kioptrix1_scan

Report generated by Nessus™ Mon, 23 Dec 2019 17:49:36 CET

TABLE OF CONTENTS

Vulnerabilities by Host

Remediations

Vulnerabilities by Host

192.168.10.105

CRITICAL	HIGH	MEDIUM	LOW	INFO
5	38	59	11	58

Scan Information

Start time: Mon Dec 23 17:44:17 2019
End time: Mon Dec 23 17:49:36 2019

Host Information

Netbios Name: KIOPTRIX
IP: 192.168.10.105
MAC Address: 08:00:27:12:48:07
OS: Linux Kernel 2.4

Vulnerabilities

10883 - OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation

Synopsis

Arbitrary code may be run on the remote host.

Description

You are running a version of OpenSSH which is older than 3.1.

Versions prior than 3.1 are vulnerable to an off by one error that allows local users to gain root access, and it may be possible for remote users to similarly compromise the daemon for remote access.

In addition, a vulnerable SSH client may be compromised by connecting to a malicious SSH daemon that exploits this vulnerability in the client code, thus compromising the client system.

Solution

Upgrade to OpenSSH 3.1 or apply the patch for prior versions. (See: http://www.openssh.org)

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	4241
CVE	CVE-2002-0083
XREF	CWE:189

Exploitable With

Core Impact (true)

Plugin Information

Published: 2002/03/07, Modified: 2018/07/16

Plugin Output

tcp/22

11031 - OpenSSH < 3.4 Multiple Remote Overflows

Synopsis

The remote host has an application that is affected multiple vulnerabilities.

Description

According to its banner, the remote host appears to be running OpenSSH version 3.4 or older. Such versions are reportedly affected by multiple flaws. An attacker may exploit these vulnerabilities to gain a shell on the remote system.

Note that several distributions patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :

rpm -q openssh-server Returns :

openssh-server-3.1p1-6

See Also

http://www.openssh.com/txt/preauth.adv

Solution

Upgrade to OpenSSH 3.4 or contact your vendor for a patch.

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	5093
CVE	CVE-2002-0639
CVE	CVE-2002-0640

Plugin Information

Published: 2002/06/25, Modified: 2018/07/16

Plugin Output

tcp/22

11837 - OpenSSH < 3.7.1 Multiple Vulnerabilities

Synopsis

The remote SSH service is affected by various memory bugs.

Description

According to its banner, the remote SSH server is running a version of OpenSSH older than 3.7.1. Such versions are vulnerable to a flaw in the buffer management functions that might allow an attacker to execute arbitrary commands on this host.

An exploit for this issue is rumored to exist.

Note that several distributions patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :

rpm -q openssh-server

returns :

openssh-server-3.1p1-13 (RedHat 7.x) openssh-server-3.4p1-7 (RedHat 8.0) openssh-server-3.5p1-11 (RedHat 9)

See Also

https://marc.info/?l=openbsd-misc&m=106375452423794&w=2

https://marc.info/?l=openbsd-misc&m=106375456923804&w=2

Solution

Upgrade to OpenSSH 3.7.1 or later.

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	8628

CVE	CVE-2003-0682
CVE	CVE-2003-0693
CVE	CVE-2003-0695
CVE	CVE-2004-2760
XREF	RHSA:2003:279
XREF	SuSE:SUSE-SA:2003:039
XREF	CWE:16

Plugin Information

Published: 2003/09/16, Modified: 2018/11/15

Plugin Output

tcp/22

78555 - OpenSSL Unsupported

Synopsis

An unsupported service is running on the remote host.

Description

According to its banner, the remote web server is running a version of OpenSSL that is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

https://www.openssl.org/policies/releasestrat.html

http://www.nessus.org/u?4d55548d

Solution

Upgrade to a version of OpenSSL that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information

Published: 2014/10/17, Modified: 2017/01/12

Plugin Output

tcp/80

```
Installed version  : 0.9.6b
Supported versions : 1.1.0 / 1.0.2
EOL URL            : https://www.openssl.org/policies/releasestrat.html
```

78555 - OpenSSL Unsupported

Synopsis

An unsupported service is running on the remote host.

Description

According to its banner, the remote web server is running a version of OpenSSL that is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

https://www.openssl.org/policies/releasestrat.html

http://www.nessus.org/u?4d55548d

Solution

Upgrade to a version of OpenSSL that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information

Published: 2014/10/17, Modified: 2017/01/12

Plugin Output

tcp/443

```
Installed version  : 0.9.6b
Supported versions : 1.1.0 / 1.0.2
EOL URL            : https://www.openssl.org/policies/releasestrat.html
```

11137 - Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The remote host is running a version of Apache web server prior to 1.3.27. It is, therefore, affected by multiple vulnerabilities :

- There is a cross-site scripting vulnerability caused by a failure to filter HTTP/1.1 'Host' headers that are sent by browsers.

- A vulnerability in the handling of the Apache scorecard could allow an attacker to cause a denial of service.

- A buffer overflow vulnerability exists in the 'support/ab.c' read_connection() function. The ab.c file is a benchmarking support utility that is provided with the Apache web server.

See Also

https://seclists.org/bugtraq/2002/Oct/199

http://www.nessus.org/u?767573c2

https://seclists.org/bugtraq/2002/Nov/163

http://www.nessus.org/u?e06ce83b

Solution

Upgrade to Apache web server version 1.3.27 or later.

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)

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	5847
BID	5884
BID	5887
BID	5995
BID	5996
CVE	CVE-2002-0839
CVE	CVE-2002-0840
CVE	CVE-2002-0843
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2002/10/04, Modified: 2018/11/15

Plugin Output

tcp/80

```
Version source    : Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version     : 1.3.27
```

11137 - Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The remote host is running a version of Apache web server prior to 1.3.27. It is, therefore, affected by multiple vulnerabilities :

- There is a cross-site scripting vulnerability caused by a failure to filter HTTP/1.1 'Host' headers that are sent by browsers.

- A vulnerability in the handling of the Apache scorecard could allow an attacker to cause a denial of service.

- A buffer overflow vulnerability exists in the 'support/ab.c' read_connection() function. The ab.c file is a benchmarking support utility that is provided with the Apache web server.

See Also

https://seclists.org/bugtraq/2002/Oct/199

http://www.nessus.org/u?767573c2

https://seclists.org/bugtraq/2002/Nov/163

http://www.nessus.org/u?e06ce83b

Solution

Upgrade to Apache web server version 1.3.27 or later.

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)

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	5847
BID	5884
BID	5887
BID	5995
BID	5996
CVE	CVE-2002-0839
CVE	CVE-2002-0840
CVE	CVE-2002-0843
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2002/10/04, Modified: 2018/11/15

Plugin Output

tcp/443

```
Version source    : Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version     : 1.3.27
```

11793 - Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The remote host appears to be running a version of Apache which is older than 1.3.28

There are several flaws in this version, including a denial of service in redirect handling, a denial of service with control character handling in the 'rotatelogs' utility and a file descriptor leak in third-party module handling.

*** Note that Nessus solely relied on the version number

*** of the remote server to issue this warning. This might

*** be a false positive

See Also

http://www.apache.org/dist/httpd/Announcement.html

Solution

Upgrade to version 1.3.28

Risk Factor

High

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)

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	8226

CVE CVE-2003-0460

Plugin Information

Published: 2003/07/18, Modified: 2018/06/29

Plugin Output

tcp/80

```
Version source    : Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version     : 1.3.28
```

11793 - Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The remote host appears to be running a version of Apache which is older than 1.3.28

There are several flaws in this version, including a denial of service in redirect handling, a denial of service with control character handling in the 'rotatelogs' utility and a file descriptor leak in third-party module handling.

*** Note that Nessus solely relied on the version number

*** of the remote server to issue this warning. This might

*** be a false positive

See Also

http://www.apache.org/dist/httpd/Announcement.html

Solution

Upgrade to version 1.3.28

Risk Factor

High

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)

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	8226

CVE CVE-2003-0460

Plugin Information

Published: 2003/07/18, Modified: 2018/06/29

Plugin Output

tcp/443

```
Version source    : Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version     : 1.3.28
```

11915 - Apache < 1.3.29 Multiple Modules Local Overflow

Synopsis

The remote web server is affected by multiple local buffer overflow vulnerabilities.

Description

The remote host appears to be running a version of the Apache web server which is older than 1.3.29. Such versions are reportedly affected by local buffer overflow vulnerabilities in the mod_alias and mod_rewrite modules. An attacker could exploit these vulnerabilities to execute arbitrary code in the context of the affected application.

*** Note that Nessus solely relied on the version number

*** of the remote server to issue this warning. This might

*** be a false positive

See Also

https://www.securityfocus.com/archive/1/342674/30/0/threaded

Solution

Upgrade to Apache web server version 1.3.29 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)

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	8911

CVE	CVE-2003-0542
XREF	Secunia:10096
XREF	Secunia:10845
XREF	Secunia:17311
XREF	CWE:119

Plugin Information

Published: 2003/11/01, Modified: 2018/11/15

Plugin Output

tcp/80

```
Version source    : Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version     : 1.3.29
```

11915 - Apache < 1.3.29 Multiple Modules Local Overflow

Synopsis

The remote web server is affected by multiple local buffer overflow vulnerabilities.

Description

The remote host appears to be running a version of the Apache web server which is older than 1.3.29. Such versions are reportedly affected by local buffer overflow vulnerabilities in the mod_alias and mod_rewrite modules. An attacker could exploit these vulnerabilities to execute arbitrary code in the context of the affected application.

*** Note that Nessus solely relied on the version number

*** of the remote server to issue this warning. This might

*** be a false positive

See Also

https://www.securityfocus.com/archive/1/342674/30/0/threaded

Solution

Upgrade to Apache web server version 1.3.29 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)

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	8911

CVE	CVE-2003-0542
XREF	Secunia:10096
XREF	Secunia:10845
XREF	Secunia:17311
XREF	CWE:119

Plugin Information

Published: 2003/11/01, Modified: 2018/11/15

Plugin Output

tcp/443

```
Version source    : Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version     : 1.3.29
```

31654 - Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow

Synopsis

The remote version of Apache is vulnerable to an off-by-one buffer overflow attack.

Description

The remote host appears to be running a version of Apache which is older than 1.3.37.

This version contains an off-by-one buffer overflow in the mod_rewrite module.

See Also

https://seclists.org/fulldisclosure/2006/Jul/671

https://www.securityfocus.com/archive//443870

Solution

Upgrade to version 1.3.37 or later.

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)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	19204
CVE	CVE-2006-3747
XREF	EDB-ID:3680
XREF	CWE:189

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2008/03/26, Modified: 2018/11/15

Plugin Output

tcp/80

```
Version source    : Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version     : 1.3.37
```

31654 - Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow

Synopsis

The remote version of Apache is vulnerable to an off-by-one buffer overflow attack.

Description

The remote host appears to be running a version of Apache which is older than 1.3.37.

This version contains an off-by-one buffer overflow in the mod_rewrite module.

See Also

https://seclists.org/fulldisclosure/2006/Jul/671

https://www.securityfocus.com/archive//443870

Solution

Upgrade to version 1.3.37 or later.

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)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	19204
CVE	CVE-2006-3747
XREF	EDB-ID:3680
XREF	CWE:189

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2008/03/26, Modified: 2018/11/15

Plugin Output

tcp/443

```
Version source    : Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version     : 1.3.37
```

11030 - Apache Chunked Encoding Remote Overflow

Synopsis

The remote web server is vulnerable to a remote code execution attack.

Description

The remote Apache web server is affected by the Apache web server chunk handling vulnerability.

If safe checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched Apache versions 1.2.2 and above, 1.3 through 1.3.24, and 2.0 through 2.0.36 are affected, the remote server may be running a patched version of Apache.

See Also

http://httpd.apache.org/info/security_bulletin_20020617.txt

http://httpd.apache.org/info/security_bulletin_20020620.txt

Solution

Upgrade to Apache web server version 1.3.26 / 2.0.39 or later.

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)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	5033
CVE	CVE-2002-0392

Exploitable With

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

Plugin Information

Published: 2002/06/17, Modified: 2018/06/29

Plugin Output

tcp/80

11030 - Apache Chunked Encoding Remote Overflow

Synopsis

The remote web server is vulnerable to a remote code execution attack.

Description

The remote Apache web server is affected by the Apache web server chunk handling vulnerability.

If safe checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched Apache versions 1.2.2 and above, 1.3 through 1.3.24, and 2.0 through 2.0.36 are affected, the remote server may be running a patched version of Apache.

See Also

http://httpd.apache.org/info/security_bulletin_20020617.txt

http://httpd.apache.org/info/security_bulletin_20020620.txt

Solution

Upgrade to Apache web server version 1.3.26 / 2.0.39 or later.

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)

CVSS v3.0 Temporal Score

6.8 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	5033
CVE	CVE-2002-0392

Exploitable With

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

Plugin Information

Published: 2002/06/17, Modified: 2018/06/29

Plugin Output

tcp/443

13651 - Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String

Synopsis

The remote web server is using a module that is affected by a remote code execution vulnerability.

Description

The remote host is using a version vulnerable of mod_ssl which is older than 2.8.19. There is a format string condition in the log functions of the remote module which may allow an attacker to execute arbitrary code on the remote host.

*** Some vendors patched older versions of mod_ssl, so this

*** might be a false positive. Check with your vendor to determine

*** if you have a version of mod_ssl that is patched for this

*** vulnerability

See Also

http://marc.info/?l=apache-modssl&m=109001100906749&w=2

https://marc.info/?l=bugtraq&m=109005001205991&w=2

Solution

Upgrade to mod_ssl version 2.8.19 or newer

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	10736
CVE	CVE-2004-0700

Plugin Information

Published: 2004/07/16, Modified: 2018/11/15

Plugin Output

tcp/80

13651 - Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String

Synopsis

The remote web server is using a module that is affected by a remote code execution vulnerability.

Description

The remote host is using a version vulnerable of mod_ssl which is older than 2.8.19. There is a format string condition in the log functions of the remote module which may allow an attacker to execute arbitrary code on the remote host.

