My scan

Fri, 19 Nov 2021 09:23:06 Pacific Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

172.16.11.5

CRITICAL	HIGH	MEDIUM	LOW	INFO
11	10	25	5	128

Scan Information

Start time: Fri Nov 19 09:00:27 2021
End time: Fri Nov 19 09:06:59 2021

Host Information

Netbios Name: METASPLOITABLE
IP: 172.16.11.5
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat) -

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

See Also

http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e
https://access.redhat.com/security/cve/CVE-2020-1745
https://access.redhat.com/solutions/4851251
http://www.nessus.org/u?dd218234
http://www.nessus.org/u?dd772531
http://www.nessus.org/u?2a01d6bf
http://www.nessus.org/u?3b5af27e
http://www.nessus.org/u?9dab109f
http://www.nessus.org/u?5eafcf70

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2020-1745
CVE CVE-2020-1938

Plugin Information

Published: 2020/03/24, Modified: 2021/10/19

Plugin Output

tcp/8009/ajp13

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

0x0000: 02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F ....HTTP/1.1.../
0x0010: 61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00 asdf/xxxxx.jsp..
0x0020: 09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C .localhost.....l
0x0030: 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06 ocalhost..P.....
0x0040: 00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41 ..keep-alive...A
0x0050: 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00 ccept-Language..
0x0060: 0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00 .en-US,en;q=0.5.
0x0070: A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45 ....0...Accept-E
0x0080: 6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20 ncoding...gzip,
0x0090: 64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D deflate, sdch...
0x00A0: 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09 Cache-Control...
0x00B0: 6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F max-age=0.....Mo
0x00C0: 7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D zilla...Upgrade-
0x00D0: 49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74 Insecure-Request
0x00E0: 73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68 s...1.....text/h
```

```
0x00F0: 74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73 tml.....localhos
0x0100: 74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C t...!javax.servl
0x0110: 65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65 et.include.reque
0x0120: 73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61 st_uri...1....ja
0x0130: 76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C vax.servlet.incl
0x0140: 75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10 ude.path_info...
0x0150: 2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C /WEB-INF/web.xml
0x0160: 00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65 ..."javax.servle
0x0170: 74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65 t.include.servle
0x0180: 74 5F 70 61 74 68 00 00 00 00 FF t_path.....


This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
...<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0
[...]

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

51988 - Bind Shell Backdoor Detection -

Synopsis

The remote host may have been compromised.

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2011/02/15, Modified: 2019/05/10

Plugin Output

tcp/1524/wild_shell

```
Nessus was able to execute the command "id" using the
following request :


This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

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

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness -

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/14, Modified: 2018/11/15

Plugin Output

tcp/22/ssh

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) -

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

Plugin Output

tcp/25/smtp

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) -

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

Plugin Output

tcp/5432/postgresql

11356 - NFS Exported Share Information Disclosure -

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Risk Factor

Critical

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

Exploitable With

Metasploit (true)

Plugin Information

Published: 2003/03/12, Modified: 2018/09/17

Plugin Output

udp/2049/rpc-nfs

```
The following NFS shares could be mounted :

+ /
+ Contents of / :
- -GT
- .
- ..
- Q.aP{#.kijU
- bin
- boot
- cdrom
- dev
- etc
- home
- initrd
- initrd.img
- lcr
- lib
- lost+found
- media
- mnt
- nohup.out
- opt
- proc
- root
- sbin
- srv
- sys
- tmp
- usr
- var
- vmlinuz
```

33850 - Unix Operating System Unsupported Version Detection -

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host 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.

Solution

Upgrade to a version of the Unix operating system 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 v2.0 Base Score

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

References

XREF	IAVA:0001-A-0502
XREF	IAVA:0001-A-0648

Plugin Information

Published: 2008/08/08, Modified: 2021/09/30

Plugin Output

tcp/0

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.

For more information, see : https://wiki.ubuntu.com/Releases
```

46882 - UnrealIRCd Backdoor Detection -

Synopsis

The remote IRC server contains a backdoor.

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

See Also

https://seclists.org/fulldisclosure/2010/Jun/277
https://seclists.org/fulldisclosure/2010/Jun/284
http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	40820
CVE	CVE-2010-2075

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2010/06/14, Modified: 2018/11/28

Plugin Output

tcp/6667/irc

```
The remote IRC server is running as :

uid=0(root) gid=0(root)
```

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 web server if it is no longer needed. Otherwise, upgrade to a supported 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 v2.0 Base Score

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

References

XREF	IAVA:0001-A-0617

Plugin Information

Published: 2008/10/21, Modified: 2021/11/17

Plugin Output

tcp/8180/www

```
Product : Tomcat
Installed version : 5.5
Support ended : 2012-09-30
Supported versions : 8.5.x / 9.x / 10.x
Additional information : http://tomcat.apache.org/tomcat-55-eol.html
```

61708 - VNC Server 'password' Password -

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Risk Factor

Critical

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

tcp/5900/vnc

```
Nessus logged in using a password of "password".
```

10203 - rexecd Service Detection -

Synopsis

The rexecd service is running on the remote host.

