9PYmoeztMQtL5RIIQ4vro4GnzS7dPOpu
I44VtNlmeJqzdtMCKCHrr7/EQlZqHf5q0XME31jf6/
k1USkVUD5HYpDRK9YkcD0eyqD2YzYR6tEUsE2XaIZY3AFvZdJIoyf0G4+W2aTo76WrrWjYweaNQXXxD9O1165j5mQ
+m45AgMBAAGjJDAiMBMGAlUdJQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQUFAAOCAQEAN7ZC5Tk4MFfb7F7Za4L1G/
XqNtr5AAOJICVZqN+Up1LVcgyNb1fUJ1OkBAPlwNMIMzrBVpkZRVJzoZFwDhzfUuYrb8xHJhEA3+yAILD5VPMnAlf3QPsn0I/
BczYDgy76uJtjPWluwp6H0TL5qUwhTZ1DZAGSoNhevRaQb9uuL3CZDyeh7thqrlofpv2p48h6hvtwNO5Ayy5GYbmSfFcCSr9jYE
+03au+t2L0jkpleeZUAbeXg3aFZsmNh2s0gSe
+BvLzxqWNjNmKvjDqE4iyTqBwOw2Efmk4TaaKMVAK1OzqoUhElGE2M0YUG7qTbLh5ZPipEW8Jr5MXPWhQWbxzg==
-----END CERTIFICATE-----
```

10546 - Microsoft Windows LAN Manager SNMP LanMan Users Disclosure

Synopsis

The list of LanMan users of the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of LanMan users on the remote host by sending SNMP requests with the OID 1.3.6.1.4.1.77.1.2.25.1.1

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

3.4

EPSS Score

0.0035

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0499

Plugin Information

Published: 2000/11/10, Modified: 2023/11/08

Plugin Output

udp/161/snmp

Guest
roots
martha
Administrator

18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a publicly known hard-coded RSA private key. Any attacker in a privileged network location can use the key for this attack.

See Also

<http://www.nessus.org/u?8033da0d>

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and
- On Microsoft Windows operating systems, select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

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)

VPR Score

2.5

EPSS Score

0.0127

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	13818
CVE	CVE-2005-1794

Plugin Information

Published: 2005/06/01, Modified: 2022/08/24

Plugin Output

tcp/3389/msrdp

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/3389/msrdp

```
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=Deimos
| -Issuer  : CN=Deimos
```

57582 - SSL Self-Signed Certificate

Synopsis

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

Description

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/3389/msrdp

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

```
| -Subject : CN=Deimos
```

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/3389/msrdp

TLsv1 is enabled and the server supports at least one cipher.

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis

The remote Terminal Services doesn't use Network Level Authentication only.

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11))

<http://www.nessus.org/u?e2628096>

Solution

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/03/23, Modified: 2024/07/17

Plugin Output

tcp/3389/msrdp

```
Nessus was able to negotiate non-NLA (Network Level Authentication) security.
```


57690 - Terminal Services Encryption Level is Medium or Low

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.

Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Solution

Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/25, Modified: 2024/07/17

Plugin Output

tcp/3389/msrdp

```
The terminal services encryption level is set to :  
  
2. Medium
```

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant

Synopsis

The remote host is not FIPS-140 compliant.

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Solution

Change RDP encryption level to :

4. FIPS Compliant

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2008/02/11, Modified: 2024/07/17

Plugin Output

tcp/3389/msrdp

```
The terminal services encryption level is set to :  
2. Medium (Client Compatible)
```

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: 2024/11/12

Plugin Output

tcp/0

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

```
cpe:/o:microsoft:windows_server_2008 -> Microsoft Windows Server 2008  
cpe:/o:microsoft:windows_vista -> Microsoft Windows Vista
```

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 : 75
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
00:50:56:A1:E6:2A : VMware, Inc.
```

```
00:50:56:A1:F1:9D : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 00:50:56:A1:E6:2A  
- 50:50:54:50:30:30  
- 33:50:6F:45:30:30  
- EA:94:20:52:41:53  
- 00:50:56:A1:F1:9D
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/0

```
Nessus SNMP scanner was able to retrieve the open port list
with the community name: p*****
It found 8 open TCP ports and 7 open UDP ports.
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/123

```
Port 123/udp was found to be open
```


Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/135

```
Port 135/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/137

```
Port 137/udp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/138

```
Port 138/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/139

```
Port 139/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
Port 161/udp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/500

```
Port 500/udp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/3389/msrdp

```
Port 3389/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/4500

```
Port 4500/udp was found to be open
```


Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/5355

```
Port 5355/udp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/49152

```
Port 49152/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/49153

```
Port 49153/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/49154

```
Port 49154/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/49155

```
Port 49155/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/49156

```
Port 49156/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: 2024/10/04

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202411171908
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 10.12.0.25
Port scanner(s) : snmp_scanner
Port range : default
Ping RTT : 149.177 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/11/17 17:04 CST
Scan duration : 435 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: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Vista
Microsoft Windows Server 2008
Confidence level : 75
Method : SNMP
```

```
The remote host is running one of these operating systems :
Microsoft Windows Vista
Microsoft Windows Server 2008
```

21745 - OS Security Patch Assessment Failed

Synopsis

Errors prevented OS Security Patch Assessment.

Description

OS Security Patch Assessment is not available for this host because either the credentials supplied in the scan policy did not allow Nessus to log into it or some other problem occurred.

Solution

Fix the problem(s) so that OS Security Patch Assessment is possible.

Risk Factor

None

References

XREF IAVB:0001-B-0501

Plugin Information

Published: 2006/06/23, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following service errors were logged :  
- It was not possible to log into the remote host via smb (unable to create a socket).
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

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

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/11/12

Plugin Output

tcp/0

```
. You need to take the following action :  
[ Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) (125313) ]  
+ Action to take : Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008  
R2.  
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

Synopsis

It is possible to take a screenshot of the remote login screen.

Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.

While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/22, Modified: 2024/07/17

Plugin Output

tcp/3389/msrdp

```
It was possible to gather the following screenshot of the remote login screen.
```

10940 - Remote Desktop Protocol Service Detection

Synopsis

The remote host has an remote desktop protocol service enabled.

Description

The Remote Desktop Protocol allows a user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable the service if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2023/08/21

Plugin Output

tcp/3389/msrdp

35296 - SNMP Protocol Version Detection

Synopsis

This plugin reports the protocol version negotiated with the remote SNMP agent.

Description

By sending an SNMP 'get-next-request', it is possible to determine the protocol version of the remote SNMP agent.

See Also

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

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2019/11/22

Plugin Output

udp/161/snmp

```
Nessus has negotiated SNMP communications at SNMPv2c.
```

34022 - SNMP Query Routing Information Disclosure

Synopsis

The list of IP routes on the remote host can be obtained via SNMP.

Description

It is possible to obtain the routing information on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.4.21

An attacker may use this information to gain more knowledge about the network topology.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2008/08/21, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
10.12.0.0/255.255.255.0
10.12.0.161/255.255.255.255
10.12.0.255/255.255.255.255
127.0.0.0/255.0.0.0
127.0.0.1/255.255.255.255
127.255.255.255/255.255.255.255
224.0.0.0/240.0.0.0
255.255.255.255/255.255.255.255
```

10550 - SNMP Query Running Process List Disclosure

Synopsis

The list of processes running on the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of running processes on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.25.4.2.1.2

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2000/11/13, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
PID    CPU    MEM  COMMAND                ARGS
  1   7848    24 System Idle Process
  4      2   1704 System
 388      0    688 smss.exe
 456      0   4804 csrss.exe      ObjectDirectory=\Windows SharedSection=1024,12288,512 Windows=On
SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User
 500      0   4404 csrss.exe      ObjectDirectory=\Windows SharedSection=1024,12288,512 Windows=On
SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User
 508      0    3856 wininit.exe
 536      0    3772 winlogon.exe
 584      0    5956 services.exe
 596      0    8512 lsass.exe
 612      0    4668 lsm.exe
 760      0    4784 svchost.exe
 824      0    5268 svchost.exe
 876      0    7460 svchost.exe
 892      0   11264 LogonUI.exe
 916      0    6412 msdtc.exe
 948      0    5468 svchost.exe      -k GPSvcGroup
 972      3   25220 svchost.exe
 996      2    9480 SLsvc.exe
1048      0    7960 svchost.exe
1084      0    5512 UI0Detect.exe
1132      0    5208 svchost.exe
1156      0   13816 svchost.exe
1272      0    7964 svchost.exe
```



```
1328      0  3964 calc.exe          FLAG: CSEC-4848-SNMP      HINT: Use the information from SNMP
output to help you get access.
1404      0  8496 spoolsv.exe
1468      0  4436 svchost.exe
1496      0  2788 svchost.exe
1540      0  4764 snmp.exe
1572      0  2056 svchost.exe
1992      0  5280 taskeng.exe      {6E35EA7A-B87D-402D-9567-6314D3773AD0}
```

10800 - SNMP Query System Information Disclosure

Synopsis

The System Information of the remote host can be obtained via SNMP.