*** Some vendors patched older versions of mod_ssl, so this

*** might be a false positive. Check with your vendor to determine

*** if you have a version of mod_ssl that is patched for this

*** vulnerability

See Also

http://marc.info/?l=apache-modssl&m=109001100906749&w=2

https://marc.info/?l=bugtraq&m=109005001205991&w=2

Solution

Upgrade to mod_ssl version 2.8.19 or newer

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	10736
CVE	CVE-2004-0700

Plugin Information

Published: 2004/07/16, Modified: 2018/11/15

Plugin Output

tcp/443

10771 - OpenSSH 2.5.x - 2.9 Multiple Vulnerabilities

Synopsis

The remote version of OpenSSH contains multiple vulnerabilities.

Description

According to its banner, the remote host appears to be running OpenSSH version between 2.5.x and 2.9. Such versions reportedly contain multiple vulnerabilities :

- sftp-server does not respect the 'command=' argument of keys in the authorized_keys2 file. (CVE-2001-0816)

- sshd does not properly handle the 'from=' argument of keys in the authorized_keys2 file. If a key of one type (e.g. RSA) is followed by a key of another type (e.g. DSA) then the options for the latter will be applied to the former, including 'from=' restrictions. This problem allows users to circumvent the system policy and login from disallowed source IP addresses. (CVE-2001-1380)

See Also

http://www.openbsd.org/advisories/ssh_option.txt

http://www.nessus.org/u?759da6a7

http://www.openssh.com/txt/release-2.9.9

Solution

Upgrade to OpenSSH 2.9.9

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	3345
BID	3369
CVE	CVE-2001-0816
CVE	CVE-2001-1380
XREF	CERT:905795

Plugin Information

Published: 2001/09/28, Modified: 2018/11/15

Plugin Output

tcp/22

```
Version source    : SSH-1.99-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version     : 2.9.9
```

10823 - OpenSSH < 3.0.2 Multiple Vulnerabilities

Synopsis

The SSH service running on the remote host has multiple vulnerabilities.

Description

You are running a version of OpenSSH which is older than 3.0.2.

Versions prior than 3.0.2 have the following vulnerabilities :

- When the UseLogin feature is enabled, a local user could export environment variables, resulting in command execution as root. The UseLogin feature is disabled by default. (CVE-2001-0872)

- A local information disclosure vulnerability.

Only FreeBSD hosts are affected by this issue.

(CVE-2001-1029)

See Also

https://seclists.org/bugtraq/2001/Sep/208

https://www.freebsd.org/releases/4.4R/errata.html

http://www.nessus.org/u?f85ed76c

Solution

Upgrade to OpenSSH 3.0.2 or apply the patch for prior versions. (Available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH)

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	3614
CVE	CVE-2001-0872
CVE	CVE-2001-1029

Plugin Information

Published: 2001/12/10, Modified: 2018/11/15

Plugin Output

tcp/22

44072 - OpenSSH < 3.2.3 YP Netgroups Authentication Bypass

Synopsis

The remote SSH server has an authentication bypass vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is older than 3.2.3. It therefore may be affected by an authentication bypass issue. On systems using YP with netgroups, sshd authenticates users via ACL by checking for the requested username and password. Under certain conditions when doing ACL checks, it may instead use the password entry of a different user for authentication. This means unauthorized users could authenticate successfully, and authorized users could be locked out.

See Also

http://monkey.org/openbsd/archive/bugs/0205/msg00141.html

https://www.openssh.com/txt/release-3.2.3

http://www.openbsd.org/errata31.html#sshbsdauth

Solution

Upgrade to OpenSSH 3.2.3 or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	4803
CVE	CVE-2002-0765

Plugin Information

Published: 2011/10/04, Modified: 2018/11/15

Plugin Output

tcp/22

```
Version source    : SSH-1.99-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version     : 3.2.3
```

17702 - OpenSSH < 3.6.1p2 Multiple Vulnerabilities

Synopsis

The SSH server running on the remote host is affected by multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH running on the remote host is ealier than 3.6.1p2. When compiled for the AIX operating system with a compiler other than that of the native AIX compiler, an error exists that can allow dynamic libraries in the current directory to be loaded before dynamic libraries in the system paths. This behavior can allow local users to escalate privileges by creating, loading and executing their own malicious replacement libraries.

See Also

https://www.openssh.com/txt/release-3.6.1p2

https://www.securityfocus.com/archive/1/320038/2003-04-25/2003-05-01/0

Solution

Upgrade to OpenSSH 3.6.1p2 or later.

Risk Factor

High

CVSS Base Score

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

References

CVE CVE-2002-0746

Plugin Information

Published: 2011/11/18, Modified: 2018/11/15

Plugin Output

tcp/22

```
Version source    : SSH-1.99-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version     : 3.6.1p2
```

11712 - OpenSSH < 3.6.2 Reverse DNS Lookup Bypass

Synopsis

The remote host has an application that is affected by DNS lookup bypass vulnerability.

Description

According to its banner, the remote host appears to be running OpenSSH-portable version 3.6.1 or older.

There is a flaw in such version that could allow an attacker to bypass the access controls set by the administrator of this server.

OpenSSH features a mechanism that can restrict the list of hosts a given user can log from by specifying a pattern in the user key file (ie: *.mynetwork.com would let a user connect only from the local network).

However there is a flaw in the way OpenSSH does reverse DNS lookups.

If an attacker configures a DNS server to send a numeric IP address when a reverse lookup is performed, this mechanism could be circumvented.

Solution

Upgrade to OpenSSH 3.6.2 or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	7831
CVE	CVE-2003-0386
XREF	CERT:978316

Plugin Information

Published: 2003/06/10, Modified: 2018/07/16

Plugin Output

tcp/22

44077 - OpenSSH < 4.5 Multiple Vulnerabilities

Synopsis

The remote SSH service is affected by multiple vulnerabilities.

Description

According to its banner, the remote host is running a version of OpenSSH prior to 4.5. Versions before 4.5 are affected by the following vulnerabilities :

- A client-side NULL pointer dereference, caused by a protocol error from a malicious server, which could cause the client to crash. (CVE-2006-4925)

- A privilege separation vulnerability exists, which could allow attackers to bypass authentication. The vulnerability is caused by a design error between privileged processes and their child processes. Note that this particular issue is only exploitable when other vulnerabilities are present. (CVE-2006-5794)

- An attacker that connects to the service before it has finished creating keys could force the keys to be recreated. This could result in a denial of service for any processes that relies on a trust relationship with the server. Note that this particular issue only affects the Apple implementation of OpenSSH on Mac OS X. (CVE-2007-0726)

See Also

https://www.openssh.com/txt/release-4.5

https://support.apple.com/kb/TA24626?locale=en_US

https://www.openssh.com/security.html

Solution

Upgrade to OpenSSH 4.5 or later.

For Mac OS X 10.3, apply Security Update 2007-003.

For Mac OS X 10.4, upgrade to 10.4.9.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	20956
CVE	CVE-2006-4925
CVE	CVE-2006-5794
CVE	CVE-2007-0726

Plugin Information

Published: 2011/10/04, Modified: 2018/11/15

Plugin Output

tcp/22

```
Version source    : SSH-1.99-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version     : 4.5
```

44078 - OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass

Synopsis

Remote attackers may be able to bypass authentication.

Description

According to the banner, OpenSSH earlier than 4.7 is running on the remote host. Such versions contain an authentication bypass vulnerability. In the event that OpenSSH cannot create an untrusted cookie for X, for example due to the temporary partition being full, it will use a trusted cookie instead. This allows attackers to violate intended policy and gain privileges by causing their X client to be treated as trusted.

See Also

http://www.openssh.com/txt/release-4.7

Solution

Upgrade to OpenSSH 4.7 or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	25628
CVE	CVE-2007-4752
CVE	CVE-2007-2243
XREF	CWE:20
XREF	CWE:287

Plugin Information

Published: 2011/10/04, Modified: 2018/07/16

Plugin Output

tcp/22

```
Version source    : SSH-1.99-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version     : 4.7
```

10954 - OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow

Synopsis

Arbitrary code may be run on the remote host.

Description

You are running a version of OpenSSH older than OpenSSH 3.2.1.

A buffer overflow exists in the daemon if AFS is enabled on your system, or if the options KerberosTgtPassing or AFSTokenPassing are enabled. Even in this scenario, the vulnerability may be avoided by enabling UsePrivilegeSeparation.

Versions prior to 2.9.9 are vulnerable to a remote root exploit. Versions prior to 3.2.1 are vulnerable to a local root exploit.

Solution

Upgrade to version 3.2.1 or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	4560
CVE	CVE-2002-0575

Plugin Information

Published: 2002/05/12, Modified: 2018/07/16

Plugin Output

tcp/22

17751 - OpenSSL 0.9.6 CA Basic Constraints Validation Vulnerability

Synopsis

The remote server is affected by a certificate validation vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7.

Such versions do not verify the Basic Constraint for some certificates. A remote attacker could perform a man-in-the-middle attack.

Details on this weakness are missing. It is related to CVE-2002-0970. OpenSSL 0.9.6 was reported as 'probably' vulnerable.

See Also

http://www.nessus.org/u?8e41b7c3

Solution

Upgrade to OpenSSL 0.9.7 or later.

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2009-0653
XREF	CWE:287

Plugin Information

Published: 2012/01/04, Modified: 2018/08/13

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.7
```

17751 - OpenSSL 0.9.6 CA Basic Constraints Validation Vulnerability

Synopsis

The remote server is affected by a certificate validation vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7.

Such versions do not verify the Basic Constraint for some certificates. A remote attacker could perform a man-in-the-middle attack.

Details on this weakness are missing. It is related to CVE-2002-0970. OpenSSL 0.9.6 was reported as 'probably' vulnerable.

See Also

http://www.nessus.org/u?8e41b7c3

Solution

Upgrade to OpenSSL 0.9.7 or later.

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-2009-0653
XREF	CWE:287

Plugin Information

Published: 2012/01/04, Modified: 2018/08/13

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.7
```

17746 - OpenSSL < 0.9.6e Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple SSL-related vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6e. Such versions have the following vulnerabilities :

- On 64 bit architectures, these versions are vulnerable to a buffer overflow that leads to a denial of service. (CVE-2002-0655)

- Buffer overflows allow a remote attacker to execute arbitrary code. (CVE-2002-0656)

- A remote attacker can trigger a denial of service by sending invalid ASN.1 data. (CVE-2002-0659)

Solution

Upgrade to OpenSSL 0.9.6e or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	5362
BID	5363
BID	5364
BID	5366
CVE	CVE-2002-0655
CVE	CVE-2002-0656
CVE	CVE-2002-0659
XREF	CERT-CC:CA-2002-23
XREF	CERT:102795
XREF	CERT:308891

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2012/01/04, Modified: 2018/07/16

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.6e
```

17746 - OpenSSL < 0.9.6e Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple SSL-related vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6e. Such versions have the following vulnerabilities :

- On 64 bit architectures, these versions are vulnerable to a buffer overflow that leads to a denial of service. (CVE-2002-0655)

- Buffer overflows allow a remote attacker to execute arbitrary code. (CVE-2002-0656)

- A remote attacker can trigger a denial of service by sending invalid ASN.1 data. (CVE-2002-0659)

Solution

Upgrade to OpenSSL 0.9.6e or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	5362
BID	5363
BID	5364
BID	5366
CVE	CVE-2002-0655
CVE	CVE-2002-0656
CVE	CVE-2002-0659
XREF	CERT-CC:CA-2002-23
XREF	CERT:102795
XREF	CERT:308891

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2012/01/04, Modified: 2018/07/16

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.6e
```

17752 - OpenSSL < 0.9.7-beta3 Buffer Overflow

Synopsis

The remote server is affected by an arbitrary code execution vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7-beta3.

If Kerberos is enabled, a remote attacker could trigger a buffer overflow with a long master key and execute arbitrary code.

Solution

Upgrade to OpenSSL 0.9.7 or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	5361
CVE	CVE-2002-0657
XREF	CERT-CC:CA-2002-23
XREF	CERT:561275

Plugin Information

Published: 2012/01/04, Modified: 2018/07/16

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.7-beta3
```

17752 - OpenSSL < 0.9.7-beta3 Buffer Overflow

Synopsis

The remote server is affected by an arbitrary code execution vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7-beta3.

If Kerberos is enabled, a remote attacker could trigger a buffer overflow with a long master key and execute arbitrary code.

Solution

Upgrade to OpenSSL 0.9.7 or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	5361
CVE	CVE-2002-0657
XREF	CERT-CC:CA-2002-23
XREF	CERT:561275

Plugin Information

Published: 2012/01/04, Modified: 2018/07/16

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.7-beta3
```

17760 - OpenSSL < 0.9.8f Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8f. As such, it is affected by the following vulnerabilities :

- A local attacker could perform a side-channel attack against the Montgomery multiplication code and retrieve RSA private keys. Note that this has not been exploited outside a laboratory environment. (CVE-2007-3108)

- A remote attacker could execute arbitrary code by exploiting an off-by-one error in the DTLS implementation. (CVE-2007-4995)

See Also

http://web.archive.org/web/20071014185140/http://cvs.openssl.org:80/chngview?cn=16275

http://www.nessus.org/u?cbc3fb3e

http://www.kb.cert.org/vuls/id/RGII-74KLP3

https://www.openssl.org/news/secadv/20071012.txt

Solution

Upgrade to OpenSSL 0.9.8f or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	25163
BID	26055
CVE	CVE-2007-3108
CVE	CVE-2007-4995
XREF	CERT:724968
XREF	CWE:189

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8f
```

17760 - OpenSSL < 0.9.8f Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8f. As such, it is affected by the following vulnerabilities :

- A local attacker could perform a side-channel attack against the Montgomery multiplication code and retrieve RSA private keys. Note that this has not been exploited outside a laboratory environment. (CVE-2007-3108)

- A remote attacker could execute arbitrary code by exploiting an off-by-one error in the DTLS implementation. (CVE-2007-4995)

See Also

http://web.archive.org/web/20071014185140/http://cvs.openssl.org:80/chngview?cn=16275

http://www.nessus.org/u?cbc3fb3e

http://www.kb.cert.org/vuls/id/RGII-74KLP3

https://www.openssl.org/news/secadv/20071012.txt

Solution

Upgrade to OpenSSL 0.9.8f or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	25163
BID	26055
CVE	CVE-2007-3108
CVE	CVE-2007-4995
XREF	CERT:724968
XREF	CWE:189

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8f
```

57459 - OpenSSL < 0.9.8s Multiple Vulnerabilities

Synopsis

The remote web server has multiple SSL-related vulnerabilities.