Description

The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely.
However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

Solution

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

Risk Factor

Critical

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0618

Plugin Information

Published: 1999/08/31, Modified: 2018/08/13

Plugin Output

tcp/512/rexecd

136808 - ISC BIND Denial of Service -

Synopsis

The remote name server is affected by an assertion failure vulnerability.

Description

A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.

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

See Also

https://kb.isc.org/docs/cve-2020-8617

Solution

Upgrade to the patched release most closely related to your current version of BIND.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE CVE-2020-8617
XREF IAVA:2020-A-0217-S

Plugin Information

Published: 2020/05/22, Modified: 2020/12/10

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version : 9.11.19
```

136769 - ISC BIND Service Downgrade / Reflected DoS -

Synopsis

The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities.

Description

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.

An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

See Also

https://kb.isc.org/docs/cve-2020-8616

Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-8616
XREF	IAVA:2020-A-0217-S

Plugin Information

Published: 2020/05/22, Modified: 2020/06/26

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version : 9.11.19
```

42256 - NFS Shares World Readable -

Synopsis

The remote NFS server exports world-readable shares.

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Solution

Place the appropriate restrictions on all NFS shares.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2009/10/26, Modified: 2020/05/05

Plugin Output

tcp/2049/rpc-nfs

```
The following shares have no access restrictions :

/ *
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

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

Description

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-2016-2183

Plugin Information

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

Plugin Output

tcp/25/smtp

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

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-MD5 0x07, 0x00, 0xC0 RSA RSA 3DES-CBC(168) MD5
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
```

```
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

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

Description

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

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

Plugin Output

tcp/5432/postgresql

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

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

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

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 1.2 (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 v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/25/smtp

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

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EXP-RC2-CBC-MD5 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 RSA(512) RSA RC4(40) MD5 export

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

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DES-CBC3-MD5 RSA RSA 3DES-CBC(168) MD5

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
RC4-MD5 RSA RSA RC4(128) MD5

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={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)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EXP-EDH-RSA-DES-CBC-SHA DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 RSA(512) RSA RC4(40) MD5 export
DES-CBC-SHA RSA RSA DES-CBC(56) SHA1

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

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA DH None 3DES-CBC(168) SHA1
DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA DH RSA AES-CBC(256) SHA1
ADH-AES128-SHA DH None AES-CBC(128) SHA1
ADH-AES256-SHA DH None AES-CBC(256) SHA1
ADH-RC4-MD5 DH None RC4(128) MD5
AES128-SHA RSA RSA AES-CBC(128) SHA1
AES256-SHA RSA RSA AES-CBC(256) SHA1
RC4-MD5 RSA RSA RC4(128) MD5
RC4-SHA RSA RSA RC4(128) SHA1

The fields above are :

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

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 1.2 (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 v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/5432/postgresql

```
- 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


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

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA DH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA DH RSA AES-CBC(256) SHA1
AES128-SHA RSA RSA AES-CBC(128) SHA1
AES256-SHA RSA RSA AES-CBC(256) SHA1
RC4-SHA RSA RSA RC4(128) SHA1

The fields above are :

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

90509 - Samba Badlock Vulnerability -

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

http://badlock.org
https://www.samba.org/samba/security/CVE-2016-2118.html

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	86002
CVE	CVE-2016-2118
XREF	CERT:813296

Plugin Information

Published: 2016/04/13, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Nessus detected that the Samba Badlock patch has not been applied.
```

10205 - rlogin Service Detection -

Synopsis

The rlogin service is running on the remote host.

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.
Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0651

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/08/30, Modified: 2018/08/13

Plugin Output

tcp/513/rlogin

10245 - rsh Service Detection -

Synopsis

The rsh service is running on the remote host.

Description

The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.
Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0651

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/08/22, Modified: 2018/08/13

Plugin Output

tcp/514/rsh

12085 - Apache Tomcat Default Files -

Synopsis

The remote web server contains default files.

Description

The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

See Also

http://www.nessus.org/u?4cb3b4dd
https://www.owasp.org/index.php/Securing_tomcat

Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

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 v2.0 Base Score

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

Plugin Information

Published: 2004/03/02, Modified: 2019/08/12

Plugin Output

tcp/8180/www

```
The following default files were found :

http://172.16.11.5:8180/tomcat-docs/index.html

The server is not configured to return a custom page in the event of a client requesting a non-existent resource.
This may result in a potential disclosure of sensitive information about the server to attackers.
```

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 HTTP methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2020/06/12

Plugin Output

tcp/80/www

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus199449813.html HTTP/1.1
Connection: Close
Host: 172.16.11.5
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: Thu, 18 Nov 2021 20:54:07 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus199449813.html HTTP/1.1
Connection: Keep-Alive
Host: 172.16.11.5
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 ------------------------------
```

139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS -

Synopsis

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

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.