Description

It is possible to obtain the system information about the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.1.1.

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2001/11/06, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
System information :
sysDescr      : Hardware: x86 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE - Software: Windows
Version 6.0 (Build 6001 Multiprocessor Free)
sysObjectID   : 1.3.6.1.4.1.311.1.1.3.1.2
sysUptime     : 0d 0h 13m 4s
sysContact    :
sysName       : DEIMOS
sysLocation   :
sysServices   : 76
```

10551 - SNMP Request Network Interfaces Enumeration

Synopsis

The list of network interfaces cards of the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of the network interfaces installed on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.2.1.0

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2000/11/13, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
Interface 1 information :
ifIndex      : 1
ifDescr      : Software Loopback Interface 1
```

185519 - SNMP Server Detection

Synopsis

An SNMP server is listening on the remote host.

Description

The remote service is an SNMP agent which provides management data about the device.

See Also

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

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: 2023/11/14, Modified: 2023/11/14

Plugin Output

udp/161/snmp

```
Nessus detected the following SNMP versions:  
- SNMPv1 (public community)  
- SNMPv1 (configured community)  
- SNMPv2c (public community)  
- SNMPv2c (configured community)
```

40448 - SNMP Supported Protocols Detection

Synopsis

This plugin reports all the protocol versions successfully negotiated with the remote SNMP agent.

Description

Extend the SNMP settings data already gathered by testing for\ SNMP versions other than the highest negotiated.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/07/31, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
This host supports SNMP version SNMPv1.  
This host supports SNMP version SNMPv2c.
```

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/3389/msrdp

```
This port supports TLSv1.0.
```

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/3389/msrdp

```
Subject Name:

Common Name: Deimos

Issuer Name:

Common Name: Deimos

Serial Number: A3 4D 3F 29 51 F3 11 A8 45 1B D4 C0 A4 27 C6 F7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Nov 16 20:56:42 2024 GMT
Not Valid After: May 18 20:56:42 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C2 8C 70 7F 3E 23 61 6C 3F 93 47 FD DC 66 49 A1 03 90 5F
             33 FE F1 69 BA 53 8B B1 2B AF 22 27 EE DC 43 8E 19 10 5C 0D
             04 D7 13 DC B7 D3 A5 27 06 12 03 92 2E EC 5B 58 36 B6 1E 69
             43 BB E3 52 A6 16 99 00 2E B3 59 F4 F6 26 A1 EC ED 31 0B 4B
             E5 12 08 43 8B EB A3 81 A7 CD 2E DD 3C EA 6E 13 3E 08 A2 24
             74 F8 92 D0 62 2A 27 16 35 5B EB 26 F2 B1 78 3A 0A C6 29 6E
             AA EA 58 A2 A0 C7 2A B7 55 27 9A 95 A7 BC F6 23 6F 1E 4C 10
             02 0D 37 C3 84 34 48 1B 4C 04 97 26 94 D1 7F 23 8E 15 B4 DD
             66 78 9A B3 76 D3 02 90 21 EB AF BF C4 42 5C EA 1D FE 6A D1
             73 04 DE 58 DF EB F9 35 51 29 15 50 3E 47 62 90 D1 2B D6 24
             70 3D 1E CA A0 F6 63 36 11 EA D1 14 B0 4D 97 68 86 58 DC 01
```

```
6F 65 D2 48 A3 27 F4 1B 8F 96 D9 A4 E8 EF A5 AB AE 85 A3 63
07 9A 35 05 D7 C4 3F 4E D6 5E B9 8F 99 90 FA 6E 39
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 37 B6 42 E5 39 38 30 57 DB EC 5E D9 6B 82 F5 1B F5 EA 35
3A F9 00 03 89 20 25 59 A8 DF 94 A7 52 D5 72 0C 8D 6F 57 D4
26 53 A4 04 03 E5 C0 D3 08 33 3A C1 56 99 19 45 52 73 A1 91
70 0E 1C DF 52 E6 2B 6F CC 47 26 11 00 DF EC 80 20 B0 F9 54
F3 27 03 57 F7 40 FB 27 D0 8F C1 73 3B 58 0E 0C BB EA E2 6D
8C F5 B5 BB 0A 7A 1F 44 CB E6 A5 30 85 36 75 0D 90 06 4A 83
61 7A F4 5A 41 BF 6E B8 BD C2 64 3C 9E 87 BB 61 AA B9 68 7E
9B F6 A7 8F 21 EA 1B ED C0 D3 B9 03 2C B9 19 86 E6 49 F1 5C
09 2A FD 8D 81 3E D3 76 AE FA DD 8B 3A 39 29 95 E7 99 50 06
DE 5E 0D DA 15 9B 26 36 1D AC D2 04 9E [...]
```


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/3389/msrdp

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 SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	

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: 2024/09/11

Plugin Output

tcp/3389/msrdp

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

```
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					

```
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 service does not encrypt traffic by default but does support upgrading to an encrypted connection using STARTTLS.

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/3389/msrdp

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}
```

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

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 recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/3389/msrdp

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 SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	

The fields above are :

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

64814 - Terminal Services Use SSL/TLS

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/22, Modified: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: Deimos

Issuer Name:

Common Name: Deimos

Serial Number: A3 4D 3F 29 51 F3 11 A8 45 1B D4 C0 A4 27 C6 F7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Nov 16 20:56:42 2024 GMT
Not Valid After: May 18 20:56:42 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C2 8C 70 7F 3E 23 61 6C 3F 93 47 FD DC 66 49 A1 03 90 5F
             33 FE F1 69 BA 53 8B B1 2B AF 22 27 EE DC 43 8E 19 10 5C 0D
             04 D7 13 DC B7 D3 A5 27 06 12 03 92 2E EC 5B 58 36 B6 1E 69
             43 BB E3 52 A6 16 99 00 2E B3 59 F4 F6 26 A1 EC ED 31 0B 4B
             E5 12 08 43 8B EB A3 81 A7 CD 2E DD 3C EA 6E 13 3E 08 A2 24
             74 F8 92 D0 62 2A 27 16 35 5B EB 26 F2 B1 78 3A 0A C6 29 6E
             AA EA 58 A2 A0 C7 2A B7 55 27 9A 95 A7 BC F6 23 6F 1E 4C 10
             02 0D 37 C3 84 34 48 1B 4C 04 97 26 94 D1 7F 23 8E 15 B4 DD
             66 78 9A B3 76 D3 02 90 21 EB AF BF C4 42 5C EA 1D FE 6A D1
             73 04 DE 58 DF EB F9 35 51 29 15 50 3E 47 62 90 D1 2B D6 24
             70 3D 1E CA A0 F6 63 36 11 EA D1 14 B0 4D 97 68 86 58 DC 01
```

```
6F 65 D2 48 A3 27 F4 1B 8F 96 D9 A4 E8 EF A5 AB AE 85 A3 63
07 9A 35 05 D7 C4 3F 4E D6 5E B9 8F 99 90 FA 6E 39
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 37 B6 42 E5 39 38 30 57 DB EC 5E D9 6B 82 F5 1B F5 EA 35
3A F9 00 03 89 20 25 59 A8 DF 94 A7 52 D5 72 0C 8D 6F 57 D4
26 53 A4 04 03 E5 C0 D3 08 33 3A C1 56 99 19 45 52 73 A1 91
70 0E 1C DF 52 E6 2B 6F CC 47 26 11 00 DF EC 80 20 B0 F9 54
F3 27 03 57 F7 40 FB 27 D0 8F C1 73 3B 58 0E 0C BB EA E2 6D
8C F5 B5 BB 0A 7A 1F 44 CB E6 A5 30 85 36 75 0D 90 06 4A 83
61 7A F4 5A 41 BF 6E B8 BD C2 64 3C 9E 87 BB 61 AA B9 68 7E
9B F6 A7 8F 21 EA 1B ED C0 D3 B9 03 2C B9 19 86 E6 49 F1 5C
09 2A FD 8D 81 3E D3 76 AE FA DD 8B 3A 39 29 95 E7 99 50 06
DE 5E 0D DA 15 9B 26 36 1D AC D2 04 9E [...]
```

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: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.12.0.25 to 10.12.0.161 :  
10.12.0.25
```

```
ttl was greater than 50 - Completing Traceroute.
```

```
?
```

```
Hop Count: 1
```

```
An error was detected along the way.
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

10.12.0.203



Scan Information

Start time: Sun Nov 17 17:10:32 2024

End time: Sun Nov 17 17:20:45 2024

Host Information

IP: 10.12.0.203

MAC Address: 00:50:56:A1:76:BE

OS: Microsoft Windows Server 2012 R2

Vulnerabilities

128033 - Apache 2.4.x < 2.4.41 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.41. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.41 advisory, including the following:

- A limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed. (CVE-2019-10092)

- HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with H2PushResource, could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client. (CVE-2019-10081)

- Some HTTP/2 implementations are vulnerable to unconstrained internal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint;

however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both. (CVE-2019-9517)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.41 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.8108

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-9517
CVE	CVE-2019-10081
CVE	CVE-2019-10082
CVE	CVE-2019-10092
CVE	CVE-2019-10097
CVE	CVE-2019-10098
XREF	CEA-ID:CEA-2019-0643

Plugin Information

Published: 2019/08/20, Modified: 2022/12/05

Plugin Output

tcp/80/www