Description

According to its banner, the remote web server is running a version of OpenSSL older than 0.9.8s. Such versions have the following vulnerabilities :

- An error exists related to ECDSA signatures and binary curves. The implementation of curves over binary fields could allow a remote, unauthenticated attacker to determine private key material via timing attacks.

(CVE-2011-1945)

- The Datagram Transport Layer Security (DTLS) implementation is vulnerable to plaintext recovery attacks when decrypting in CBC mode. (CVE-2011-4108)

- A double-free error exists during a policy check failure if the flag 'X509_V_FLAG_POLICY_CHECK' is set.

(CVE-2011-4109)

- An error exists related to SSLv3.0 records that can lead to disclosure of uninitialized memory because the library does not clear all bytes used as block cipher padding. (CVE-2011-4576)

- An error exists related to RFC 3779 processing that can allow denial of service attacks. Note that this functionality is not enabled by default and must be configured at compile time via the 'enable-rfc3779'

option. (CVE-2011-4577)

- An error exists related to handshake restarts for server gated cryptography (SGC) that can allow denial of service attacks. (CVE-2011-4619)

See Also

https://www.openssl.org/news/secadv/20120104.txt

https://www.openssl.org/news/changelog.html

http://www.nessus.org/u?c0f10f36

https://eprint.iacr.org/2011/232.pdf

http://cvs.openssl.org/chngview?cn=21301

Solution

Upgrade to OpenSSL 0.9.8s or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	51281
BID	47888
CVE	CVE-2011-1945
CVE	CVE-2011-4108
CVE	CVE-2011-4109
CVE	CVE-2011-4576
CVE	CVE-2011-4577
CVE	CVE-2011-4619
XREF	CERT:536044

Plugin Information

Published: 2012/01/09, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8s
```

57459 - OpenSSL < 0.9.8s Multiple Vulnerabilities

Synopsis

The remote web server has multiple SSL-related vulnerabilities.

Description

According to its banner, the remote web server is running a version of OpenSSL older than 0.9.8s. Such versions have the following vulnerabilities :

- An error exists related to ECDSA signatures and binary curves. The implementation of curves over binary fields could allow a remote, unauthenticated attacker to determine private key material via timing attacks.

(CVE-2011-1945)

- The Datagram Transport Layer Security (DTLS) implementation is vulnerable to plaintext recovery attacks when decrypting in CBC mode. (CVE-2011-4108)

- A double-free error exists during a policy check failure if the flag 'X509_V_FLAG_POLICY_CHECK' is set.

(CVE-2011-4109)

- An error exists related to SSLv3.0 records that can lead to disclosure of uninitialized memory because the library does not clear all bytes used as block cipher padding. (CVE-2011-4576)

- An error exists related to RFC 3779 processing that can allow denial of service attacks. Note that this functionality is not enabled by default and must be configured at compile time via the 'enable-rfc3779'

option. (CVE-2011-4577)

- An error exists related to handshake restarts for server gated cryptography (SGC) that can allow denial of service attacks. (CVE-2011-4619)

See Also

https://www.openssl.org/news/secadv/20120104.txt

https://www.openssl.org/news/changelog.html

http://www.nessus.org/u?c0f10f36

https://eprint.iacr.org/2011/232.pdf

http://cvs.openssl.org/chngview?cn=21301

Solution

Upgrade to OpenSSL 0.9.8s or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	51281
BID	47888
CVE	CVE-2011-1945
CVE	CVE-2011-4108
CVE	CVE-2011-4109
CVE	CVE-2011-4576
CVE	CVE-2011-4577
CVE	CVE-2011-4619
XREF	CERT:536044

Plugin Information

Published: 2012/01/09, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8s
```

58799 - OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption

Synopsis

The remote host may be affected by a memory corruption vulnerability.

Description

According to its banner, the remote web server is running a version of OpenSSL earlier than 0.9.8w. As such, the OpenSSL library itself is reportedly affected by a memory corruption vulnerability via an integer truncation error in the function 'asn1_d2i_read_bio' when reading ASN.1 DER format data.

Applications using the 'BIO' or 'FILE' based functions (i.e., 'd2i_*_bio' or 'd2i_*_fp' functions) are affected by this issue.

Also affected are 'S/MIME' or 'CMS' applications using 'SMIME_read_PKCS7' or 'SMIME_read_CMS' parsers. The OpenSSL command line utility is affected if used to handle untrusted DER formatted data.

Note that the SSL/TLS code of OpenSSL is not affected. Also not affected are applications using memory-based ASN.1 functions (e.g., 'd2i_X509', 'd2i_PKCS12', etc.) nor are applications using only PEM functions.

Note also that the original fix for CVE-2012-2110 in 0.9.8v was incomplete because the functions 'BUF_MEM_grow' and 'BUF_MEM_grow_clean', in file 'openssl/crypto/buffer/buffer.c', did not properly account for negative values of the argument 'len'.

See Also

https://www.openssl.org/news/secadv/20120419.txt

http://seclists.org/fulldisclosure/2012/Apr/210

https://www.openssl.org/news/secadv/20120424.txt

http://cvs.openssl.org/chngview?cn=22479

https://www.openssl.org/news/changelog.html

Solution

Upgrade to OpenSSL 0.9.8w or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	53158
BID	53212
CVE	CVE-2012-2110
CVE	CVE-2012-2131
XREF	EDB-ID:18756

Plugin Information

Published: 2012/04/24, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8w
```

58799 - OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption

Synopsis

The remote host may be affected by a memory corruption vulnerability.

Description

According to its banner, the remote web server is running a version of OpenSSL earlier than 0.9.8w. As such, the OpenSSL library itself is reportedly affected by a memory corruption vulnerability via an integer truncation error in the function 'asn1_d2i_read_bio' when reading ASN.1 DER format data.

Applications using the 'BIO' or 'FILE' based functions (i.e., 'd2i_*_bio' or 'd2i_*_fp' functions) are affected by this issue.

Also affected are 'S/MIME' or 'CMS' applications using 'SMIME_read_PKCS7' or 'SMIME_read_CMS' parsers. The OpenSSL command line utility is affected if used to handle untrusted DER formatted data.

Note that the SSL/TLS code of OpenSSL is not affected. Also not affected are applications using memory-based ASN.1 functions (e.g., 'd2i_X509', 'd2i_PKCS12', etc.) nor are applications using only PEM functions.

Note also that the original fix for CVE-2012-2110 in 0.9.8v was incomplete because the functions 'BUF_MEM_grow' and 'BUF_MEM_grow_clean', in file 'openssl/crypto/buffer/buffer.c', did not properly account for negative values of the argument 'len'.

See Also

https://www.openssl.org/news/secadv/20120419.txt

http://seclists.org/fulldisclosure/2012/Apr/210

https://www.openssl.org/news/secadv/20120424.txt

http://cvs.openssl.org/chngview?cn=22479

https://www.openssl.org/news/changelog.html

Solution

Upgrade to OpenSSL 0.9.8w or later.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	53158
BID	53212
CVE	CVE-2012-2110
CVE	CVE-2012-2131
XREF	EDB-ID:18756

Plugin Information

Published: 2012/04/24, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8w
```

10882 - SSH Protocol Version 1 Session Key Retrieval

Synopsis

The remote service offers an insecure cryptographic protocol.

Description

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Solution

Disable compatibility with version 1 of the protocol.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	2344
CVE	CVE-2001-0361
CVE	CVE-2001-0572
CVE	CVE-2001-1473
XREF	CWE:310

Plugin Information

Published: 2002/03/06, Modified: 2018/09/17

Plugin Output

tcp/22

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

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 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2019/03/27

Plugin Output

tcp/443

```
- SSLv2 is enabled and the server supports at least one cipher.

  Low Strength Ciphers (<= 64-bit key)

    DES-CBC-MD5                 Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=MD5
    EXP-RC2-CBC-MD5             Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
 export
    EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
 export
    RC4-64-MD5                  Kx=RSA         Au=RSA      Enc=RC4(64)              Mac=MD5

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

    DES-CBC3-MD5                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=MD5

  High Strength Ciphers (>= 112-bit key)

    RC2-CBC-MD5                 Kx=RSA         Au=RSA      Enc=RC2-CBC(128)         Mac=MD5
    RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}

- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Low Strength Ciphers (<= 64-bit key)

    EXP-EDH-RSA-DES-CBC-SHA     Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
    EDH-RSA-DES-CBC-SHA         Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
    EXP1024-DES-CBC-SHA         Kx=RSA(1024)   Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
 export
    EXP1024-RC2-CBC-MD5         Kx=RSA(1024)   Au=RSA      Enc=RC2-CBC(56)          Mac=MD5
 export
    EXP1024-RC4-MD5             Kx=RSA(1024)   Au=RSA      Enc=RC4(56)              Mac=MD5
 export
    EXP1024-RC4-SHA             Kx=RSA(1024)   Au=RSA      Enc=RC4(56)              Mac=SHA1
 export
    EXP-DES-CBC-SHA             Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
```

```
    EXP-RC2-CBC-MD5             [...]
```

34460 - Unsupported Web Server Detection

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information

Published: 2008/10/21, Modified: 2018/06/29

Plugin Output

tcp/80

```
Product                : Apache 1.x
Server response header : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Supported versions     : Apache HTTP Server 2.4.x
Additional information : http://archive.apache.org/dist/httpd/Announcement1.3.html
```

34460 - Unsupported Web Server Detection

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information

Published: 2008/10/21, Modified: 2018/06/29

Plugin Output

tcp/443

```
Product                : Apache 1.x
Server response header : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Supported versions     : Apache HTTP Server 2.4.x
Additional information : http://archive.apache.org/dist/httpd/Announcement1.3.html
```

12255 - mod_ssl ssl_util_uuencode_binary Remote Overflow

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote host is using a version of mod_ssl that is older than 2.8.18.

This version is vulnerable to a flaw that could allow an attacker to disable the remote website remotely, or to execute arbitrary code on the remote host.

Note that several Linux distributions patched the old version of this module. Therefore, this alert might be a false-positive. Please check with your vendor to determine if you really are vulnerable to this flaw.

Solution

Upgrade to version 2.8.18 (Apache 1.3) or to Apache 2.0.50.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	10355
CVE	CVE-2004-0488

Plugin Information

Published: 2004/05/29, Modified: 2018/07/14

Plugin Output

tcp/80

12255 - mod_ssl ssl_util_uuencode_binary Remote Overflow

Synopsis

Arbitrary code can be executed on the remote host.

Description

The remote host is using a version of mod_ssl that is older than 2.8.18.

This version is vulnerable to a flaw that could allow an attacker to disable the remote website remotely, or to execute arbitrary code on the remote host.

Note that several Linux distributions patched the old version of this module. Therefore, this alert might be a false-positive. Please check with your vendor to determine if you really are vulnerable to this flaw.

Solution

Upgrade to version 2.8.18 (Apache 1.3) or to Apache 2.0.50.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	10355
CVE	CVE-2004-0488

Plugin Information

Published: 2004/05/29, Modified: 2018/07/14

Plugin Output

tcp/443

17696 - Apache HTTP Server 403 Error Page UTF-7 Encoded XSS

Synopsis

The web server running on the remote host has a cross-site scripting vulnerability.

Description

According to its banner, the version of Apache HTTP Server running on the remote host can be used in cross-site scripting (XSS) attacks. Making a specially crafted request can inject UTF-7 encoded script code into a 403 response page, resulting in XSS attacks.

This is actually a web browser vulnerability that occurs due to non-compliance with RFC 2616 (refer to BID 29112). Apache HTTP Server is not vulnerable, but its default configuration can trigger the non-compliant, exploitable behavior in vulnerable browsers.

See Also

https://seclists.org/bugtraq/2008/May/109

https://seclists.org/bugtraq/2008/May/166

Solution

Upgrade to Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 or later. These versions use a default configuration setting that prevents exploitation in vulnerable web browsers.

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 v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	29112

CVE	CVE-2008-2168
XREF	CWE:79

Plugin Information

Published: 2011/11/18, Modified: 2018/11/15

Plugin Output

tcp/80

```
Version source    : Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version     : 1.3.41
```

17696 - Apache HTTP Server 403 Error Page UTF-7 Encoded XSS

Synopsis

The web server running on the remote host has a cross-site scripting vulnerability.

Description

According to its banner, the version of Apache HTTP Server running on the remote host can be used in cross-site scripting (XSS) attacks. Making a specially crafted request can inject UTF-7 encoded script code into a 403 response page, resulting in XSS attacks.

This is actually a web browser vulnerability that occurs due to non-compliance with RFC 2616 (refer to BID 29112). Apache HTTP Server is not vulnerable, but its default configuration can trigger the non-compliant, exploitable behavior in vulnerable browsers.

See Also

https://seclists.org/bugtraq/2008/May/109

https://seclists.org/bugtraq/2008/May/166

Solution

Upgrade to Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 or later. These versions use a default configuration setting that prevents exploitation in vulnerable web browsers.

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 v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	29112

CVE	CVE-2008-2168
XREF	CWE:79

Plugin Information

Published: 2011/11/18, Modified: 2018/11/15

Plugin Output

tcp/443

```
Version source    : Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Installed version : 1.3.20
Fixed version     : 1.3.41
```

88098 - Apache Server ETag Header Information Disclosure

Synopsis

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

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	6939
CVE	CVE-2003-1418
XREF	CWE:200

Plugin Information

Published: 2016/01/22, Modified: 2019/11/19

Plugin Output

tcp/80

```
Nessus was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                 : ETag: "8805-b4a-3b96e9ae"
  Inode number           : 34821
  File size              : 2890 bytes
  File modification time : Sep.  6, 2001 at 03:12:46 GMT
```

88098 - Apache Server ETag Header Information Disclosure

Synopsis

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

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	6939
CVE	CVE-2003-1418
XREF	CWE:200

Plugin Information

Published: 2016/01/22, Modified: 2019/11/19

Plugin Output

tcp/443

```
Nessus was able to determine that the Apache Server listening on
port 443 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                 : ETag: "8805-b4a-3b96e9ae"
  Inode number           : 34821
  File size              : 2890 bytes
  File modification time : Sep.  6, 2001 at 03:12:46 GMT
```

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

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these 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)

CVSS Base Score

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

CVSS 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: 2019/03/27

Plugin Output

tcp/80

```
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 :

------------------------------ snip ------------------------------
TRACE /Nessus1258332008.html HTTP/1.1
Connection: Close
Host: 192.168.10.105
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 ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Mon, 23 Dec 2019 21:45:40 GMT
Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1258332008.html HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: iso-8859-1,*,utf-8
Accept-Language: en
Connection: Close
Host: 192.168.10.105
Pragma: no-cache
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)

------------------------------ snip ------------------------------
```

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

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these 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)

CVSS Base Score

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

CVSS 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: 2019/03/27

Plugin Output

tcp/443

```
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 :

------------------------------ snip ------------------------------
TRACE /Nessus1872639425.html HTTP/1.1
Connection: Close
Host: 192.168.10.105
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 ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Mon, 23 Dec 2019 21:45:40 GMT
Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1872639425.html HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: iso-8859-1,*,utf-8
Accept-Language: en
Connection: Close
Host: 192.168.10.105
Pragma: no-cache
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)

------------------------------ snip ------------------------------
```

44076 - OpenSSH < 4.3 scp Command Line Filename Processing Command Injection

Synopsis

The version of SSH running on the remote host has a command injection vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is potentially affected by an arbitrary command execution vulnerability. The scp utility does not properly sanitize user-supplied input prior to using a system() function call. A local attacker could exploit this by creating filenames with shell metacharacters, which could cause arbitrary code to be executed if copied by a user running scp.