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

See Also

https://kb.isc.org/docs/cve-2020-8622

Solution

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-8622
XREF	IAVA:2020-A-0385-S

Plugin Information

Published: 2020/08/27, Modified: 2021/06/03

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version : 9.11.22, 9.16.6, 9.17.4 or later
```

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

http://www.nessus.org/u?df39b8b3
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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

Plugin Information

Published: 2012/01/19, Modified: 2021/03/15

Plugin Output

tcp/445/cifs

52611 - SMTP Service STARTTLS Plaintext Command Injection -

Synopsis

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

Description

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

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

See Also

https://tools.ietf.org/html/rfc2487
https://www.securityfocus.com/archive/1/516901/30/0/threaded

Solution

Contact the vendor to see if an update is available.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	46767
CVE	CVE-2011-0411
CVE	CVE-2011-1430
CVE	CVE-2011-1431
CVE	CVE-2011-1432
CVE	CVE-2011-1506
CVE	CVE-2011-2165
XREF	CERT:555316

Plugin Information

Published: 2011/03/10, Modified: 2019/03/06

Plugin Output

tcp/25/smtp

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

STARTTLS\r\nRSET\r\n

And the server sent the following two responses :

220 2.0.0 Ready to start TLS
250 2.0.0 Ok
```

90317 - SSH Weak Algorithms Supported -

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/22/ssh

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

arcfour
arcfour128
arcfour256

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

arcfour
arcfour128
arcfour256
```

31705 - SSL Anonymous Cipher Suites Supported -

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

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

Solution

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

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	28482
CVE	CVE-2007-1858

Plugin Information

Published: 2008/03/28, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1

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

```
Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5

The fields above are :

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

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/25/smtp

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

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise
Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain
|-Not After : Apr 16 14:07:45 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=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise
Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain
|-Issuer : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple
Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain
```


51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/5432/postgresql

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

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise
Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain
|-Not After : Apr 16 14:07:45 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=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise
Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain
|-Issuer : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple
Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.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 v2.0 Base Score

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

Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
The SSL certificate has already expired :

Subject : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise
Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
Issuer : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise
Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
Not valid before : Mar 17 14:07:45 2010 GMT
Not valid after : Apr 16 14:07:45 2010 GMT
```

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 v2.0 Base Score

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

Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

Plugin Output

tcp/5432/postgresql

```
The SSL certificate has already expired :

Subject : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise
Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
Issuer : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise
Simple Affairs, CN=ubuntu804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
Not valid before : Mar 17 14:07:45 2010 GMT
Not valid after : Apr 16 14:07:45 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 SSL 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 v2.0 Base Score

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

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/25/smtp

```
The identities known by Nessus are :

172.16.11.5
172.16.11.5

The Common Name in the certificate is :

ubuntu804-base.localdomain
```

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 SSL 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 v2.0 Base Score

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

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/5432/postgresql

```
The identities known by Nessus are :

172.16.11.5
172.16.11.5

The Common Name in the certificate is :

ubuntu804-base.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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	83733
CVE	CVE-2016-0800
XREF	CERT:583776

Plugin Information

Published: 2016/03/01, Modified: 2019/11/20

Plugin Output

tcp/25/smtp

```
The remote host is affected by SSL DROWN and supports the following
vulnerable cipher suites :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-RC2-CBC-MD5 0x04, 0x00, 0x80 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x02, 0x00, 0x80 RSA(512) RSA RC4(40) MD5 export

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
RC4-MD5 0x01, 0x00, 0x80 RSA RSA RC4(128) MD5

The fields above are :

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

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

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

See Also

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

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

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-RC4-MD5 0x02, 0x00, 0x80 RSA(512) RSA RC4(40) MD5 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
RC4-MD5 0x01, 0x00, 0x80 RSA RSA RC4(128) MD5
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :
```

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

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

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

See Also

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/5432/postgresql

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

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

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

57582 - SSL Self-Signed Certificate -

Synopsis

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

Description

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/25/smtp

```
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=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise
Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain
```