```
URL           : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.41
```

139574 - Apache 2.4.x < 2.4.46 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.46. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.46 advisory.

- Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE (CVE-2020-11984)

- Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above info will mitigate this vulnerability for unpatched servers. (CVE-2020-11993)

- Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards.

Configuring the HTTP/2 feature via H2Push off will mitigate this vulnerability for unpatched servers. (CVE-2020-9490)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.46 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0108

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-9490
CVE	CVE-2020-11984
CVE	CVE-2020-11993
XREF	IAVA:2020-A-0376-S
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2020/08/13, Modified: 2022/12/06

Plugin Output

tcp/80/www

```
URL           : http://10.12.0.203/
Installed version : 2.4.38
Fixed version  : 2.4.46
```

150280 - Apache 2.4.x < 2.4.47 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.47. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.47 changelog:

- Unexpected <Location> section matching with 'MergeSlashes OFF' (CVE-2021-30641)
- mod_auth_digest: possible stack overflow by one nul byte while validating the Digest nonce. (CVE-2020-35452)
- mod_session: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service with a malicious backend server and SessionHeader. (CVE-2021-26691)
- mod_session: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service. (CVE-2021-26690)
- mod_proxy_http: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service. (CVE-2020-13950)
- Windows: Prevent local users from stopping the httpd process (CVE-2020-13938)
- mod_proxy_wstunnel, mod_proxy_http: Handle Upgradable protocols end-to-end negotiation. (CVE-2019-17567)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

Solution

Upgrade to Apache version 2.4.47 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.6847

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2019-17567
CVE	CVE-2020-13938
CVE	CVE-2020-13950
CVE	CVE-2020-35452
CVE	CVE-2021-26690
CVE	CVE-2021-26691
CVE	CVE-2021-30641
XREF	IAVA:2021-A-0259-S

Plugin Information

Published: 2021/06/04, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/
Installed version : 2.4.38
Fixed version  : 2.4.47
```

161454 - Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow

Synopsis

The remote web server is affected by a buffer overflow vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.52. It is, therefore, affected by a flaw related to mod_lua when handling multipart content. A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.52 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.1305

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE CVE-2021-44790
XREF IAVA:2021-A-0604-S

Plugin Information

Published: 2022/05/24, Modified: 2023/10/26

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.52
```

158900 - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.

- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)
- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)
- Possible buffer overflow with very large or unlimited LimitXMLRequestBody in core: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721)
- Read/write beyond bounds in mod_sed: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. Acknowledgements: Ronald Crane (Zippenhop LLC) (CVE-2022-23943)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<http://www.apache.org/dist/httpd/Announcement2.4.html>
https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.53 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.3992

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-22719
CVE	CVE-2022-22720
CVE	CVE-2022-22721
CVE	CVE-2022-23943
XREF	IAVA:2022-A-0124-S

Plugin Information

Published: 2022/03/14, Modified: 2023/11/06

Plugin Output

tcp/80/www

```
URL           : http://10.12.0.203/
Installed version : 2.4.38
Fixed version  : 2.4.53
```

193421 - Apache 2.4.x < 2.4.54 Authentication Bypass

Synopsis

The remote web server is affected by an authentication bypass vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by an authentication bypass vulnerability as referenced in the 2.4.54 advisory.

- X-Forwarded-For dropped by hop-by-hop mechanism in mod_proxy: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

Acknowledgements: The Apache HTTP Server project would like to thank Gaetan Ferry (Synacktiv) for reporting this issue

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0104

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE CVE-2022-31813
XREF IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.54
```

161948 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Read beyond bounds via ap_rwrite(): The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_lua's r:puts() function. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28614)
- Read beyond bounds in ap_strcmp_match(): Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28615)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.0147

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE CVE-2022-28614
CVE CVE-2022-28615
XREF IAVA:2022-A-0230-S

Plugin Information

Published: 2022/06/08, Modified: 2024/04/18

Plugin Output

tcp/80/www

```
URL : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version : 2.4.54
```

170113 - Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.55. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.55 advisory.

- A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier. (CVE-2006-20001)

- Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions. (CVE-2022-36760)

- Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client. (CVE-2022-37436)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.55 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.5

EPSS Score

0.0235

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2006-20001
CVE	CVE-2022-36760
CVE	CVE-2022-37436
XREF	IAVA:2023-A-0047-S

Plugin Information

Published: 2023/01/18, Modified: 2023/03/10

Plugin Output

tcp/80/www

```
URL           : http://10.12.0.203/
Installed version : 2.4.38
Fixed version  : 2.4.55
```

172186 - Apache 2.4.x < 2.4.56 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.56. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.56 advisory.

- HTTP request splitting with mod_rewrite and mod_proxy: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule ^/here/(.*) http://example.com:8080/elsewhere?\$1 http://example.com:8080/elsewhere ; [P] ProxyPassReverse /here/ http://example.com:8080/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Acknowledgements: finder: Lars Krapf of Adobe (CVE-2023-25690)

- Apache HTTP Server: mod_proxy_uwsgi HTTP response splitting: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.

Special characters in the origin response header can truncate/split the response forwarded to the client.

Acknowledgements: finder: Dimas Fariski Setyawan Putra (nyxsorcerer) (CVE-2023-27522)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.56 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0135

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-25690
CVE	CVE-2023-27522
XREF	IAVA:2023-A-0124-S

Plugin Information

Published: 2023/03/07, Modified: 2023/10/21

Plugin Output

tcp/80/www

```
URL           : http://10.12.0.203/
Installed version : 2.4.38
Fixed version   : 2.4.56
```

201198 - Apache 2.4.x < 2.4.60 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.60. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.60 advisory.

- Serving WebSocket protocol upgrades over a HTTP/2 connection could result in a Null Pointer dereference, leading to a crash of the server process, degrading performance. (CVE-2024-36387)
- SSRF in Apache HTTP Server on Windows allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests or content Users are recommended to upgrade to version 2.4.60 which fixes this issue. Note: Existing configurations that access UNC paths will have to configure new directive UNCList to allow access during request processing. (CVE-2024-38472)
- Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38473)
- Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag UnsafeAllow3F is specified. (CVE-2024-38474)
- Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/ directly reachable by any URL, resulting in code execution or source code disclosure. Substitutions in server context that use a backreferences or variables as the first segment of the substitution are affected. Some unsafe RewriteRules will be broken by this change and the rewrite flag UnsafePrefixStat can be used to opt back in once ensuring the substitution is appropriately constrained. (CVE-2024-38475)
- Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38476)
- null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-38477)
- Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy. Users are recommended to upgrade to version 2.4.60, which fixes this issue. (CVE-2024-39573)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.60 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0359

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-36387
CVE	CVE-2024-38472
CVE	CVE-2024-38473
CVE	CVE-2024-38474
CVE	CVE-2024-38475
CVE	CVE-2024-38476
CVE	CVE-2024-38477
CVE	CVE-2024-39573
XREF	IAVA:2024-A-0378-S

Plugin Information

Published: 2024/07/01, Modified: 2024/08/22

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.60
```

156255 - Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF

Synopsis

The remote web server is affected by a denial of service or server-side request forgery vulnerability.

Description

The version of Apache httpd installed on the remote host is equal to or greater than 2.4.7 and prior to 2.4.52.

It is, therefore, affected by a flaw related to acting as a forward proxy.

A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.52 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.2048

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-44224
CVE	CVE-2021-44790
XREF	IAVA:2021-A-0604-S

Plugin Information

Published: 2021/12/23, Modified: 2023/11/22

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.52
```

153583 - Apache < 2.4.49 Multiple Vulnerabilities

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog.

- A crafted request uri-path can cause mod_proxy to forward the request to an origin server chosen by the remote user. (CVE-2021-40438)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.1

EPSS Score

0.967

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-40438
XREF	IAVA:2021-A-0440-S
XREF	CISA-KNOWN-EXPLOITED:2021/12/15

Plugin Information

Published: 2021/09/23, Modified: 2023/04/25

Plugin Output

tcp/80/www

```
URL           : http://10.12.0.203/
Installed version : 2.4.38
Fixed version  : 2.4.49
```

153584 - Apache < 2.4.49 Multiple Vulnerabilities

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.49 changelog.

- ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. (CVE-2021-39275)
- Malformed requests may cause the server to dereference a NULL pointer. (CVE-2021-34798)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0087

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-34798
CVE	CVE-2021-39275
XREF	IAVA:2021-A-0440-S

Plugin Information

Published: 2021/09/23, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.49
```


160480 - OpenSSL 1.0.2 < 1.0.2ze Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2ze. It is, therefore, affected by a vulnerability as referenced in the 1.0.2ze advisory.

- The `c_rehash` script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the `c_rehash` script is considered obsolete and should be replaced by the OpenSSL `rehash` command line tool.

Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).

Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd). (CVE-2022-1292)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://www.cve.org/CVERecord?id=CVE-2022-1292>

<http://www.nessus.org/u?f1567dce>

<https://www.openssl.org/news/secadv/20220503.txt>

Solution

Upgrade to OpenSSL version 1.0.2ze or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.1023

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE CVE-2022-1292
XREF IAVA:2022-A-0186-S

Plugin Information

Published: 2022/05/04, Modified: 2024/10/23

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2ze
```

162419 - OpenSSL 1.0.2 < 1.0.2zf Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2zf. It is, therefore, affected by a vulnerability as referenced in the 1.0.2zf advisory.

- In addition to the `c_rehash` shell command injection identified in CVE-2022-1292, further circumstances where the `c_rehash` script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the `c_rehash` script is considered obsolete and should be replaced by the OpenSSL `rehash` command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze). (CVE-2022-2068)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?5b3cb0db>

<https://www.cve.org/CVERecord?id=CVE-2022-2068>

<https://www.openssl.org/news/secadv/20220621.txt>

Solution

Upgrade to OpenSSL version 1.0.2zf or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.1226

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-2068

Plugin Information

Published: 2022/06/21, Modified: 2024/11/05

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2zf
```

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2zk. It is, therefore, affected by a vulnerability as referenced in the 1.0.2zk advisory.

- Issue summary: Calling the OpenSSL API function `SSL_select_next_proto` with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application behaviour or a crash.

In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the `SSL_select_next_proto` function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function `SSL_select_next_proto` is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The `SSL_select_next_proto` function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where `SSL_select_next_proto` is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the `SSL_select_next_proto` function has been called as expected (with the list supplied by the client passed in the `client/client_len` parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the `client/client_len` parameters, and has additionally failed to correctly handle a no overlap response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the `SSL_select_next_proto` function is accidentally called with a `client_len` of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. Found by Joseph Birr-Pixton. Thanks to David Benjamin (Google). Fix developed by Matt Caswell. Fixed in OpenSSL 1.1.1za (premium support) (Affected since 1.1.1). (CVE-2024-5535)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://www.cve.org/CVERecord?id=CVE-2024-5535>

Solution

Upgrade to OpenSSL version 1.0.2zk or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2024-5535

Plugin Information

Published: 2024/06/27, Modified: 2024/10/07

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2zk
```

123642 - Apache 2.4.x < 2.4.39 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.39. It is, therefore, affected by multiple vulnerabilities:

- A privilege escalation vulnerability exists in module scripts due to an ability to execute arbitrary code as the parent process by manipulating the scoreboard. (CVE-2019-0211)
- An access control bypass vulnerability exists in mod_auth_digest due to a race condition when running in a threaded server. An attacker with valid credentials could authenticate using another username. (CVE-2019-0217)
- An access control bypass vulnerability exists in mod_ssl when using per-location client certificate verification with TLSv1.3. (CVE-2019-0215)

In addition, Apache httpd is also affected by several additional vulnerabilities including a denial of service, read-after-free and URL path normalization inconsistencies.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?a84bee48>

<http://www.nessus.org/u?586e6a34>

Solution

Upgrade to Apache version 2.4.39 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

EPSS Score

0.9607

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-0196
CVE	CVE-2019-0197
CVE	CVE-2019-0211
CVE	CVE-2019-0215
CVE	CVE-2019-0217
CVE	CVE-2019-0220
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CEA-ID:CEA-2019-0203

Plugin Information

Published: 2019/04/02, Modified: 2023/04/25

Plugin Output

tcp/80/www

```
URL           : http://10.12.0.203/
Installed version : 2.4.38
Fixed version   : 2.4.39
```

193422 - Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability

Synopsis

The remote web server is affected by a HTTP request smuggling vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by a http request smuggling vulnerability as referenced in the 2.4.54 advisory.

- Possible request smuggling in mod_proxy_ajp: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions. Acknowledgements: Richter Z @ 360 Noah Lab

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0064

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-26377
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.54
```

193423 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Denial of Service mod_sed: If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort. Acknowledgements: This issue was found by Brian Moussalli from the JFrog Security Research team

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.2877

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-30522
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.54
```

193424 - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Denial of service in mod_lua r:parsebody: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-29404)

- Information Disclosure in mod_lua with websockets: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-30556)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0243

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-29404
CVE	CVE-2022-30556
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/80/www

```
URL           : http://10.12.0.203/
Installed version : 2.4.38
Fixed version   : 2.4.54
```

183391 - Apache 2.4.x < 2.4.58 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.58. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.58 advisory.

- Apache HTTP Server: DoS in HTTP/2 with initial windows size 0: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known slow loris attack pattern. This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57. Users are recommended to upgrade to version 2.4.58, which fixes the issue.

Acknowledgements: (CVE-2023-43622)

- Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window where the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During normal HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue. Acknowledgements: (CVE-2023-45802)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.58 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0017

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE CVE-2023-43622
CVE CVE-2023-45802
XREF IAVA:2023-A-0572-S

Plugin Information

Published: 2023/10/19, Modified: 2024/04/29

Plugin Output

tcp/80/www

```
URL : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version : 2.4.58
```

193419 - Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)

Synopsis

The remote web server is affected by an out-of-bounds read vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.58. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.58 advisory.

- mod_macro buffer over-read: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server. This issue affects Apache HTTP Server: through 2.4.57.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.58 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0283

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-31122
XREF	IAVA:2023-A-0572-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/29

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.58
```

192923 - Apache 2.4.x < 2.4.59 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.59. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.59 advisory.

- Apache HTTP Server: HTTP Response Splitting in multiple modules: HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack. Users are recommended to upgrade to version 2.4.59, which fixes this issue. Acknowledgements: (CVE-2024-24795)

- Apache HTTP Server: HTTP/2 DoS by memory exhaustion on endless continuation frames: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nhttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

Acknowledgements: finder: Bartek Nowotarski (<https://nowotarski.info/>) (CVE-2024-27316)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.59 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0013

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-38709
CVE	CVE-2024-24795
CVE	CVE-2024-27316
XREF	IAVA:2024-A-0202-S

Plugin Information

Published: 2024/04/04, Modified: 2024/07/12

Plugin Output

tcp/80/www

```
URL           : http://10.12.0.203/
Installed version : 2.4.38
Fixed version  : 2.4.59
```

210450 - Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.62. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.62 advisory.

- SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue. (CVE-2024-40898)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.62 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.1

EPSS Score

0.0008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2024-40898

Plugin Information

Published: 2024/11/06, Modified: 2024/11/06

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/
Installed version : 2.4.38
Fixed version  : 2.4.62
```

153585 - Apache >= 2.4.17 < 2.4.49 mod_http2

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is greater than 2.4.17 and prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog. A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0013

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-33193
XREF	IAVA:2021-A-0440-S

Plugin Information

Published: 2021/09/23, Modified: 2023/11/29

Plugin Output

tcp/80/www

```
URL           : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.49
```

153586 - Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host greater than 2.4.30 and is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog. A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS).

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0016

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-36160
XREF	IAVA:2021-A-0440-S

Plugin Information

Published: 2021/09/23, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.49
```

79638 - MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)

Synopsis

The remote Windows host is affected by a remote code execution vulnerability.

Description

The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.

Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent.

See Also

<http://www.nessus.org/u?64e97902>

Solution

Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.9632

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	70954
CVE	CVE-2014-6321
MSKB	2992611
XREF	CERT:505120
XREF	MSFT:MS14-066

Exploitable With

Core Impact (true)

Plugin Information

Published: 2014/12/01, Modified: 2024/09/11

Plugin Output

tcp/3389/msrdp

152780 - OpenSSL 1.0.2 < 1.0.2za Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2za. It is, therefore, affected by a vulnerability as referenced in the 1.0.2za advisory.

- ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are represented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own d2i functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the data and length fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the data field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack).

It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y). (CVE-2021-3712)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?c568570a>

<https://www.cve.org/CVERecord?id=CVE-2021-3712>

<https://www.openssl.org/news/secadv/20210824.txt>

Solution

Upgrade to OpenSSL version 1.0.2za or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0049

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-3712
XREF	IAVA:2021-A-0395-S

Plugin Information

Published: 2021/08/24, Modified: 2024/10/23

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2za
```

158973 - OpenSSL 1.0.2 < 1.0.2zd Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2zd. It is, therefore, affected by a vulnerability as referenced in the 1.0.2zd advisory.