See Also

https://bugzilla.mindrot.org/show_bug.cgi?id=1094

http://www.openssh.com/txt/release-4.3

Solution

Upgrade to OpenSSH 4.3 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	16369
CVE	CVE-2006-0225

Plugin Information

Published: 2011/10/04, Modified: 2018/07/16

Plugin Output

tcp/22

```
  Version source    : SSH-1.99-OpenSSH_2.9p2
  Installed version : 2.9p2
  Fixed version     : 4.3
```

10802 - OpenSSH < 3.0.1 Multiple Flaws

Synopsis

The remote host has an application that is affected by multiple vulnerabilities.

Description

According to its banner, the remote host appears to be running OpenSSH version 3.0.1 or older. Such versions are reportedly affected by multiple flaws :

- Provided KerberosV is enabled (disabled by default), it may be possible for an attacker to partially authenticate.

- It may be possible to crash the daemon due to a excessive memory clearing bug.

See Also

https://seclists.org/bugtraq/2001/Nov/152

Solution

Upgrade to OpenSSH 3.0.1 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	3560
CVE	CVE-2001-1507

Plugin Information

Published: 2001/11/20, Modified: 2018/11/15

Plugin Output

tcp/22

44079 - OpenSSH < 4.9 'ForceCommand' Directive Bypass

Synopsis

The remote SSH service is affected by a security bypass vulnerability.

Description

According to its banner, the version of OpenSSH installed on the remote host is earlier than 4.9. It may allow a remote, authenticated user to bypass the 'sshd_config' 'ForceCommand' directive by modifying the '.ssh/rc' session file.

See Also

https://www.openssh.com/txt/release-4.9

Solution

Upgrade to OpenSSH version 4.9 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	28531
CVE	CVE-2008-1657
XREF	CWE:264

Plugin Information

Published: 2011/10/04, Modified: 2018/11/15

Plugin Output

tcp/22

```
Version source    : SSH-1.99-OpenSSH_2.9p2
```

```
    Installed version : 2.9p2
    Fixed version     : 4.9
```

44065 - OpenSSH < 5.2 CBC Plaintext Disclosure

Synopsis

The SSH service running on the remote host has an information disclosure vulnerability.

Description

The version of OpenSSH running on the remote host has an information disclosure vulnerability. A design flaw in the SSH specification could allow a man-in-the-middle attacker to recover up to 32 bits of plaintext from an SSH-protected connection in the standard configuration. An attacker could exploit this to gain access to sensitive information.

See Also

http://www.nessus.org/u?4984aeb9

http://www.openssh.com/txt/cbc.adv

http://www.openssh.com/txt/release-5.2

Solution

Upgrade to OpenSSH 5.2 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

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

Plugin Information

Published: 2011/09/27, Modified: 2018/07/16

Plugin Output

tcp/22

```
  Version source    : SSH-1.99-OpenSSH_2.9p2
  Installed version : 2.9p2
  Fixed version     : 5.2
```

44073 - OpenSSH With OpenPAM DoS

Synopsis

The SSH server running on the remote host has a denial of service vulnerability.

Description

According to its banner, the version of OpenSSH running on the remote host is affected by a remote denial of service vulnerability. When used with OpenPAM, OpenSSH does not properly handle when a forked child process ends during PAM authentication. This could allow a remote attacker to cause a denial of service by connecting several times to the SSH server, waiting for the password prompt and then disconnecting.

See Also

https://bugzilla.mindrot.org/show_bug.cgi?id=839

http://www.nessus.org/u?170f19e3

Solution

Upgrade to OpenSSH 3.8.1p1 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	16892
CVE	CVE-2006-0883

Plugin Information

Published: 2011/10/04, Modified: 2018/07/16

Plugin Output

tcp/22

```
  Version source    : SSH-1.99-OpenSSH_2.9p2
  Installed version : 2.9p2
  Fixed version     : 3.8.1p1
```

31737 - OpenSSH X11 Forwarding Session Hijacking

Synopsis

The remote SSH service is prone to an X11 session hijacking vulnerability.

Description

According to its banner, the version of SSH installed on the remote host is older than 5.0. Such versions may allow a local user to hijack X11 sessions because it improperly binds TCP ports on the local IPv6 interface if the corresponding ports on the IPv4 interface are in use.

See Also

https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011

https://www.openssh.com/txt/release-5.0

Solution

Upgrade to OpenSSH version 5.0 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	28444
CVE	CVE-2008-1483
CVE	CVE-2008-3234
XREF	Secunia:29522
XREF	CWE:264

Plugin Information

Published: 2008/04/03, Modified: 2018/11/15

Plugin Output

tcp/22

```
The remote OpenSSH server returned the following banner :

SSH-1.99-OpenSSH_2.9p2
```

59076 - OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service

Synopsis

The remote host may be affected by a denial of service vulnerability.

Description

According to its banner, the remote web server is running a version of OpenSSL 0.9.8 earlier than 0.9.8x. As such, the OpenSSL library itself is reportedly affected by a denial of service vulnerability.

An integer underflow error exists in the file 'ssl/d1_enc.c' in the function 'dtls1_enc'. When in CBC mode, DTLS record length values and explicit initialization vector length values related to DTLS packets are not handled properly, which can lead to memory corruption and application crashes.

See Also

https://www.openssl.org/news/secadv/20120510.txt

https://www.openssl.org/news/changelog.html

http://cvs.openssl.org/chngview?cn=22538

https://bugzilla.redhat.com/show_bug.cgi?id=820686

Solution

Upgrade to OpenSSL 0.9.8x or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	53476
CVE	CVE-2012-2333

Plugin Information

Published: 2012/05/11, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8x
```

59076 - OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service

Synopsis

The remote host may be affected by a denial of service vulnerability.

Description

According to its banner, the remote web server is running a version of OpenSSL 0.9.8 earlier than 0.9.8x. As such, the OpenSSL library itself is reportedly affected by a denial of service vulnerability.

An integer underflow error exists in the file 'ssl/d1_enc.c' in the function 'dtls1_enc'. When in CBC mode, DTLS record length values and explicit initialization vector length values related to DTLS packets are not handled properly, which can lead to memory corruption and application crashes.

See Also

https://www.openssl.org/news/secadv/20120510.txt

https://www.openssl.org/news/changelog.html

http://cvs.openssl.org/chngview?cn=22538

https://bugzilla.redhat.com/show_bug.cgi?id=820686

Solution

Upgrade to OpenSSL 0.9.8x or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	53476
CVE	CVE-2012-2333

Plugin Information

Published: 2012/05/11, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8x
```

17747 - OpenSSL < 0.9.6f Denial of Service

Synopsis

The remote server is vulnerable to a denial of service attack.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6f.

A remote attacker can trigger a denial of service by sending a specially crafted SSLv2 CLIENT_MASTER_KEY message.

See Also

http://cvs.openssl.org/chngview?cn=7659

https://www.securityfocus.com/archive/1/339948

Solution

Upgrade to OpenSSL 0.9.6f or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	8746
CVE	CVE-2002-1568
XREF	RHSA:2003:291

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.6f
```

17747 - OpenSSL < 0.9.6f Denial of Service

Synopsis

The remote server is vulnerable to a denial of service attack.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6f.

A remote attacker can trigger a denial of service by sending a specially crafted SSLv2 CLIENT_MASTER_KEY message.

See Also

http://cvs.openssl.org/chngview?cn=7659

https://www.securityfocus.com/archive/1/339948

Solution

Upgrade to OpenSSL 0.9.6f or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	8746
CVE	CVE-2002-1568
XREF	RHSA:2003:291

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.6f
```

11267 - OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities

Synopsis

The remote host has an application that is affected by multiple vulnerabilities.

Description

According to its banner, the remote host is using a version of OpenSSL older than 0.9.6j or 0.9.7b.

This version is vulnerable to a timing-based attack that could allow an attacker to guess the content of fixed data blocks and may eventually be able to guess the value of the private RSA key of the server.

An attacker may use this implementation flaw to sniff the data going to this host and decrypt some parts of it, as well as impersonate the server and perform man-in-the-middle attacks.

See Also

https://www.openssl.org/news/secadv/20030219.txt

http://eprint.iacr.org/2003/052/

Solution

Upgrade to version 0.9.6j (0.9.7b) or newer.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	6884
BID	7148
CVE	CVE-2003-0078
CVE	CVE-2003-0131
CVE	CVE-2003-0147
XREF	RHSA:2003:101-01
XREF	SuSE:SUSE-SA:2003:024

Plugin Information

Published: 2003/02/20, Modified: 2018/07/16

Plugin Output

tcp/80

11267 - OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities

Synopsis

The remote host has an application that is affected by multiple vulnerabilities.

Description

According to its banner, the remote host is using a version of OpenSSL older than 0.9.6j or 0.9.7b.

This version is vulnerable to a timing-based attack that could allow an attacker to guess the content of fixed data blocks and may eventually be able to guess the value of the private RSA key of the server.

An attacker may use this implementation flaw to sniff the data going to this host and decrypt some parts of it, as well as impersonate the server and perform man-in-the-middle attacks.

See Also

https://www.openssl.org/news/secadv/20030219.txt

http://eprint.iacr.org/2003/052/

Solution

Upgrade to version 0.9.6j (0.9.7b) or newer.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	6884
BID	7148
CVE	CVE-2003-0078
CVE	CVE-2003-0131
CVE	CVE-2003-0147
XREF	RHSA:2003:101-01
XREF	SuSE:SUSE-SA:2003:024

Plugin Information

Published: 2003/02/20, Modified: 2018/07/16

Plugin Output

tcp/443

17748 - OpenSSL < 0.9.6k Denial of Service

Synopsis

The remote server is vulnerable to a denial of service attack.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6k.

A remote attacker can trigger a denial of service by using an invalid client certificate.

Solution

Upgrade to OpenSSL 0.9.6k or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	8732
CVE	CVE-2003-0543
CVE	CVE-2003-0544
XREF	CERT-CC:CA-2003-26
XREF	CERT:255484
XREF	CERT:380864

Plugin Information

Published: 2012/01/04, Modified: 2018/07/16

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
```

```
    Fixed version    : 0.9.6k
```

17748 - OpenSSL < 0.9.6k Denial of Service

Synopsis

The remote server is vulnerable to a denial of service attack.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6k.

A remote attacker can trigger a denial of service by using an invalid client certificate.

Solution

Upgrade to OpenSSL 0.9.6k or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	8732
CVE	CVE-2003-0543
CVE	CVE-2003-0544
XREF	CERT-CC:CA-2003-26
XREF	CERT:255484
XREF	CERT:380864

Plugin Information

Published: 2012/01/04, Modified: 2018/07/16

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
```

```
    Fixed version    : 0.9.6k
```

17749 - OpenSSL < 0.9.6l Denial of Service

Synopsis

The remote server is vulnerable to a denial of service attack.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6l.

A remote attacker can trigger a denial of service by using an invalid client certificate.

See Also

https://www.openssl.org/news/secadv/20031104.txt

https://marc.info/?l=bugtraq&m=106796246511667&w=2

Solution

Upgrade to OpenSSL 0.9.6l or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	8970
CVE	CVE-2003-0851
XREF	CERT:412478

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/80

```
    Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
    Reported version : 0.9.6b
    Fixed version    : 0.9.6l
```

17749 - OpenSSL < 0.9.6l Denial of Service

Synopsis

The remote server is vulnerable to a denial of service attack.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6l.

A remote attacker can trigger a denial of service by using an invalid client certificate.

See Also

https://www.openssl.org/news/secadv/20031104.txt

https://marc.info/?l=bugtraq&m=106796246511667&w=2

Solution

Upgrade to OpenSSL 0.9.6l or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	8970
CVE	CVE-2003-0851
XREF	CERT:412478

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/443

```
    Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
    Reported version : 0.9.6b
    Fixed version    : 0.9.6l
```

17750 - OpenSSL < 0.9.6m / 0.9.7d Denial of Service

Synopsis

The remote server is vulnerable to a denial of service attack.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6m or 0.9.7d.

A remote attacker can crash the server by sending an overly long Kerberos ticket or a crafted SSL/TLS handshake.

See Also

https://www.us-cert.gov/ncas/alerts/ta04-078a

https://www.openssl.org/news/secadv/20040317.txt

http://marc.info/?l=bugtraq&m=107953412903636&w=2

Solution

Upgrade to OpenSSL 0.9.6m / 0.9.7d or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	9899
CVE	CVE-2004-0079
CVE	CVE-2004-0112
XREF	CERT:484726

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.6m
```

17750 - OpenSSL < 0.9.6m / 0.9.7d Denial of Service

Synopsis

The remote server is vulnerable to a denial of service attack.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.6m or 0.9.7d.

A remote attacker can crash the server by sending an overly long Kerberos ticket or a crafted SSL/TLS handshake.

See Also

https://www.us-cert.gov/ncas/alerts/ta04-078a

https://www.openssl.org/news/secadv/20040317.txt

http://marc.info/?l=bugtraq&m=107953412903636&w=2

Solution

Upgrade to OpenSSL 0.9.6m / 0.9.7d or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	9899
CVE	CVE-2004-0079
CVE	CVE-2004-0112
XREF	CERT:484726

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.6m
```

12110 - OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS

Synopsis

The remote service is prone to a denial of service attack.