- The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self- signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc). (CVE-2022-0778)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://www.cve.org/CVERecord?id=CVE-2022-0778>

<http://www.nessus.org/u?dcd01c29>

<https://www.openssl.org/news/secadv/20220315.txt>

Solution

Upgrade to OpenSSL version 1.0.2zd or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.1

EPSS Score

0.0158

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE CVE-2022-0778
XREF IAVA:2022-A-0121-S

Plugin Information

Published: 2022/03/16, Modified: 2024/10/23

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2zd
```

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2zg. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.0.2zg advisory.

- There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName.

X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network. (CVE-2023-0286)

- The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected. (CVE-2023-0215)

- A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption.

The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection. (CVE-2022-4304)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://www.cve.org/CVERecord?id=CVE-2023-0286>
<https://www.openssl.org/news/secadv/20230207.txt>
<https://www.openssl.org/policies/secpolicy.html>
<https://www.cve.org/CVERecord?id=CVE-2023-0215>
<https://www.cve.org/CVERecord?id=CVE-2022-4304>

Solution

Upgrade to OpenSSL version 1.0.2zg or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0064

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-4304
CVE	CVE-2023-0215
CVE	CVE-2023-0286

Plugin Information

10.12.0.203

Published: 2023/02/07, Modified: 2024/10/23

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2zg
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

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

Description

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

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

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

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

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

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

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

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

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

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.2

EPSS Score

0.0111

0.0111

CVSS v2.0 Base Score

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

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

CVSS v2.0 Temporal Score

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

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

References	
BID	11849

BID 11849

BID 33065

CVE CVE-2004-2761

CVE CVE-2005-4900

XREF CERT:836068

XREF CWE:310

Plugin Information
Published: 2009/01/05, Modified: 2023/12/15

Published: 2009/01/05, Modified: 2023/12/15

Plugin Output

tcp/3389/msrdp

tcp/3389/msrdp

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

Subject : CN=Mercury.csec388.depaulsec labs.com

Signature Algorithm : SHA-1 With RSA Encryption

Valid From : Nov 17 03:56:10 2024 GMT

Valid To : May 19 03:56:10 2025 GMT

```
Raw PEM certificate :
```

-----BEGIN CERTIFICATE-----

MIIDBjCCAe6gAwIBAgIQTZp/

Hth3CJJCMbdqsRjwwjANBqkqhkiG9w0BAQUFADAsMSowKAYDVQQDEyFNZXJjdXJ5LmNzZWZmZDguZGVwYXVsc2VjbGFicy5jb20wHh

+9DJmQLc/xGYnzZu34rv+H2OOCuFlrcRNidau0rnRb0a7HiB67OYfLcARJu47pQuZ9U34ZmnSPoEZPS

+oGsbNhLQy4Cj3Mch2cVogcrOsDXt/BY21kM/SbgbZpysLosH1TYe+fBwX8B/x1b+kCrL/5b2gVh2cha3XavDS1f1trzuYy

+yy7V6D9Wz0Ye//

WPI5Et5qERh8a0D8yp4eUwwUifaWXIe0sYSHvUNSFRCVhkKX6EOXZ0cdTJyxCJXSY1mkMCbou7uSwbogkdGaaln5lSbc6o1DlyavC5

+Eam6usybTKG99FPWrFqujj74xa33erIQjG4zyHrWWDDtEs95669bvM3YsUSDs

+ryKMnLNOeNNHYRwiYAWzhsOG2NELukrK8wOfmWbqEuM68+b7FMLeYEGu8N7xk+A6XZp2jnExW4zJg9iGtPH//

Vpx6gwO667RAeYZjIo+0Vng+Oxcfe4sxrJCL0m7CPkw+gia3MAmSnu2TvIrZW0+zL9cofWJzQid/wg==

-----END CERTIFICATE-----

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

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

<https://sweet32.info>

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.1

EPSS Score

0.0053

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

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

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	
SHA1					

The fields above are :

{Tenable ciphername}

{Cipher ID code}

Kex={key exchange}

Auth={authentication}

Encrypt={symmetric encryption method}

MAC={message authentication code}

{export flag}

135290 - Apache 2.4.x < 2.4.42 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.42. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.42 advisory.

- In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server. (CVE-2020-1934)

- In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL. (CVE-2020-1927)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.42 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.0

EPSS Score

0.0026

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

10.12.0.203

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

STIG Severity

I

References

CVE	CVE-2020-1927
CVE	CVE-2020-1934
XREF	IAVA:2020-A-0129-S
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/04/10, Modified: 2022/12/05

Plugin Output

tcp/80/www

```
URL           : http://10.12.0.203/
Installed version : 2.4.38
Fixed version  : 2.4.42
```

193420 - Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)

Synopsis

The remote web server is affected by an out-of-bound read vulnerability

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by an out-of-bounds read vulnerability as referenced in the 2.4.54 advisory.

- Read beyond bounds in mod_isapi: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0016

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE CVE-2022-28330
XREF IAVA:2022-A-0230-S

Plugin Information

Published: 2024/04/17, Modified: 2024/04/18

Plugin Output

tcp/80/www

```
URL          : http://10.12.0.203/  
Installed version : 2.4.38  
Fixed version  : 2.4.54
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

<http://www.nessus.org/u?e979b5cb>

<http://www.apacheweek.com/issues/03-01-24>

<https://download.oracle.com/sunalerts/1000718.1.html>

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.0

EPSS Score

0.0058

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2024/04/09

Plugin Output

tcp/80/www

To disable these methods, add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.

Nessus sent the following TRACE request : \n\n----- snip
-----\nTRACE /Nessus1628726117.html HTTP/1.1

Connection: Close
Host: 10.12.0.203
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

----- snip ----- \n\nand received the
following response from the remote server : \n\n----- snip
-----\nHTTP/1.1 200 OK

Date: Mon, 18 Nov 2024 06:16:35 GMT
Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http

TRACE /Nessus1628726117.html HTTP/1.1
Connection: Keep-Alive

```
Host: 10.12.0.203
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

```
----- snip -----\n
```

122504 - OpenSSL 1.0.2 < 1.0.2r Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2r. It is, therefore, affected by a vulnerability as referenced in the 1.0.2r advisory.

- If an application encounters a fatal protocol error and then calls `SSL_shutdown()` twice (once to send a `close_notify`, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable non-stitched ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call `SSL_shutdown()` twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). (CVE-2019-1559)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?015dc646>

<https://www.cve.org/CVERecord?id=CVE-2019-1559>

<https://www.openssl.org/news/secadv/20190226.txt>

Solution

Upgrade to OpenSSL version 1.0.2r or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0131

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	107174
CVE	CVE-2019-1559
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2019/03/01, Modified: 2024/10/23

Plugin Output

tcp/80/www

```
Banner          : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version    : 1.0.2r
```

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2t. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.0.2t advisory.

- In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/ PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s). (CVE-2019-1563)

- Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s). (CVE-2019-1547)

- OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub- directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c).

Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

(CVE-2019-1552)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?2c98b1de>

<http://www.nessus.org/u?41db39fc>
<http://www.nessus.org/u?bd4abed7>
<https://www.cve.org/CVERecord?id=CVE-2019-1547>
<https://www.cve.org/CVERecord?id=CVE-2019-1552>
<https://www.cve.org/CVERecord?id=CVE-2019-1563>
<https://www.openssl.org/news/secadv/20190910.txt>
<https://www.openssl.org/news/secadv/20190730.txt>

Solution

Upgrade to OpenSSL version 1.0.2t or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0314

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE CVE-2019-1547

CVE	CVE-2019-1552
CVE	CVE-2019-1563
XREF	IAVA:2019-A-0303-S

Plugin Information

Published: 2019/08/23, Modified: 2024/10/23

Plugin Output

tcp/80/www

```
Banner          : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version    : 1.0.2t
```

132726 - OpenSSL 1.0.2 < 1.0.2u Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2u. It is, therefore, affected by a vulnerability as referenced in the 1.0.2u advisory.

- There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t). (CVE-2019-1551)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?4da1722d>

<https://www.cve.org/CVERecord?id=CVE-2019-1551>

<https://www.openssl.org/news/secadv/20191206.txt>

Solution

Upgrade to OpenSSL version 1.0.2u or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

10.12.0.203

325

0.0022

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2019-1551
XREF	IAVA:2019-A-0303-S

Plugin Information

Published: 2020/01/09, Modified: 2024/10/23

Plugin Output

tcp/80/www

```
Banner           : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version    : 1.0.2u
```

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2x. It is, therefore, affected by a vulnerability as referenced in the 1.0.2x advisory.

- The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMES contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified.

OpenSSL's s_server, s_client and verify tools have support for the -crl_download option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue.

Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). (CVE-2020-1971)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?db9e764c>

<https://www.cve.org/CVERecord?id=CVE-2020-1971>

<https://www.openssl.org/news/secadv/20201208.txt>

Solution

Upgrade to OpenSSL version 1.0.2x or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.1

EPSS Score

0.0044

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-1971
XREF	IAVA:2020-A-0566-S
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/12/10, Modified: 2024/10/23

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2x
```


200206 - OpenSSL 1.0.2 < 1.0.2zc Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2zc. It is, therefore, affected by a vulnerability as referenced in the 1.0.2zc advisory.