Description

According to its banner, the remote host is using a version of OpenSSL which is older than 0.9.6m / 0.9.7d. There are several bugs in such versions that may allow an attacker to cause a denial of service against the remote host.

See Also

https://www.openssl.org/news/secadv/20040317.txt

https://seclists.org/bugtraq/2004/Mar/155

Solution

Upgrade to version 0.9.6m / 0.9.7d or newer.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	9899
CVE	CVE-2004-0079
CVE	CVE-2004-0081
CVE	CVE-2004-0112

Plugin Information

Published: 2004/03/17, Modified: 2018/11/15

Plugin Output

tcp/80

12110 - OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS

Synopsis

The remote service is prone to a denial of service attack.

Description

According to its banner, the remote host is using a version of OpenSSL which is older than 0.9.6m / 0.9.7d. There are several bugs in such versions that may allow an attacker to cause a denial of service against the remote host.

See Also

https://www.openssl.org/news/secadv/20040317.txt

https://seclists.org/bugtraq/2004/Mar/155

Solution

Upgrade to version 0.9.6m / 0.9.7d or newer.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	9899
CVE	CVE-2004-0079
CVE	CVE-2004-0081
CVE	CVE-2004-0112

Plugin Information

Published: 2004/03/17, Modified: 2018/11/15

Plugin Output

tcp/443

17759 - OpenSSL < 0.9.8 Weak Default Configuration

Synopsis

The default configuration of OpenSSL on the remote server uses a weak hash algorithm.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8.

The default configuration uses MD5 instead of a stronger hash algorithm. An attacker could forge certificates.

If you never generate certificates on this machine, you may ignore this warning.

See Also

https://bugs.launchpad.net/ubuntu/+source/openssl/+bug/19835

https://usn.ubuntu.com/179-1/

Solution

Upgrade to OpenSSL 0.9.8 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2005-2946
XREF	CWE:310

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8
```

17759 - OpenSSL < 0.9.8 Weak Default Configuration

Synopsis

The default configuration of OpenSSL on the remote server uses a weak hash algorithm.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8.

The default configuration uses MD5 instead of a stronger hash algorithm. An attacker could forge certificates.

If you never generate certificates on this machine, you may ignore this warning.

See Also

https://bugs.launchpad.net/ubuntu/+source/openssl/+bug/19835

https://usn.ubuntu.com/179-1/

Solution

Upgrade to OpenSSL 0.9.8 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2005-2946
XREF	CWE:310

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8
```

56996 - OpenSSL < 0.9.8h Multiple Vulnerabilities

Synopsis

The remote web server has multiple SSL-related vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL older than 0.9.8h. As such, it may be affected by the following vulnerabilities :

- A double-free error exists related to the handling of server name extension data and specially crafted TLS 1.0 'Client Hello' packets. This can cause application crashes. Note that successful exploitation requires that OpenSSL is compiled with the TLS server name extensions.

(CVE-2008-0891)

- A NULL pointer dereference error exists related to anonymous Diffie-Hellman key exchange and TLS handshakes. This can be exploited by omitting the 'Server Key exchange message' from the handshake and can cause application crashes. (CVE-2008-1672)

- On 32-bit builds, an information disclosure vulnerability exists during certain calculations for NIST elliptic curves P-256 or P-384. This error can allow an attacker to recover the private key of the TLS server.

The following are required for exploitation :

- 32-bit build

- Use of elliptic curves P-256 and/or P-384

- Either the use of ECDH family ciphers and/or the use of ECDHE family ciphers without the SSL_OP_SINGLE_ECDH_USE context option

(CVE-2011-4354)

Note that Nessus has not attempted to verify that these issues are actually exploitable or have been patched but instead has relied on the version number found in the Server response header.

See Also

https://www.openwall.com/lists/oss-security/2011/12/01/6

https://www.openssl.org/news/secadv/20080528.txt

Solution

Upgrade to OpenSSL 0.9.8h or later or apply the vendor-supplied patches.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	29405
BID	50882
CVE	CVE-2008-0891
CVE	CVE-2008-1672
CVE	CVE-2011-4354
XREF	CERT:520586
XREF	CERT:661475
XREF	CWE:189
XREF	CWE:287

Plugin Information

Published: 2011/12/02, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8h
```

56996 - OpenSSL < 0.9.8h Multiple Vulnerabilities

Synopsis

The remote web server has multiple SSL-related vulnerabilities.

Description

According to its banner, the remote web server uses a version of OpenSSL older than 0.9.8h. As such, it may be affected by the following vulnerabilities :

- A double-free error exists related to the handling of server name extension data and specially crafted TLS 1.0 'Client Hello' packets. This can cause application crashes. Note that successful exploitation requires that OpenSSL is compiled with the TLS server name extensions.

(CVE-2008-0891)

- A NULL pointer dereference error exists related to anonymous Diffie-Hellman key exchange and TLS handshakes. This can be exploited by omitting the 'Server Key exchange message' from the handshake and can cause application crashes. (CVE-2008-1672)

- On 32-bit builds, an information disclosure vulnerability exists during certain calculations for NIST elliptic curves P-256 or P-384. This error can allow an attacker to recover the private key of the TLS server.

The following are required for exploitation :

- 32-bit build

- Use of elliptic curves P-256 and/or P-384

- Either the use of ECDH family ciphers and/or the use of ECDHE family ciphers without the SSL_OP_SINGLE_ECDH_USE context option

(CVE-2011-4354)

Note that Nessus has not attempted to verify that these issues are actually exploitable or have been patched but instead has relied on the version number found in the Server response header.

See Also

https://www.openwall.com/lists/oss-security/2011/12/01/6

https://www.openssl.org/news/secadv/20080528.txt

Solution

Upgrade to OpenSSL 0.9.8h or later or apply the vendor-supplied patches.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	29405
BID	50882
CVE	CVE-2008-0891
CVE	CVE-2008-1672
CVE	CVE-2011-4354
XREF	CERT:520586
XREF	CERT:661475
XREF	CWE:189
XREF	CWE:287

Plugin Information

Published: 2011/12/02, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8h
```

17761 - OpenSSL < 0.9.8i Denial of Service

Synopsis

The remote server is affected by a denial of service vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8i.

A remote attacker can crash the server by sending a DTLS ChangeCipherSpec packet before the ClientHello.

See Also

http://cvs.openssl.org/chngview?cn=17369

https://rt.openssl.org/Ticket/Display.html?id=1679&user=guest&pass=guest

Solution

Upgrade to OpenSSL 0.9.8i or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

References

BID	35174
CVE	CVE-2009-1386
XREF	EDB-ID:8873

Exploitable With

Core Impact (true)

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8i
```

17761 - OpenSSL < 0.9.8i Denial of Service

Synopsis

The remote server is affected by a denial of service vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8i.

A remote attacker can crash the server by sending a DTLS ChangeCipherSpec packet before the ClientHello.

See Also

http://cvs.openssl.org/chngview?cn=17369

https://rt.openssl.org/Ticket/Display.html?id=1679&user=guest&pass=guest

Solution

Upgrade to OpenSSL 0.9.8i or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.1 (CVSS2#E:F/RL:OF/RC:C)

References

BID	35174
CVE	CVE-2009-1386
XREF	EDB-ID:8873

Exploitable With

Core Impact (true)

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8i
```

17762 - OpenSSL < 0.9.8j Signature Spoofing

Synopsis

The remote server is affected by a signature validation bypass vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8j.

A remote attacker could implement a man-in-the-middle attack by forging an SSL/TLS signature using DSA and ECDSA keys which bypass validation of the certificate chain.

See Also

https://www.us-cert.gov/ncas/alerts/TA09-133A

Solution

Upgrade to OpenSSL 0.9.8j or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	33150
CVE	CVE-2008-5077
XREF	CWE:20

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/80

```
    Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
    Reported version : 0.9.6b
    Fixed version    : 0.9.8j
```

17762 - OpenSSL < 0.9.8j Signature Spoofing

Synopsis

The remote server is affected by a signature validation bypass vulnerability.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8j.

A remote attacker could implement a man-in-the-middle attack by forging an SSL/TLS signature using DSA and ECDSA keys which bypass validation of the certificate chain.

See Also

https://www.us-cert.gov/ncas/alerts/TA09-133A

Solution

Upgrade to OpenSSL 0.9.8j or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	33150
CVE	CVE-2008-5077
XREF	CWE:20

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/443

```
    Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
    Reported version : 0.9.6b
    Fixed version    : 0.9.8j
```

17763 - OpenSSL < 0.9.8k Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL prior to 0.9.8k. It is, therefore, affected by multiple vulnerabilities :

- A denial of service vulnerability exists in the ASN1_STRING_print_ex() function due to improper string handling. A remote attacker can exploit this to cause an invalid memory access and application crash.

(CVE-2009-0590)

- A flaw exists in the CMS_verify() function due to improper handling of errors associated with malformed signed attributes. A remote attacker can exploit this to repudiate a signature that originally appeared to be valid but was actually invalid. (CVE-2009-0591)

- A denial of service vulnerability exists due to improper handling of malformed ASN.1 structures. A remote attacker can exploit this to cause an invalid memory access and application crash. (CVE-2009-0789)

- A memory leak exists in the SSL_free() function in ssl_lib.c. A remote attacker can exploit this to exhaust memory resources, resulting in a denial of service condition. (CVE-2009-5146)

See Also

https://www.openssl.org/news/secadv/20090325.txt

Solution

Upgrade to OpenSSL version 0.9.8k or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	34256
BID	73121
CVE	CVE-2009-0590

CVE	CVE-2009-0591
CVE	CVE-2009-0789
CVE	CVE-2009-5146
XREF	CWE:119
XREF	CWE:189
XREF	CWE:287

Plugin Information

Published: 2012/01/04, Modified: 2018/07/16

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8k
```

17763 - OpenSSL < 0.9.8k Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL prior to 0.9.8k. It is, therefore, affected by multiple vulnerabilities :

- A denial of service vulnerability exists in the ASN1_STRING_print_ex() function due to improper string handling. A remote attacker can exploit this to cause an invalid memory access and application crash.

(CVE-2009-0590)

- A flaw exists in the CMS_verify() function due to improper handling of errors associated with malformed signed attributes. A remote attacker can exploit this to repudiate a signature that originally appeared to be valid but was actually invalid. (CVE-2009-0591)

- A denial of service vulnerability exists due to improper handling of malformed ASN.1 structures. A remote attacker can exploit this to cause an invalid memory access and application crash. (CVE-2009-0789)

- A memory leak exists in the SSL_free() function in ssl_lib.c. A remote attacker can exploit this to exhaust memory resources, resulting in a denial of service condition. (CVE-2009-5146)

See Also

https://www.openssl.org/news/secadv/20090325.txt

Solution

Upgrade to OpenSSL version 0.9.8k or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	34256
BID	73121
CVE	CVE-2009-0590

CVE	CVE-2009-0591
CVE	CVE-2009-0789
CVE	CVE-2009-5146
XREF	CWE:119
XREF	CWE:189
XREF	CWE:287

Plugin Information

Published: 2012/01/04, Modified: 2018/07/16

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8k
```

17765 - OpenSSL < 0.9.8l Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8l. As such, it may be affected by multiple vulnerabilities :

- A remote attacker could crash the server by sending malformed ASN.1 data. This flaw only affects some architectures, Win64 and other unspecified platforms. (CVE-2009-0789)

- A remote attacker could saturate the server by sending a big number of 'future epoch' DTLS records. (CVE-2009-1377)

- A remote attacker could saturate the server by sending duplicate DTLS records, or DTLS records with too big sequence numbers. (CVE-2009-1378)

- A remote attacker could spoof certificates by computing MD2 hash collisions. (CVE-2009-2409)

See Also

http://voodoo-circle.sourceforge.net/sa/sa-20090326-01.html

https://www.openssl.org/news/secadv/20090325.txt

http://voodoo-circle.sourceforge.net/sa/sa-20091012-01.html

https://rt.openssl.org/Ticket/Display.html?id=1930&user=guest&pass=guest

https://rt.openssl.org/Ticket/Display.html?id=1931&user=guest&pass=guest

http://cvs.openssl.org/chngview?cn=18187

http://cvs.openssl.org/chngview?cn=18188

Solution

Upgrade to OpenSSL 0.9.8l or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	34256
BID	35001
CVE	CVE-2009-0789
CVE	CVE-2009-1377
CVE	CVE-2009-1378
CVE	CVE-2009-2409
XREF	EDB-ID:8720
XREF	CWE:119
XREF	CWE:189
XREF	CWE:310
XREF	CWE:399

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8l
```

17765 - OpenSSL < 0.9.8l Multiple Vulnerabilities

Synopsis

The remote server is affected by multiple vulnerabilities.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8l. As such, it may be affected by multiple vulnerabilities :

- A remote attacker could crash the server by sending malformed ASN.1 data. This flaw only affects some architectures, Win64 and other unspecified platforms. (CVE-2009-0789)

- A remote attacker could saturate the server by sending a big number of 'future epoch' DTLS records. (CVE-2009-1377)

- A remote attacker could saturate the server by sending duplicate DTLS records, or DTLS records with too big sequence numbers. (CVE-2009-1378)

- A remote attacker could spoof certificates by computing MD2 hash collisions. (CVE-2009-2409)

See Also

http://voodoo-circle.sourceforge.net/sa/sa-20090326-01.html

https://www.openssl.org/news/secadv/20090325.txt

http://voodoo-circle.sourceforge.net/sa/sa-20091012-01.html

https://rt.openssl.org/Ticket/Display.html?id=1930&user=guest&pass=guest

https://rt.openssl.org/Ticket/Display.html?id=1931&user=guest&pass=guest

http://cvs.openssl.org/chngview?cn=18187

http://cvs.openssl.org/chngview?cn=18188

Solution

Upgrade to OpenSSL 0.9.8l or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	34256
BID	35001
CVE	CVE-2009-0789
CVE	CVE-2009-1377
CVE	CVE-2009-1378
CVE	CVE-2009-2409
XREF	EDB-ID:8720
XREF	CWE:119
XREF	CWE:189
XREF	CWE:310
XREF	CWE:399

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8l
```

58564 - OpenSSL < 0.9.8u Multiple Vulnerabilities

Synopsis

The remote host may be affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses an OpenSSL version prior to 0.9.8u. As such, it is reportedly affected by the following vulnerabilities :

- An error exists in the function 'mime_hdr_cmp' that could allow a NULL pointer to be dereferenced when parsing certain MIME headers. (CVE-2006-7250)

- The fix for CVE-2011-4619 was not complete.