- There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc- dev (Affected 1.0.2-1.0.2zb). (CVE-2021-4160)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?bcb95c72>

<https://www.cve.org/CVERecord?id=CVE-2021-4160>

<https://www.openssl.org/news/secadv/20220128.txt>

Solution

Upgrade to OpenSSL version 1.0.2zc or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0065

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-4160
XREF	IAVA:2021-A-0602-S

Plugin Information

Published: 2024/06/07, Modified: 2024/10/07

Plugin Output

tcp/80/www

```
Banner          : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version    : 1.0.2zc
```

157231 - OpenSSL 1.0.2 < 1.0.2zc-dev Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2zc-dev. It is, therefore, affected by a vulnerability as referenced in the 1.0.2zc-dev advisory.

- There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb). (CVE-2021-4160)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?acbd2764>

<https://www.openssl.org/news/secadv/20220128.txt>

Solution

Upgrade to OpenSSL version 1.0.2zc-dev or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0065

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-4160

Plugin Information

Published: 2022/01/29, Modified: 2024/10/07

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2zc-dev
```

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2zh. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.0.2zh advisory.

- Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that use `OBJ_obj2txt()` directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit may experience notable to very long delays when processing those messages, which may lead to a Denial of Service. An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers - most of which have no size limit.

`OBJ_obj2txt()` may be used to translate an ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSL type `ASN1_OBJECT`) to its canonical numeric text form, which are the sub-identifiers of the OBJECT IDENTIFIER in decimal form, separated by periods. When one of the sub-identifiers in the OBJECT IDENTIFIER is very large (these are sizes that are seen as absurdly large, taking up tens or hundreds of KiBs), the translation to a decimal number in text may take a very long time. The time complexity is $O(n^2)$ with 'n'

being the size of the sub-identifiers in bytes (*). With OpenSSL 3.0, support to fetch cryptographic algorithms using names / identifiers in string form was introduced. This includes using OBJECT IDENTIFIERS in canonical numeric text form as identifiers for fetching algorithms. Such OBJECT IDENTIFIERS may be received through the ASN.1 structure `AlgorithmIdentifier`, which is commonly used in multiple protocols to specify what cryptographic algorithm should be used to sign or verify, encrypt or decrypt, or digest passed data. Applications that call `OBJ_obj2txt()` directly with untrusted data are affected, with any version of OpenSSL. If the use is for the mere purpose of display, the severity is considered low. In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS. It also impacts anything that processes X.509 certificates, including simple things like verifying its signature. The impact on TLS is relatively low, because all versions of OpenSSL have a 100KiB limit on the peer's certificate chain. Additionally, this only impacts clients, or servers that have explicitly enabled client authentication. In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects, such as X.509 certificates. This is assumed to not happen in such a way that it would cause a Denial of Service, so these versions are considered not affected by this issue in such a way that it would be cause for concern, and the severity is therefore considered low. (CVE-2023-2650)

- Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks. Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether. Policy processing is disabled by default but can be enabled by passing the ``-policy'` argument to the command line utilities or by calling the ``X509_VERIFY_PARAM_set1_policies()'` function. (CVE-2023-0465)

- The function `X509_VERIFY_PARAM_add0_policy()` is documented to implicitly enable the certificate policy check when doing certificate verification. However the implementation of the function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification.

As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the `X509_VERIFY_PARAM_add0_policy()` function. Instead the applications that require OpenSSL to perform certificate policy check need to use `X509_VERIFY_PARAM_set1_policies()` or explicitly enable

the policy check by calling `X509_VERIFY_PARAM_set_flags()` with the `X509_V_FLAG_POLICY_CHECK` flag argument.

Certificate policy checks are disabled by default in OpenSSL and are not commonly used by applications. (CVE-2023-0466)

- A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy` argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()` function. (CVE-2023-0464)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://www.openssl.org/news/secadv/20230328.txt>
<https://www.openssl.org/news/secadv/20230530.txt>
<https://www.openssl.org/policies/general/security-policy.html>
<https://www.openssl.org/policies/secpolicy.html>
<https://www.openssl.org/news/secadv/20230322.txt>
<https://www.cve.org/CVERecord?id=CVE-2023-0464>
<https://www.cve.org/CVERecord?id=CVE-2023-0464>
<https://www.cve.org/CVERecord?id=CVE-2023-0465>
<https://www.cve.org/CVERecord?id=CVE-2023-0466>
<https://www.cve.org/CVERecord?id=CVE-2023-2650>

Solution

Upgrade to OpenSSL version 1.0.2zh or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0051

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-0464
CVE	CVE-2023-0464
CVE	CVE-2023-0465
CVE	CVE-2023-0466
CVE	CVE-2023-2650
XREF	IAVA:2023-A-0158-S

Plugin Information

Published: 2023/03/22, Modified: 2024/10/23

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2zh
```

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2zi. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.0.2zi advisory.

- Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary:

Applications that use the functions `DH_check()`, `DH_check_ex()` or `EVP_PKEY_param_check()` to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function `DH_check()` performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large `q` parameter value can also trigger an overly long computation during some of these checks. A correct `q` value, if present, cannot be larger than the modulus `p` parameter, thus it is unnecessary to perform these checks if `q` is larger than `p`. An application that calls `DH_check()` and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function `DH_check()` is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are `DH_check_ex()` and `EVP_PKEY_param_check()`.

Also vulnerable are the OpenSSL `dhparam` and `pkeyparam` command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-3817)

- Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary:

Applications that use the functions `DH_check()`, `DH_check_ex()` or `EVP_PKEY_param_check()` to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function `DH_check()` performs various checks on DH parameters. One of those checks confirms that the modulus ('`p`' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the `DH_check()` function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls `DH_check()` and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function `DH_check()` is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are `DH_check_ex()` and `EVP_PKEY_param_check()`. Also vulnerable are the OpenSSL `dhparam` and `pkeyparam` command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-3446)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://www.openssl.org/news/secadv/20230719.txt>

<https://www.openssl.org/news/secadv/20230731.txt>

<https://www.openssl.org/policies/secpolicy.html>

<https://www.cve.org/CVERecord?id=CVE-2023-3446>

<https://www.cve.org/CVERecord?id=CVE-2023-3817>

Solution

Upgrade to OpenSSL version 1.0.2zi or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.9

EPSS Score

0.0014

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-3446
CVE	CVE-2023-3817
XREF	IAVA:2023-A-0398-S

Plugin Information

Published: 2023/07/19, Modified: 2024/10/07

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2zi
```

184812 - OpenSSL 1.0.2 < 1.0.2zj Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2zj. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.0.2zj advisory.

- Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are:

PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. (CVE-2024-0727)

- Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the -pubcheck option, as well as the OpenSSL genpkey command line application.

The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-5678)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://www.cve.org/CVERecord?id=CVE-2023-5678>

<https://www.cve.org/CVERecord?id=CVE-2024-0727>

Solution

Upgrade to OpenSSL version 1.0.2zj or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0023

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-5678
CVE	CVE-2024-0727
XREF	IAVA:2024-A-0121-S

Plugin Information

Published: 2023/11/07, Modified: 2024/10/07

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
```

Fixed version : 1.0.2zj

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2zl. It is, therefore, affected by a vulnerability as referenced in the 1.0.2zl advisory.

- Issue summary: Use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes. Impact summary: Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only named curves are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary (GF(2^m)) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low. In particular, the X9.62 encoding is used for ECC keys in X.509 certificates, so problematic inputs cannot occur in the context of processing X.509 certificates. Any problematic use-cases would have to be using an exotic curve encoding. The affected APIs include:

EC_GROUP_new_curve_GF2m(), EC_GROUP_new_from_params(), and various supporting BN_GF2m_*() functions.

Applications working with exotic explicit binary (GF(2^m)) curve parameters, that make it possible to represent invalid field polynomials with a zero constant term, via the above or similar APIs, may terminate abruptly as a result of reading or writing outside of array bounds. Remote code execution cannot easily be ruled out. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.