- An error exists in the Cryptographic Message Syntax (CMS) and PKCS #7 implementation such that data can be decrypted using Million Message Attack (MMA) adaptive chosen cipher text attack. (CVE-2012-0884)

- An error exists in the function 'mime_param_cmp' in the file 'crypto/asn1/asn_mime.c' that can allow a NULL pointer to be dereferenced when handling certain S/MIME content. (CVE-2012-1165)

Note that SSL/TLS applications are not necessarily affected, but those using CMS, PKCS #7 and S/MIME decryption operations are.

See Also

https://marc.info/?l=openssl-dev&m=115685408414194&w=2

https://www.openssl.org/news/secadv/20120312.txt

https://www.openssl.org/news/changelog.html

https://www.openwall.com/lists/oss-security/2012/03/13/2

https://www.openwall.com/lists/oss-security/2012/02/28/14

http://www.nessus.org/u?82fc5c0b

https://rt.openssl.org/Ticket/Display.html?id=2711&user=guest&pass=guest

Solution

Upgrade to OpenSSL 0.9.8u or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	51281
BID	52181
BID	52428
BID	52764
CVE	CVE-2006-7250
CVE	CVE-2011-4619
CVE	CVE-2012-0884
CVE	CVE-2012-1165

Plugin Information

Published: 2012/04/02, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8u
```

58564 - OpenSSL < 0.9.8u Multiple Vulnerabilities

Synopsis

The remote host may be affected by multiple vulnerabilities.

Description

According to its banner, the remote web server uses an OpenSSL version prior to 0.9.8u. As such, it is reportedly affected by the following vulnerabilities :

- An error exists in the function 'mime_hdr_cmp' that could allow a NULL pointer to be dereferenced when parsing certain MIME headers. (CVE-2006-7250)

- The fix for CVE-2011-4619 was not complete.

- An error exists in the Cryptographic Message Syntax (CMS) and PKCS #7 implementation such that data can be decrypted using Million Message Attack (MMA) adaptive chosen cipher text attack. (CVE-2012-0884)

- An error exists in the function 'mime_param_cmp' in the file 'crypto/asn1/asn_mime.c' that can allow a NULL pointer to be dereferenced when handling certain S/MIME content. (CVE-2012-1165)

Note that SSL/TLS applications are not necessarily affected, but those using CMS, PKCS #7 and S/MIME decryption operations are.

See Also

https://marc.info/?l=openssl-dev&m=115685408414194&w=2

https://www.openssl.org/news/secadv/20120312.txt

https://www.openssl.org/news/changelog.html

https://www.openwall.com/lists/oss-security/2012/03/13/2

https://www.openwall.com/lists/oss-security/2012/02/28/14

http://www.nessus.org/u?82fc5c0b

https://rt.openssl.org/Ticket/Display.html?id=2711&user=guest&pass=guest

Solution

Upgrade to OpenSSL 0.9.8u or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	51281
BID	52181
BID	52428
BID	52764
CVE	CVE-2006-7250
CVE	CVE-2011-4619
CVE	CVE-2012-0884
CVE	CVE-2012-1165

Plugin Information

Published: 2012/04/02, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8u
```

64532 - OpenSSL < 0.9.8y Multiple Vulnerabilities

Synopsis

The remote host may be affected by multiple vulnerabilities.

Description

According to its banner, the remote web server is running a version of OpenSSL prior to 0.9.8y. The OpenSSL library is, therefore, reportedly affected by the following vulnerabilities :

- An error exists related to the handling of OCSP response verification that could allow denial of service attacks. (CVE-2013-0166)

- An error exists related to the SSL/TLS/DTLS protocols, CBC mode encryption and response time. An attacker could obtain plaintext contents of encrypted traffic via timing attacks. (CVE-2013-0169)

See Also

https://www.openssl.org/news/secadv/20130204.txt

Solution

Upgrade to OpenSSL 0.9.8y or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	57778
BID	60268
CVE	CVE-2013-0166
CVE	CVE-2013-0169

Plugin Information

Published: 2013/02/09, Modified: 2018/07/16

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8y
```

64532 - OpenSSL < 0.9.8y Multiple Vulnerabilities

Synopsis

The remote host may be affected by multiple vulnerabilities.

Description

According to its banner, the remote web server is running a version of OpenSSL prior to 0.9.8y. The OpenSSL library is, therefore, reportedly affected by the following vulnerabilities :

- An error exists related to the handling of OCSP response verification that could allow denial of service attacks. (CVE-2013-0166)

- An error exists related to the SSL/TLS/DTLS protocols, CBC mode encryption and response time. An attacker could obtain plaintext contents of encrypted traffic via timing attacks. (CVE-2013-0169)

See Also

https://www.openssl.org/news/secadv/20130204.txt

Solution

Upgrade to OpenSSL 0.9.8y or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	57778
BID	60268
CVE	CVE-2013-0166
CVE	CVE-2013-0169

Plugin Information

Published: 2013/02/09, Modified: 2018/07/16

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version    : 0.9.8y
```

51892 - OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue

Synopsis

The remote host allows resuming SSL sessions with a weaker cipher than the one originally negotiated.

Description

The version of OpenSSL on the remote host has been shown to allow resuming session with a weaker cipher than was used when the session was initiated. This means that an attacker that sees (i.e., by sniffing) the start of an SSL connection can manipulate the OpenSSL session cache to cause subsequent resumptions of that session to use a weaker cipher chosen by the attacker.

Note that other SSL implementations may also be affected by this vulnerability.

See Also

https://www.openssl.org/news/secadv/20101202.txt

Solution

Upgrade to OpenSSL 0.9.8q / 1.0.0.c or later, or contact your vendor for a patch.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	45164
CVE	CVE-2010-4180

Plugin Information

Published: 2011/02/07, Modified: 2018/07/16

Plugin Output

tcp/443

```
The server allowed the following session over TLSv1 to be resumed as follows :

  Session ID     : 5977072df72fee19399afd8278a006e7303881e0aee7a114b4607a7c0c31acbf
  Initial Cipher : TLS1_CK_RSA_WITH_RC4_128_SHA (0x0005)
  Resumed Cipher : TLS1_CK_RSA_EXPORT1024_WITH_RC4_56_SHA (0x0064)
```

44074 - Portable OpenSSH < 3.8p1 Multiple Vulnerabilities

Synopsis

Remote attackers may be able to cause information to leak from aborted sessions.

Description

According to its banner, a version of OpenSSH earlier than 3.8p1 is running on the remote host and is affected by the following issues:

- There is an issue in the handling of PAM modules in such versions of OpenSSH. As a result, OpenSSH may not correctly handle aborted conversations with PAM modules. Consequently, that memory may not be scrubbed of sensitive information such as credentials, which could lead to credentials leaking into swap space and core dumps. Other vulnerabilities in PAM modules could come to light because of unpredictable behavior.

- Denial of service attacks are possible when privilege separation is in use. This version of OpenSSH does not properly signal non-privileged processes after session termination when 'LoginGraceTime' is exceeded. This can allow connections to remain open thereby allowing the denial of service when resources are exhausted. (CVE-2004-2069)

See Also

https://www.cl.cam.ac.uk/~mgk25/otpw.html#opensshbug

https://bugzilla.mindrot.org/show_bug.cgi?id=632

http://www.nessus.org/u?e86aec66

http://www.nessus.org/u?bbd79dfd

http://www.nessus.org/u?d2f25e5c

Solution

Upgrade to OpenSSH 3.8p1 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	9040

BID	14963
CVE	CVE-2004-2069

Plugin Information

Published: 2011/10/04, Modified: 2018/11/15

Plugin Output

tcp/22

```
Version source    : SSH-1.99-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version     : 3.8p1
```

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

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)

CVSS Base Score

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

CVSS Temporal Score

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

Plugin Information

Published: 2012/01/19, Modified: 2018/11/15

Plugin Output

tcp/139

90317 - SSH Weak Algorithms Supported

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS Base Score

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

Plugin Information

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

Plugin Output

tcp/22

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

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

  arcfour
```

42880 - SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Synopsis

The remote service allows insecure renegotiation of TLS / SSL connections.

Description

The remote service encrypts traffic using TLS / SSL but allows a client to insecurely renegotiate the connection after the initial handshake.

An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.

See Also

http://www.ietf.org/mail-archive/web/tls/current/msg03948.html

http://www.g-sec.lu/practicaltls.pdf

https://tools.ietf.org/html/rfc5746

Solution

Contact the vendor for specific patch information.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	36935
CVE	CVE-2009-3555
XREF	CERT:120541
XREF	CWE:310

Plugin Information

Published: 2009/11/24, Modified: 2018/07/30

Plugin Output

tcp/443

```
TLSv1 supports insecure renegotiation.

SSLv3 supports insecure renegotiation.
```

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 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 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2018/11/15

Plugin Output

tcp/443

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

|-Subject   : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
|-Not After : Sep 26 09:32:06 2010 GMT

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 : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
|-Issuer  : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
```

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

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

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 Base Score

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

Plugin Information

Published: 2004/12/03, Modified: 2019/03/13

Plugin Output

tcp/443

```
The SSL certificate has already expired :

  Subject          : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit,
 CN=localhost.localdomain, emailAddress=root@localhost.localdomain
  Issuer           : C=--, ST=SomeState, L=SomeCity, O=SomeOrganization, OU=SomeOrganizationalUnit,
 CN=localhost.localdomain, emailAddress=root@localhost.localdomain
  Not valid before : Sep 26 09:32:06 2009 GMT
  Not valid after  : Sep 26 09:32:06 2010 GMT
```

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 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)

CVSS Base Score

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

CVSS Temporal Score

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

References

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

Plugin Information

Published: 2009/01/05, Modified: 2019/03/27

Plugin Output

tcp/443

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

|-Subject             : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
|-Signature Algorithm : MD5 With RSA Encryption
|-Valid From          : Sep 26 09:32:06 2009 GMT
|-Valid To            : Sep 26 09:32:06 2010 GMT
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

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 Base Score

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

Plugin Information

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/443

```
The identities known by Nessus are :

  192.168.10.105
  192.168.10.105

The Common Name in the certificate is :

  localhost.localdomain
```

89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

Synopsis

The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.

Description

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.

See Also

https://drownattack.com/

https://drownattack.com/drown-attack-paper.pdf

Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

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)

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	83733

CVE	CVE-2016-0800
XREF	CERT:583776

Plugin Information

Published: 2016/03/01, Modified: 2019/11/20

Plugin Output

tcp/443

```
The remote host is affected by SSL DROWN and supports the following
vulnerable cipher suites :

  Low Strength Ciphers (<= 64-bit key)

    DES-CBC-MD5                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=MD5
    EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
 export
    EXP-RC4-MD5                  Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
 export

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                      Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

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

Description

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

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

See Also

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

https://sweet32.info

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS 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: 2019/02/28

Plugin Output

tcp/443

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

    DES-CBC3-MD5                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=MD5
    EDH-RSA-DES-CBC3-SHA        Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/443

```
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 : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
```

26928 - SSL Weak Cipher Suites Supported

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer weak encryption.

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

See Also

http://www.nessus.org/u?6527892d

Solution

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

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 Base Score

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

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information

Published: 2007/10/08, Modified: 2018/05/16

Plugin Output

tcp/443

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

  Low Strength Ciphers (<= 64-bit key)

    DES-CBC-MD5                 Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=MD5
    EXP-RC2-CBC-MD5             Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
 export
    EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
 export
    RC4-64-MD5                  Kx=RSA         Au=RSA      Enc=RC4(64)              Mac=MD5
    EXP-EDH-RSA-DES-CBC-SHA     Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
    EDH-RSA-DES-CBC-SHA         Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
    EXP1024-DES-CBC-SHA         Kx=RSA(1024)   Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
 export
    EXP1024-RC2-CBC-MD5         Kx=RSA(1024)   Au=RSA      Enc=RC2-CBC(56)          Mac=MD5
 export
    EXP1024-RC4-MD5             Kx=RSA(1024)   Au=RSA      Enc=RC4(56)              Mac=MD5
 export
    EXP1024-RC4-SHA             Kx=RSA(1024)   Au=RSA      Enc=RC4(56)              Mac=SHA1
 export
    EXP-DES-CBC-SHA             Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
    EXP-RC2-CBC-MD5             Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
 export
    EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
 export
    DES-CBC-SHA                 Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

See Also

https://www.smacktls.com/#freak

https://www.openssl.org/news/secadv/20150108.txt

http://www.nessus.org/u?b78da2c4

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	71936
CVE	CVE-2015-0204
XREF	CERT:243585

Plugin Information

Published: 2015/03/04, Modified: 2018/09/17

Plugin Output

tcp/443

```
EXPORT_RSA cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    EXP-DES-CBC-SHA              Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
    EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
 export
    EXP-RC4-MD5                  Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
 export

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2019/11/25

Plugin Output

tcp/443

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

10816 - Webalizer < 2.01-09 Multiple XSS

Synopsis

A web application on the remote host has multiple cross-site scripting vulnerabilities.

Description

Webalizer, a web server log analysis application, was detected on the remote host. This version of Webalizer has multiple cross-site scripting vulnerabilities that could allow malicious HTML tags to be injected in the reports.

See Also

https://seclists.org/bugtraq/2001/Oct/223

Solution

Upgrade to Version 2.01-09 and change the directory in 'OutputDir'.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	3473
CVE	CVE-2001-0835
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751

XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2001/12/03, Modified: 2018/11/15

Plugin Output

tcp/80

10816 - Webalizer < 2.01-09 Multiple XSS

Synopsis

A web application on the remote host has multiple cross-site scripting vulnerabilities.

Description

Webalizer, a web server log analysis application, was detected on the remote host. This version of Webalizer has multiple cross-site scripting vulnerabilities that could allow malicious HTML tags to be injected in the reports.