(CVE-2024-9143)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?09a3136b>

<https://openssl-library.org/news/secadv/20241016.txt>

<https://openssl-library.org/policies/general/security-policy/#low>

<https://www.cve.org/CVERecord?id=CVE-2024-9143>

Solution

Upgrade to OpenSSL version 1.0.2zl or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.9

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2024-9143

Plugin Information

Published: 2024/10/16, Modified: 2024/11/11

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2zl
```

18405 - Remote Desktop Protocol Server Man-in-the-Middle Weakness

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a publicly known hard-coded RSA private key. Any attacker in a privileged network location can use the key for this attack.

See Also

<http://www.nessus.org/u?8033da0d>

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and
- On Microsoft Windows operating systems, select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

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)

VPR Score

2.5

EPSS Score

0.0127

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	13818
CVE	CVE-2005-1794

Plugin Information

Published: 2005/06/01, Modified: 2022/08/24

Plugin Output

tcp/3389/msrdp

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/3389/msrdp

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=Mercury.csec388.depaulseclabs.com  
| -Issuer  : CN=Mercury.csec388.depaulseclabs.com
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

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

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

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

See Also

<https://www.rc4nomore.com/>

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

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

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

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0076

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

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

Plugin Output

tcp/3389/msrdp

List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

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

The fields above are :

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

57582 - SSL Self-Signed Certificate

Synopsis

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

Description

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/3389/msrdp

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

```
| -Subject : CN=Mercury.csec388.depaulseclabs.com
```

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/3389/msrdp

TLsv1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

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: 2024/05/14

Plugin Output

tcp/3389/msrdp

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

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis

The remote Terminal Services doesn't use Network Level Authentication only.

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11))

<http://www.nessus.org/u?e2628096>

Solution

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/03/23, Modified: 2024/07/17

Plugin Output

tcp/3389/msrdp

```
Nessus was able to negotiate non-NLA (Network Level Authentication) security.
```

57690 - Terminal Services Encryption Level is Medium or Low

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.

Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Solution

Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/25, Modified: 2024/07/17

Plugin Output

tcp/3389/msrdp

```
The terminal services encryption level is set to :  
  
2. Medium
```

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2w. It is, therefore, affected by a vulnerability as referenced in the 1.0.2w advisory.

- The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites.

This issue affects OpenSSL 1.0.2 which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v). (CVE-2020-1968)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?825d05ae>

<https://www.cve.org/CVERecord?id=CVE-2020-1968>

<https://www.openssl.org/news/secadv/20200909.txt>

Solution

Upgrade to OpenSSL version 1.0.2w or later.

Risk Factor

Medium

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 v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.0056

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-1968
XREF	CEA-ID:CEA-2021-0004

Plugin Information

Published: 2021/02/10, Modified: 2024/10/23

Plugin Output

tcp/80/www

```
Banner      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version  : 1.0.2w
```

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 1.0.2y. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.0.2y advisory.

- The OpenSSL public API function `X509_issuer_and_serial_hash()` attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function `X509_issuer_and_serial_hash()` is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x). (CVE-2021-23841)

- Calls to `EVP_CipherUpdate`, `EVP_EncryptUpdate` and `EVP_DecryptUpdate` may overflow the output length argument in some cases where the input length is close to the maximum permissible length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash.

OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i).

Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x). (CVE-2021-23840)

- OpenSSL 1.0.2 supports SSLv2. If a client attempts to negotiate SSLv2 with a server that is configured to support both SSLv2 and more recent SSL and TLS versions then a check is made for a version rollback attack when unpadding an RSA signature. Clients that support SSL or TLS versions greater than SSLv2 are supposed to use a special form of padding. A server that supports greater than SSLv2 is supposed to reject connection attempts from a client where this special form of padding is present, because this indicates that a version rollback has occurred (i.e. both client and server support greater than SSLv2, and yet this is the version that is being requested). The implementation of this padding check inverted the logic so that the connection attempt is accepted if the padding is present, and rejected if it is absent. This means that such as server will accept a connection if a version rollback attack has occurred. Further the server will erroneously reject a connection if a normal SSLv2 connection attempt is made. Only OpenSSL 1.0.2 servers from version 1.0.2s to 1.0.2x are affected by this issue. In order to be vulnerable a 1.0.2 server must: 1) have configured SSLv2 support at compile time (this is off by default), 2) have configured SSLv2 support at runtime (this is off by default), 3) have configured SSLv2 ciphersuites (these are not in the default ciphersuite list) OpenSSL 1.1.1 does not have SSLv2 support and therefore is not vulnerable to this issue. The underlying error is in the implementation of the `RSA_padding_check_SSLv23()` function. This also affects the `RSA_SSLV23_PADDING` padding mode used by various other functions. Although 1.1.1 does not support SSLv2 the `RSA_padding_check_SSLv23()` function still exists, as does the `RSA_SSLV23_PADDING` padding mode. Applications that directly call that function or use that padding mode will encounter this issue.

However since there is no support for the SSLv2 protocol in 1.1.1 this is considered a bug and not a security issue in that version. OpenSSL 1.0.2 is out of support and no longer receiving public updates.

Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j.

Fixed in OpenSSL 1.0.2y (Affected 1.0.2s-1.0.2x). (CVE-2021-23839)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?6d58067e>

<http://www.nessus.org/u?95cac758>

<http://www.nessus.org/u?f389e444>

<https://www.cve.org/CVERecord?id=CVE-2021-23839>

<https://www.cve.org/CVERecord?id=CVE-2021-23840>

<https://www.cve.org/CVERecord?id=CVE-2021-23841>

<https://www.openssl.org/news/secadv/20210216.txt>

Solution

Upgrade to OpenSSL version 1.0.2y or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0085

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-23839
CVE	CVE-2021-23840
CVE	CVE-2021-23841
XREF	IAVA:2021-A-0103-S
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/02/19, Modified: 2024/10/23

Plugin Output

tcp/80/www

```
Banner          : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
Fixed version    : 1.0.2y
```

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant

Synopsis

The remote host is not FIPS-140 compliant.

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Solution

Change RDP encryption level to :

4. FIPS Compliant

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2008/02/11, Modified: 2024/07/17

Plugin Output

tcp/3389/msrdp

```
The terminal services encryption level is set to :  
2. Medium (Client Compatible)
```

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/www

```
URL      : http://10.12.0.203/
Version  : 2.4.38
Source   : Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
backported : 0
modules  : OpenSSL/1.0.2q PHP/5.6.40
os       : Win64
```

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: 2024/11/12

Plugin Output

tcp/0

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

```
cpe:/o:microsoft:windows_server_2012:r2 -> Microsoft Windows Server 2012
```

```
Following application CPE's matched on the remote system :
```

```
cpe:/a:apache:http_server:2.4.38 -> Apache Software Foundation Apache HTTP Server
```

```
cpe:/a:openssl:openssl:1.0.2q -> OpenSSL Project OpenSSL
```

```
cpe:/a:php:php:5.6.40 -> PHP PHP
```

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 : unknown  
Confidence level : 56
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
00:50:56:A1:76:BE : VMware, Inc.
```


86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 00:50:56:A1:76:BE
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/80/www

```
The remote web server type is :  
Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
```

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 is 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: 2024/02/26

Plugin Output

tcp/80/www

Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : yes

Options allowed : (Not implemented)

Headers :

Date: Mon, 18 Nov 2024 06:16:46 GMT

Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40

X-Powered-By: PHP/5.6.40

Location: http://10.12.0.203/dashboard/

Content-Length: 0

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html; charset=UTF-8

Response Body :

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: 2024/05/20

Plugin Output

tcp/53/dns

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

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: 2024/05/20

Plugin Output

tcp/80/www

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

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: 2024/05/20

Plugin Output

tcp/3389/msrdp

```
Port 3389/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: 2024/10/04

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202411171908
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 10.12.0.25
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 124.035 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/11/17 17:10 CST
Scan duration : 606 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: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2012 R2
Confidence level : 56
Method : MLSinFP
```

Not all fingerprints could give a match. If you think that these signatures would help us improve OS fingerprinting, please submit them by visiting <https://www.tenable.com/research/submitsignatures>.

```
HTTP::Server: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
```

```
SSLcert::i/CN:Mercury.csec388.depaulseclabs.com/CN:Mercury.csec388.depaulseclabs.com
d5fe33c5833ee3f4a4848d38af05427929e75c82
```

```
SinFP:::
P1:B11113:F0x12:W8192:00204ffff:M1460:
P2:B11113:F0x12:W8192:00204ffff010303080402080affffff44454144:M1460:
P3:B00000:F0x00:W0:00:M0
P4:191003_7_p=80
```

The remote host is running Microsoft Windows Server 2012 R2

57323 - OpenSSL Version Detection

Synopsis

Nessus was able to detect the OpenSSL version.

Description

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

See Also

<https://www.openssl.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0682

Plugin Information

Published: 2011/12/16, Modified: 2024/11/14

Plugin Output

tcp/80/www

```
Source      : Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Reported version : 1.0.2q
```

Synopsis

The remote host is missing several patches.

Description

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

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/11/12

Plugin Output

tcp/0

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

[ Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows) (210450) ]
+ Action to take : Upgrade to Apache version 2.4.62 or later.
+Impact : Taking this action will resolve 63 different vulnerabilities (CVEs).