See Also

https://seclists.org/bugtraq/2001/Oct/223

Solution

Upgrade to Version 2.01-09 and change the directory in 'OutputDir'.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	3473
CVE	CVE-2001-0835
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751

XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2001/12/03, Modified: 2018/11/15

Plugin Output

tcp/443

44075 - OpenSSH < 4.0 known_hosts Plaintext Host Information Disclosure

Synopsis

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

Description

According to its banner, the remote host is running a version of OpenSSH prior to 4.0. Versions of OpenSSH earlier than 4.0 are affected by an information disclosure vulnerability because the application stores hostnames, IP addresses, and keys in plaintext in the 'known_hosts' file. A local attacker, exploiting this flaw, could gain access to sensitive information that could be used in subsequent attacks.

See Also

https://www.openssh.com/txt/release-4.0

http://nms.csail.mit.edu/projects/ssh/

http://www.eweek.com/c/a/Security/Researchers-Reveal-Holes-in-Grid/

Solution

Upgrade to OpenSSH 4.0 or later.

Risk Factor

Low

CVSS Base Score

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

References

CVE	CVE-2005-2666
CVE	CVE-2007-4654
CVE	CVE-2004-2760
XREF	CWE:16
XREF	CWE:255
XREF	CWE:399

Plugin Information

Published: 2011/10/04, Modified: 2018/11/15

Plugin Output

tcp/22

```
Version source    : SSH-1.99-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version     : 4.0
```

19592 - OpenSSH < 4.2 Multiple Vulnerabilities

Synopsis

The remote SSH server has multiple vulnerabilities.

Description

According to its banner, the version of OpenSSH installed on the remote host has the following vulnerabilities :

- X11 forwarding may be enabled unintentionally when multiple forwarding requests are made on the same session, or when an X11 listener is orphaned after a session goes away. (CVE-2005-2797)

- GSSAPI credentials may be delegated to users who log in using something other than GSSAPI authentication if 'GSSAPIDelegateCredentials' is enabled. (CVE-2005-2798)

- Attempting to log in as a nonexistent user causes the authentication process to hang, which could be exploited to enumerate valid user accounts.

Only OpenSSH on Mac OS X 10.4.x is affected.

(CVE-2006-0393)

- Repeatedly attempting to log in as a nonexistent user could result in a denial of service.

Only OpenSSH on Mac OS X 10.4.x is affected.

(CVE-2006-0393)

See Also

http://www.openssh.com/txt/release-4.2

https://lists.apple.com/archives/security-announce/2006/Aug/msg00000.html

https://support.apple.com/?artnum=304063

Solution

Upgrade to OpenSSH 4.2 or later. For OpenSSH on Mac OS X 10.4.x, apply Mac OS X Security Update 2006-004.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	14727
BID	14729
BID	19289
CVE	CVE-2005-2797
CVE	CVE-2005-2798
CVE	CVE-2006-0393

Plugin Information

Published: 2005/09/07, Modified: 2018/11/15

Plugin Output

tcp/22

44080 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking

Synopsis

The remote SSH service may be affected by an X11 forwarding port hijacking vulnerability.

Description

According to its banner, the version of SSH installed on the remote host is older than 5.1 and may allow a local user to hijack the X11 forwarding port. The application improperly sets the 'SO_REUSEADDR'

socket option when the 'X11UseLocalhost' configuration option is disabled.

Note that most operating systems, when attempting to bind to a port that has previously been bound with the 'SO_REUSEADDR' option, will check that either the effective user-id matches the previous bind (common BSD-derived systems) or that the bind addresses do not overlap (Linux and Solaris). This is not the case with other operating systems such as HP-UX.

See Also

https://www.openssh.com/txt/release-5.1

Solution

Upgrade to OpenSSH version 5.1 or later.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	30339
CVE	CVE-2008-3259
XREF	CWE:200

Plugin Information

Published: 2011/10/04, Modified: 2018/11/15

Plugin Output

tcp/22

```
  Version source    : SSH-1.99-OpenSSH_2.9p2
  Installed version : 2.9p2
  Fixed version     : 5.1
```

17754 - OpenSSL < 0.9.7f Insecure Temporary File Creation

Synopsis

Arbitrary files could be overwritten on the remote server.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7f.

The der_chop script that is shipped with these versions allows a malicious user to overwrite arbitrary files.

Note that this was fixed in the 0.9.6 CVS but no new version was published in the 0.9.6 branch.

See Also

https://www.openssl.org/news/vulnerabilities.html#2004-0975

Solution

Upgrade to OpenSSL 0.9.7f or later.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	11293
CVE	CVE-2004-0975

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/80

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
```

```
    Reported version : 0.9.6b
    Fixed version    : 0.9.7f
```

17754 - OpenSSL < 0.9.7f Insecure Temporary File Creation

Synopsis

Arbitrary files could be overwritten on the remote server.

Description

According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.7f.

The der_chop script that is shipped with these versions allows a malicious user to overwrite arbitrary files.

Note that this was fixed in the 0.9.6 CVS but no new version was published in the 0.9.6 branch.

See Also

https://www.openssl.org/news/vulnerabilities.html#2004-0975

Solution

Upgrade to OpenSSL 0.9.7f or later.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	11293
CVE	CVE-2004-0975

Plugin Information

Published: 2012/01/04, Modified: 2018/11/15

Plugin Output

tcp/443

```
Banner           : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
```

```
    Reported version : 0.9.6b
    Fixed version    : 0.9.7f
```

53841 - Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure

Synopsis

Local attackers may be able to access sensitive information.

Description

According to its banner, the version of OpenSSH running on the remote host is earlier than 5.8p2. Such versions may be affected by a local information disclosure vulnerability that could allow the contents of the host's private key to be accessible by locally tracing the execution of the ssh-keysign utility. Having the host's private key may allow the impersonation of the host.

Note that installations are only vulnerable if ssh-rand-helper was enabled during the build process, which is not the case for *BSD, OS X, Cygwin and Linux.

See Also

http://www.openssh.com/txt/portable-keysign-rand-helper.adv

http://www.openssh.com/txt/release-5.8p2

Solution

Upgrade to Portable OpenSSH 5.8p2 or later.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	47691
CVE	CVE-2011-4327
XREF	Secunia:44347

Plugin Information

Published: 2011/05/09, Modified: 2018/07/16

Plugin Output

tcp/22

```
Version source    : SSH-1.99-OpenSSH_2.9p2
Installed version : 2.9p2
Fixed version     : 5.8p2
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

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

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

Solution

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

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

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

Plugin Information

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

Plugin Output

tcp/22

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

```
  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
  rijndael128-cbc
  rijndael192-cbc
  rijndael256-cbc

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

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
  rijndael128-cbc
  rijndael192-cbc
  rijndael256-cbc
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

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

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS Base Score

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

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22

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

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

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

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

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

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

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

2.2 (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: 2019/11/27

Plugin Output

tcp/443

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

  Low Strength Ciphers (<= 64-bit key)

    EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)             Mac=MD5
 export
    RC4-64-MD5                  Kx=RSA         Au=RSA      Enc=RC4(64)             Mac=MD5
    EXP1024-RC4-MD5             Kx=RSA(1024)   Au=RSA      Enc=RC4(56)             Mac=MD5
 export
    EXP1024-RC4-SHA             Kx=RSA(1024)   Au=RSA      Enc=RC4(56)             Mac=SHA1
 export
    EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)             Mac=MD5
 export

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
    RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
    RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

https://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Low

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)

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	74733
CVE	CVE-2015-4000

Plugin Information

Published: 2015/05/28, Modified: 2019/11/27

Plugin Output

tcp/443

```
Vulnerable connection combinations :

  SSL/TLS version  : SSLv3
  Cipher suite     : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
  Diffie-Hellman MODP size (bits) : 512
  Logjam attack difficulty : Easy (could be carried out by individuals)
```

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

https://weakdh.org/

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Low

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)

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:U/RL:ND/RC:C)

References

BID	74733
CVE	CVE-2015-4000

Plugin Information

Published: 2015/05/21, Modified: 2019/11/26

Plugin Output

tcp/443

```
EXPORT_DHE cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

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

Plugin Information

Published: 2010/07/30, Modified: 2019/11/22

Plugin Output

tcp/80

```
URL        : http://192.168.10.105/
Version    : 1.3.20
backported : 0
modules    : (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
os         : Unix
```

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

Plugin Information

Published: 2010/07/30, Modified: 2019/11/22

Plugin Output

tcp/443

```
URL        : https://192.168.10.105/
Version    : 1.3.20
backported : 0
modules    : (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
os         : Unix
```

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

Plugin Output

tcp/0

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

  cpe:/o:linux:linux_kernel:2.4

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:1.3.20 -> Apache Software Foundation Apache HTTP Server 1.3.20
  cpe:/a:modssl:mod_ssl:2.8.4 -> mod_ssl 2.8.4
  cpe:/a:openssl:openssl:0.9.6b -> OpenSSL Project OpenSSL 0.9.6b
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 70
```

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: 2018/11/15

Plugin Output

tcp/0

```
The following card manufacturers were identified :

08:00:27:12:48:07 : PCS Systemtechnik GmbH
```

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: 2018/08/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:12:48:07
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2019/09/20

Plugin Output

tcp/443

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

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

Plugin Output

tcp/80

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

```
- HTTP methods  HEAD  OPTIONS  TRACE GET are allowed on :

  /
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

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

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

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

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

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

Plugin Output

tcp/443

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

```
- HTTP methods  HEAD  OPTIONS  TRACE GET 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

Plugin Information

Published: 2000/01/04, Modified: 2019/11/22

Plugin Output

tcp/80

```
The remote web server type is :

Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
```

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

Plugin Information

Published: 2000/01/04, Modified: 2019/11/22

Plugin Output

tcp/443

```
The remote web server type is :

Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : GET, HEAD, OPTIONS, TRACE
Headers :

  Date: Mon, 23 Dec 2019 21:45:36 GMT
  Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
  Last-Modified: Thu, 06 Sep 2001 03:12:46 GMT
  ETag: "8805-b4a-3b96e9ae"
  Accept-Ranges: bytes
  Content-Length: 2890
  Connection: close
  Content-Type: text/html

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<HTML>
 <HEAD>
  <TITLE>Test Page for the Apache Web Server on Red Hat Linux</TITLE>
 </HEAD>
<!-- Background white, links blue (unvisited), navy (visited), red (active) -->
 <BODY BGCOLOR="#FFFFFF">
```

```
<H1 ALIGN="CENTER">Test Page</H1>
This page is used to test the proper operation of the Apache Web server after
it has been installed.  If you can read this page, it means that the Apache
Web server installed at this site is working properly.

<HR WIDTH="50%">

<H2 ALIGN="CENTER">If you are the administrator of this website:</H2>
<P>
You may now add content to this directory, and replace this page.  Note that
until you do so, people visiting your website will see this page, and not your
content.
</P>

<P>If you have upgraded from Red Hat Linux 6.2 and earlier, then you are
seeing this page because the default <A
href="manual/mod/core.html#documentroot"><STRONG>DocumentRoot</STRONG></A>
set in <TT>/etc/httpd/conf/httpd.conf</TT> has changed.  Any subdirectories
which existed under <TT>/home/httpd</TT> should now be moved to
<TT>/var/www</TT>.  Alternatively, the contents of <TT>/var/www</TT> can be
moved to <TT>/home/httpd</TT>, and the configuration file can be updated
accordingly.
</P>

<HR WIDTH="50%">
<H2 ALIGN="CENTER">If you are a member of the general public:</H2>

<P>
The fact that you are seeing this page indicates that the website you just
visited is either experiencing problems, or is undergoing routine maintenance.
</P>

<P>
If you would like to let the admini [...]
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443

```
Response Code : HTTP/1.0 200 OK

Protocol version : HTTP/1.0
SSL : yes
Keep-Alive : no
Options allowed : GET, HEAD, OPTIONS, TRACE
Headers :

  Date: Mon, 23 Dec 2019 21:45:36 GMT
  Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
  Last-Modified: Thu, 06 Sep 2001 03:12:46 GMT
  ETag: "8805-b4a-3b96e9ae"
  Accept-Ranges: bytes
  Content-Length: 2890
  Connection: close
  Content-Type: text/html

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<HTML>
 <HEAD>
  <TITLE>Test Page for the Apache Web Server on Red Hat Linux</TITLE>
 </HEAD>
<!-- Background white, links blue (unvisited), navy (visited), red (active) -->
 <BODY BGCOLOR="#FFFFFF">
```

```
<H1 ALIGN="CENTER">Test Page</H1>
This page is used to test the proper operation of the Apache Web server after
it has been installed.  If you can read this page, it means that the Apache
Web server installed at this site is working properly.

<HR WIDTH="50%">

<H2 ALIGN="CENTER">If you are the administrator of this website:</H2>
<P>
You may now add content to this directory, and replace this page.  Note that
until you do so, people visiting your website will see this page, and not your
content.
</P>

<P>If you have upgraded from Red Hat Linux 6.2 and earlier, then you are
seeing this page because the default <A
href="manual/mod/core.html#documentroot"><STRONG>DocumentRoot</STRONG></A>
set in <TT>/etc/httpd/conf/httpd.conf</TT> has changed.  Any subdirectories
which existed under <TT>/home/httpd</TT> should now be moved to
<TT>/var/www</TT>.  Alternatively, the contents of <TT>/var/www</TT> can be
moved to <TT>/home/httpd</TT>, and the configuration file can be updated
accordingly.
</P>

<HR WIDTH="50%">
<H2 ALIGN="CENTER">If you are a member of the general public:</H2>

<P>
The fact that you are seeing this page indicates that the website you just
visited is either experiencing problems, or is undergoing routine maintenance.
</P>

<P>
If you would like to let the admin [...]
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

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

Description

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

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

Solution

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

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -17999 seconds.
```

117886 - Local Checks Not Enabled (info)

Synopsis

Local checks were not enabled.

Description

Nessus did not enable local checks on the remote host. This does not necessarily indicate a problem with the scan. Credentials may not have been provided, local checks may not be available for the target, the target may not have been identified, or another issue may have occurred that prevented local checks from being enabled. See plugin output for details.

This plugin reports informational findings related to local checks not being enabled. For failure information, see plugin 21745 :

'Authentication Failure - Local Checks Not Run'.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/10/02, Modified: 2018/11/02

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : No Credentials Provided
    Message     :
Credentials were not provided for detected SSH service.
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2019/11/22

Plugin Output

tcp/139

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

106716 - Microsoft Windows SMB2 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2019/11/22

Plugin Output

tcp/139

```
The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2019/08/20

Plugin Output

tcp/22

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2019/08/20

Plugin Output

tcp/80

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2019/08/20

Plugin Output

tcp/111

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2019/08/20

Plugin Output

tcp/139

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2019/08/20

Plugin Output

tcp/443

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2019/08/20

Plugin Output

tcp/32768

```
Port 32768/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2019/03/06

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.8.0
Plugin feed version : 201911291250
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 192.168.10.101
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2019/12/23 17:44 CET
Scan duration : 315 sec
```

110723 - 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 unable to execute credentialed checks because no credentials were provided.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/27, Modified: 2018/10/02

Plugin Output

tcp/0

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

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: 2019/09/04

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.4
Confidence level : 70
Method : SinFP


The remote host is running Linux Kernel 2.4
```

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

Plugin Information

Published: 2011/12/16, Modified: 2019/11/22

Plugin Output

tcp/80

```
Source             : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version   : 0.9.6b
```

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

Plugin Information

Published: 2011/12/16, Modified: 2019/11/22

Plugin Output

tcp/443

```
Source             : Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version   : 0.9.6b
```

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.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2019/11/12

Plugin Output

tcp/0

```
. You need to take the following 3 actions :


[ Apache HTTP Server 403 Error Page UTF-7 Encoded XSS (17696) ]

+ Action to take : Upgrade to Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 or later. These versions
 use a default configuration setting that prevents exploitation in vulnerable web browsers.


[ OpenSSL < 0.9.8y Multiple Vulnerabilities (64532) ]

+ Action to take : Upgrade to OpenSSL 0.9.8y or later.

+Impact : Taking this action will resolve 44 different vulnerabilities (CVEs).


[ Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information
 Disclosure (53841) ]

+ Action to take : Upgrade to Portable OpenSSH 5.8p2 or later.

+Impact : Taking this action will resolve 25 different vulnerabilities (CVEs).
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/111

```
The following RPC services are available on TCP port 111 :

 - program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/111

```
The following RPC services are available on UDP port 111 :

 - program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/32768

```
The following RPC services are available on TCP port 32768 :

 - program: 100024 (status), version: 1
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/32768

```
The following RPC services are available on UDP port 32768 :

 - program: 100024 (status), version: 1
```

53335 - RPC portmapper (TCP)

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/04/08, Modified: 2011/08/29

Plugin Output

tcp/111

10223 - RPC portmapper Service Detection

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

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

Solution

n/a

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

CVE	CVE-1999-0632

Plugin Information

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

Plugin Output

udp/111

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

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

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

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  arcfour
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
  rijndael128-cbc
  rijndael192-cbc
  rijndael256-cbc

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
```

```
  aes128-cbc
  aes192-cbc
  aes256-cbc
  arcfour
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
  rijndael128-cbc
  rijndael192-cbc
  rijndael256-cbc

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib
```

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: 2019/11/22

Plugin Output

tcp/22

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

  - 1.33
  - 1.5
  - 1.99
  - 2.0


SSHv1 host key fingerprint : b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86
```

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

Plugin Information

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

Plugin Output

tcp/22

```
SSH version : SSH-1.99-OpenSSH_2.9p2
SSH supported authentication : publickey,password,keyboard-interactive
```

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: 2019/03/01

Plugin Output

tcp/443

```
This port supports SSLv2/SSLv3/TLSv1.0.
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2019/06/25

Plugin Output

tcp/443

```
The host name known by Nessus is :

  kioptrix

The Common Name in the certificate is :

  localhost.localdomain
```

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: 2019/07/18

Plugin Output

tcp/443

```
Subject Name:

Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrganization
Organization Unit: SomeOrganizationalUnit
Common Name: localhost.localdomain
Email Address: root@localhost.localdomain

Issuer Name:

Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrganization
Organization Unit: SomeOrganizationalUnit
Common Name: localhost.localdomain
Email Address: root@localhost.localdomain

Serial Number: 00

Version: 3

Signature Algorithm: MD5 With RSA Encryption

Not Valid Before: Sep 26 09:32:06 2009 GMT
Not Valid After: Sep 26 09:32:06 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 CE 01 5E 22 B9 6D 69 52 A1 BE 01 E9 AF 40 2E 62 83 6D 2C
            6A A0 C7 0C DE 9B C6 1E C7 05 B0 9B 3E 7C 71 E7 F8 28 D4 D4
            35 F8 E0 B3 C3 34 EC 30 3A 5E 94 A9 BF 86 B5 92 6F EA 3B 95
            7A D0 F0 71 36 DB A1 C0 B6 04 CF BA C7 A8 32 57 F1 FA 69 8B
            82 B2 C0 B0 AC EB 95 29 6A 7B 97 DC 55 A5 A7 63 21 35 26 86
            1F AE 07 CD 6A CA AA 29 B7 FF D9 E1 31 F0 C3 B4 9E CC B2 50
            5E 2D 7E 1A B9 A9 DE 21 43
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 56 0A E6 A6 9A DF 92 67 7C BF 2D 04 D1 49 99 BD 67 48 70
           3A C8 61 1B D4 59 CC 12 17 07 3A 6C 6A 89 78 9A F4 09 84 81
           FA 30 D0 CC 0E 82 BB B9 ED C6 3A E5 5F 11 23 1C 50 41 6C 5E
           22 10 C2 43 9E E4 13 14 6B C8 09 02 1C AE A2 68 1F 79 6A 00
           EE F7 BB 84 DE 04 38 E1 BF 99 FE 87 E4 B7 EC 21 DD D6 5B E0
           46 0A 0E 6B 2F 5D 59 A2 CA 3B 25 13 86 02 85 D8 77 0F 58 C6
           48 8F 67 EB A2 8E 5E 8A 13

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: EC E7 51 4B 43 6B 6C D0 7C 80 4F 6A 52 37 30 F0 B1 7C C4 A0


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: EC E7 51 4B 43 6B 6C D0 7C 80 4F 6A 52 37 30 F0 B1 7C C4 A0
Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrg [...]
```

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: 2018/11/15

Plugin Output

tcp/443

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

  Low Strength Ciphers (<= 64-bit key)

     DES-CBC-MD5                 Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=MD5
     EXP-RC2-CBC-MD5             Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
  export
     EXP-EDH-RSA-DES-CBC-SHA     Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
  export
     EDH-RSA-DES-CBC-SHA         Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
     EXP1024-DES-CBC-SHA         Kx=RSA(1024)   Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
  export
     EXP1024-RC2-CBC-MD5         Kx=RSA(1024)   Au=RSA      Enc=RC2-CBC(56)          Mac=MD5
  export
     EXP-DES-CBC-SHA             Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
  export
```

```
    EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
 export
    DES-CBC-SHA                  Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

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

    DES-CBC3-MD5                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=MD5
    EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    RC2-CBC-MD5                  Kx=RSA         Au=RSA      Enc=RC2-CBC(128)         Mac=MD5

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2019/05/10

Plugin Output

tcp/443

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

SSL Version : TLSv1
  Low Strength Ciphers (<= 64-bit key)

    EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
    EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
    EXP1024-DES-CBC-SHA          Kx=RSA(1024)   Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
 export
    EXP1024-RC2-CBC-MD5          Kx=RSA(1024)   Au=RSA      Enc=RC2-CBC(56)          Mac=MD5
 export
    EXP1024-RC4-MD5              Kx=RSA(1024)   Au=RSA      Enc=RC4(56)              Mac=MD5
 export
    EXP1024-RC4-SHA              Kx=RSA(1024)   Au=RSA      Enc=RC4(56)              Mac=SHA1
 export
    EXP-DES-CBC-SHA              Kx=RSA(512)    Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
    EXP-RC2-CBC-MD5              Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
 export
    EXP-RC4-MD5                  Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
 export
```

```
    DES-CBC-SHA                 Kx=RSA         Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

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

    EDH-RSA-DES-CBC3-SHA        Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
    RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1


SSL Version : SSLv3
  Low Strength Ciphers (<= 64-bit key)

    EXP-EDH-RSA-DES-CBC-SHA     Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
    EDH-RSA-DES-CBC-SHA         Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1
    EXP1024-DES-CBC-SHA         Kx=RSA(1024)   Au=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: 2018/11/15

Plugin Output

tcp/443

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

  Low Strength Ciphers (<= 64-bit key)

    EXP-EDH-RSA-DES-CBC-SHA      Kx=DH(512)     Au=RSA      Enc=DES-CBC(40)          Mac=SHA1
 export
    EDH-RSA-DES-CBC-SHA          Kx=DH          Au=RSA      Enc=DES-CBC(56)          Mac=SHA1

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

    EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
```

```
    Enc={symmetric encryption method}
    Mac={message authentication code}
    {export flag}
```

58768 - SSL Resume With Different Cipher Issue

Synopsis

The remote host allows resuming SSL sessions with a different cipher than the one originally negotiated.

Description

The SSL implementation on the remote host has been shown to allow a cipher other than the one originally negotiated when resuming a session. An attacker that sees (e.g. by sniffing) the start of an SSL connection may be able to manipulate session cache to cause subsequent resumptions of that session to use a cipher chosen by the attacker.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/04/17, Modified: 2012/04/17

Plugin Output

tcp/443

```
The server allowed the following session over TLSv1 to be resumed as follows :

  Session ID     : 5977072df72fee19399afd8278a006e7303881e0aee7a114b4607a7c0c31acbf
  Initial Cipher : TLS1_CK_RSA_WITH_RC4_128_SHA (0x0005)
  Resumed Cipher : TLS1_CK_RSA_EXPORT1024_WITH_RC4_56_SHA (0x0064)
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443

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

|-Subject             : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
|-Issuer              : C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/E=root@localhost.localdomain
|-Valid From          : Sep 26 09:32:06 2009 GMT
|-Valid To            : Sep 26 09:32:06 2010 GMT
|-Signature Algorithm : MD5 With RSA Encryption
```

53360 - SSL Server Accepts Weak Diffie-Hellman Keys

Synopsis

The remote SSL/TLS server accepts a weak Diffie-Hellman public value.

Description

The remote SSL/TLS server accepts a weak Diffie-Hellman (DH) public key value.

This flaw may aid an attacker in conducting a man-in-the-middle (MiTM) attack against the remote server since it could enable a forced calculation of a fully predictable Diffie-Hellman secret.

By itself, this flaw is not sufficient to set up a MiTM attack (hence a risk factor of 'None'), as it would require some SSL implementation flaws to affect one of the clients connecting to the remote host.

See Also

https://www.cl.cam.ac.uk/~rja14/Papers/psandqs.pdf

https://tls.mbed.org/tech-updates/security-advisories/polarssl-security-advisory-2011-01

Solution

OpenSSL is affected when compiled in FIPS mode. To resolve this issue, either upgrade to OpenSSL 1.0.0, disable FIPS mode or configure the ciphersuite used by the server to not include any Diffie-Hellman key exchanges.

PolarSSL is affected. To resolve this issue, upgrade to version 0.99-pre3 / 0.14.2 or higher.

If using any other SSL implementation, configure the ciphersuite used by the server to not include any Diffie-Hellman key exchanges or contact your vendor for a patch.

Risk Factor

None

Plugin Information

Published: 2011/04/11, Modified: 2018/11/15

Plugin Output

tcp/443

```
It was possible to complete a full SSL handshake by sending a DH key
with a value of 1.
```

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: 2013/10/18

Plugin Output

tcp/443

```
This port supports resuming SSLv3 / TLSv1 sessions.
```

131290 - SSL/TLS Deprecated Ciphers

Synopsis

The remote host utilises deprecated SSL/TLS ciphers

Description

The remote host has open SSL/TLS ports which advertise deprecated ciphers. These ciphers are no longer supported by most major ssl libraries such as openssl, nss, mbed and wolfssl and, as such, should not be utilised for secure communication.

Solution

Upgrade to a cipher suite which does not contain outlined deprecated ciphers.

Risk Factor

None

Plugin Information

Published: 2019/11/26, Modified: 2019/11/26

Plugin Output

tcp/0

```
The remote host has listening SSL/TLS ports which advertise cipher suites containing deprecated
 ciphers.
The ports and their respective, deprecated ciphers are outlined below:
Port 443:
- TLS1_CK_RSA_EXPORT_WITH_RC4_40_MD5
- TLS1_CK_RSA_WITH_DES_CBC_SHA
- TLS1_CK_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS1_CK_RSA_EXPORT_WITH_RC2_CBC_40_MD5
- TLS1_CK_DHE_RSA_WITH_DES_CBC_SHA
- TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
```

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: 2019/10/29

Plugin Output

tcp/22

```
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: 2019/10/29

Plugin Output

tcp/80

```
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: 2019/10/29

Plugin Output

tcp/443

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

tcp/443

```
A web 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: 2019/03/06

Plugin Output

tcp/0

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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

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.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information

Published: 2017/11/22, Modified: 2019/11/22

Plugin Output

tcp/443

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

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: 2019/03/06

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.10.101 to 192.168.10.105 :
192.168.10.101
192.168.10.105

Hop Count: 1
```

11422 - Web Server Unconfigured - Default Install Page Present

Synopsis

The remote web server is not configured or is improperly configured.

Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2018/08/15

Plugin Output

tcp/80

```
The default welcome page is from Apache.
```

11422 - Web Server Unconfigured - Default Install Page Present

Synopsis

The remote web server is not configured or is improperly configured.

Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2018/08/15

Plugin Output

tcp/443

```
The default welcome page is from Apache.
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/05/31

Plugin Output

udp/137

```
The following 7 NetBIOS names have been gathered :

 KIOPTRIX         = Computer name
 KIOPTRIX         = Messenger Service
 KIOPTRIX         = File Server Service
 __MSBROWSE__     = Master Browser
 MYGROUP          = Workgroup / Domain name
 MYGROUP          = Master Browser
 MYGROUP          = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 38% of the vulnerabilities on the network.

ACTION TO TAKE	VULNS	HOSTS
OpenSSL < 0.9.8y Multiple Vulnerabilities: Upgrade to OpenSSL 0.9.8y or later.	44	1
Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure: Upgrade to Portable OpenSSH 5.8p2 or later.	25	1
Apache HTTP Server 403 Error Page UTF-7 Encoded XSS: Upgrade to Apache HTTP Server 2.2.8 / 2.0.63 / 1.3.41 or later. These versions use a default configuration setting that prevents exploitation in vulnerable web browsers.	1	1