[ OpenSSL 1.0.2 < 1.0.2zl Vulnerability (209152) ]
+ Action to take : Upgrade to OpenSSL version 1.0.2zl or later.
+Impact : Taking this action will resolve 27 different vulnerabilities (CVEs).
```

Synopsis

It is possible to take a screenshot of the remote login screen.

Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.

While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/22, Modified: 2024/07/17

Plugin Output

tcp/3389/msrdp

```
It was possible to gather the following screenshot of the remote login screen.
```

10940 - Remote Desktop Protocol Service Detection

Synopsis

The remote host has an remote desktop protocol service enabled.

Description

The Remote Desktop Protocol allows a user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable the service if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2023/08/21

Plugin Output

tcp/3389/msrdp

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/3389/msrdp

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

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: Mercury.csec388.depaulseclabs.com

Issuer Name:

Common Name: Mercury.csec388.depaulseclabs.com

Serial Number: 4D 9A 7F 1E D8 77 08 92 42 31 B7 6A B1 18 F0 C2

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Nov 17 03:56:10 2024 GMT
Not Valid After: May 19 03:56:10 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 98 2A B7 18 B3 48 AD 28 96 9A CF 63 90 FB D0 C9 99 02 DC
             FF 11 98 9F 36 6E DF 8A EF F8 7D 90 38 2B 85 96 B7 11 36 27
             5A BB 4A E7 45 BD 1A EC 78 81 EB B3 98 7C B7 00 44 9B B8 EE
             94 2E 67 D5 37 E1 99 A7 48 FA 04 64 F4 BE A0 6B 1B 36 12 D0
             CB 80 A3 DC C7 21 D9 C5 68 A9 CA CE B0 35 ED FC 16 36 D6 43
             3F 49 BA 9B 66 9C AC 2E 8B 07 D5 36 1E F9 F0 70 5F C0 7F C7
             56 FE 90 2A CB FF 96 F6 81 58 76 72 16 B7 5D AB C3 4B 57 F5
             B6 BC EE 63 2F B2 CB B5 7A 0F D5 B3 D1 87 BF FD 63 C8 E4 4B
             79 80 44 61 F1 AD 03 F3 2A 78 79 4C 30 52 27 DA 59 72 1E D2
             C6 12 1E F5 0D 49 F4 42 56 19 0A 5F A1 0E 5D 9D 1C 75 32 72
             C4 22 57 49 8D 66 90 C0 9B A2 EE EE 4B 06 E8 AA 47 46 69 A9
```

```

        67 E6 54 9B 73 AA 35 0E 5C 9A BC 2E 7B BC 94 ED 80 6F 1D 45
        7A 6B CE 54 A1 C9 ED EA 96 F4 5D 4D 8E D2 0E 3E 95
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 7D 28 A4 4B 70 6D EF 11 04 9E 6F 45 B1 86 AB ED F7 EB 1B
           6D F6 84 6B 7A 1B 08 40 1A 9B 91 DF 79 E1 51 95 8E DD C2 75
           4B C6 3A 43 C2 F9 A2 C9 8E BD 05 62 3C 70 48 BF 01 20 C2 28
           6C 2E 2B 98 C9 72 6D CC CC 6A 05 C6 B5 2A 97 F0 C1 68 DA E3
           A6 95 DA 97 07 DB 5F 24 F8 46 A6 EA EB 32 6D 32 86 F7 D1 4F
           5A B1 60 BA 38 FB E3 16 B7 DD EA C8 42 31 B8 CF 21 EB 59 60
           C3 B4 4B 3D E7 AE BD 6E F3 37 62 C5 12 0E CF AB C8 A3 27 2C
           D3 9E 34 D1 D8 47 08 98 01 6C E1 B0 E1 B6 34 42 EE 92 B2 BC
           C0 E7 E6 59 BA 84 B8 CE BC F9 BE C5 30 B7 B2 10 6B BC 37 [...]
```


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/3389/msrdp

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

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

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	

SHA1

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC (128)	
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				
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?e17ffcd>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/3389/msrdp

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

SSL Version : TLSv12

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

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	

SHA1

High Strength Ciphers (>= 112-bit key)

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

SHA1

RC4-MD5	0x00, 0x04	RSA	RSA	RC4 (128)	MD5
RC4-SHA	0x00, 0x05	RSA	RSA	RC4 (128)	
SHA1					
ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC (128)	
SHA256					
RSA-AES128-SHA256	0x00, 0x3C	RSA	RSA	AES-CBC (128)	
SHA256					
RSA-AES256-SHA256	0x00, 0x3D	RSA	RSA	AES-CBC (256)	
SHA256					

SSL Version : TLSv11

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	
[...]					

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/3389/msrdp

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					
ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)	
SHA256					

The fields above are :

{Tenable ciphername}
{Cipher ID code}

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

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

```
This port supports resuming TLSv1 / TLSv1 / TLSv1 sessions.
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

- 0x13,0x01 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

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 recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/3389/msrdp

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

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	---
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	
SHA1					

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					
RC4-MD5	0x00, 0x04	RSA	RSA	RC4(128)	MD5
RC4-SHA	0x00, 0x05	RSA	RSA	RC4(128)	
SHA1					
ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)	
SHA256					
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: 2024/03/26

Plugin Output

tcp/80/www

```
A web 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: 2023/10/17

Plugin Output

tcp/0

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

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

See Also

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

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

Solution

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

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/3389/msrdp

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

64814 - Terminal Services Use SSL/TLS

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/22, Modified: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: Mercury.csec388.depaulseclabs.com

Issuer Name:

Common Name: Mercury.csec388.depaulseclabs.com

Serial Number: 4D 9A 7F 1E D8 77 08 92 42 31 B7 6A B1 18 F0 C2

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Nov 17 03:56:10 2024 GMT
Not Valid After: May 19 03:56:10 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 98 2A B7 18 B3 48 AD 28 96 9A CF 63 90 FB D0 C9 99 02 DC
             FF 11 98 9F 36 6E DF 8A EF F8 7D 90 38 2B 85 96 B7 11 36 27
             5A BB 4A E7 45 BD 1A EC 78 81 EB B3 98 7C B7 00 44 9B B8 EE
             94 2E 67 D5 37 E1 99 A7 48 FA 04 64 F4 BE A0 6B 1B 36 12 D0
             CB 80 A3 DC C7 21 D9 C5 68 A9 CA CE B0 35 ED FC 16 36 D6 43
             3F 49 BA 9B 66 9C AC 2E 8B 07 D5 36 1E F9 F0 70 5F C0 7F C7
             56 FE 90 2A CB FF 96 F6 81 58 76 72 16 B7 5D AB C3 4B 57 F5
             B6 BC EE 63 2F B2 CB B5 7A 0F D5 B3 D1 87 BF FD 63 C8 E4 4B
             79 80 44 61 F1 AD 03 F3 2A 78 79 4C 30 52 27 DA 59 72 1E D2
             C6 12 1E F5 0D 49 F4 42 56 19 0A 5F A1 0E 5D 9D 1C 75 32 72
             C4 22 57 49 8D 66 90 C0 9B A2 EE EE 4B 06 E8 AA 47 46 69 A9
```

```

        67 E6 54 9B 73 AA 35 0E 5C 9A BC 2E 7B BC 94 ED 80 6F 1D 45
        7A 6B CE 54 A1 C9 ED EA 96 F4 5D 4D 8E D2 0E 3E 95
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 7D 28 A4 4B 70 6D EF 11 04 9E 6F 45 B1 86 AB ED F7 EB 1B
           6D F6 84 6B 7A 1B 08 40 1A 9B 91 DF 79 E1 51 95 8E DD C2 75
           4B C6 3A 43 C2 F9 A2 C9 8E BD 05 62 3C 70 48 BF 01 20 C2 28
           6C 2E 2B 98 C9 72 6D CC CC 6A 05 C6 B5 2A 97 F0 C1 68 DA E3
           A6 95 DA 97 07 DB 5F 24 F8 46 A6 EA EB 32 6D 32 86 F7 D1 4F
           5A B1 60 BA 38 FB E3 16 B7 DD EA C8 42 31 B8 CF 21 EB 59 60
           C3 B4 4B 3D E7 AE BD 6E F3 37 62 C5 12 0E CF AB C8 A3 27 2C
           D3 9E 34 D1 D8 47 08 98 01 6C E1 B0 E1 B6 34 42 EE 92 B2 BC
           C0 E7 E6 59 BA 84 B8 CE BC F9 BE C5 30 B7 B2 10 6B BC 37 [...]
```

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: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.12.0.25 to 10.12.0.203 :  
10.12.0.25  
10.12.0.203  
  
Hop Count: 1
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```


Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

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

Remediations

Suggested Remediations

Taking the following actions across 2 hosts would resolve 74% of the vulnerabilities on the network.

ACTION TO TAKE	VULNS	HOSTS
Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows): Upgrade to Apache version 2.4.62 or later.	63	1
OpenSSL 1.0.2 < 1.0.2zl Vulnerability: Upgrade to OpenSSL version 1.0.2zl or later.	27	1
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check): Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.	2	1