57582 - SSL Self-Signed Certificate -

Synopsis

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

Description

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/5432/postgresql

```
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=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise
Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.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 v2.0 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: 2021/02/03

Plugin Output

tcp/25/smtp

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

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EXP-RC2-CBC-MD5 0x04, 0x00, 0x80 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x02, 0x00, 0x80 RSA(512) RSA RC4(40) MD5 export
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1

The fields above are :

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

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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	71936
CVE	CVE-2015-0204
XREF	CERT:243585

Plugin Information

Published: 2015/03/04, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
EXPORT_RSA cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/25/smtp

```
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.
```

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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/5432/postgresql

```
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.
```

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/25/smtp

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

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/5432/postgresql

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

42263 - Unencrypted Telnet Server -

Synopsis

The remote Telnet server transmits traffic in cleartext.

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2009/10/27, Modified: 2020/06/12

Plugin Output

tcp/23/telnet

```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------
_ _ _ _ _ _ ____
_ __ ___ ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
|_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
------------------------------ snip ------------------------------
```

70658 - SSH Server CBC Mode Ciphers Enabled -

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

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

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

Solution

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

Risk Factor

Low

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

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

Plugin Output

tcp/22/ssh

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

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

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

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

153953 - SSH Weak Key Exchange Algorithms Enabled -

Synopsis

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

Description

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

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

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

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

See Also

http://www.nessus.org/u?b02d91cd
https://datatracker.ietf.org/doc/html/rfc8732

Solution

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

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

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

71049 - SSH Weak MAC Algorithms Enabled -

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

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

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

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

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

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

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

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 v2.0 Base Score

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

CVSS v2.0 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: 2021/02/03

Plugin Output

tcp/25/smtp

```
EXPORT_DHE cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export

The fields above are :

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

10407 - X Server Detection -

Synopsis

An X11 server is listening on the remote host

Description

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution

Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2000/05/12, Modified: 2019/03/05

Plugin Output

tcp/6000/x11

```
X11 Version : 11.0
```

21186 - AJP Connector Detection

Synopsis

There is an AJP connector listening on the remote host.

Description

The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web server such as Apache communicates over TCP with a Java servlet container such as Tomcat.

See Also

http://tomcat.apache.org/connectors-doc/
http://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/04/05, Modified: 2019/11/22

Plugin Output

tcp/8009/ajp13

```
The connector listing on this port supports the ajp13 protocol.
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.
n/a

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2019/10/01

Plugin Output

tcp/0

```
The Linux distribution detected was :
- Ubuntu 8.04 (gutsy)
```

48204 - Apache HTTP Server Version

Synopsis

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

Description

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

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

tcp/80/www

```
URL : http://172.16.11.5/
Version : 2.2.99
backported : 1
modules : DAV/2
os : ConvertedUbuntu
```

39446 - Apache Tomcat Detection -

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2020/09/22

Plugin Output

tcp/8180/www

```
URL : http://172.16.11.5:8180/
Version : 5.5
backported : 0
source : Apache Tomcat/5.5
```

39519 - Backported Security Patch Detection (FTP) -

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2121/ftp

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

84574 - Backported Security Patch Detection (PHP) -

Synopsis

Security patches have been backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/07, Modified: 2015/07/07

Plugin Output

tcp/80/www

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

39520 - Backported Security Patch Detection (SSH) -

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

39521 - Backported Security Patch Detection (WWW) -

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

45590 - Common Platform Enumeration (CPE) -

Synopsis

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

Description

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

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

See Also

http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2021/11/08

Plugin Output

tcp/0

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

cpe:/o:canonical:ubuntu_linux:8.04

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server 2.2.8
cpe:/a:apache:http_server:2.2.99
cpe:/a:apache:tomcat:5.5
```

```
cpe:/a:isc:bind:9.4.
cpe:/a:isc:bind:9.4.2 -> ISC BIND 9.4.2
cpe:/a:mysql:mysql:5.0.51a-3ubuntu5
cpe:/a:openbsd:openssh:4.7 -> OpenBSD OpenSSH 4.7
cpe:/a:php:php:5.2.4 -> PHP 5.2.4
cpe:/a:php:php:5.2.4-2ubuntu5.10
cpe:/a:postgresql:postgresql:
cpe:/a:samba:samba:3.0.20 -> Samba 3.0.20
```

10028 - DNS Server BIND version Directive Remote Version Detection -

Synopsis

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

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF IAVT:0001-T-0583

Plugin Information

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

Plugin Output

udp/53/dns

```
Version : 9.4.2
```

11002 - DNS Server Detection -

Synopsis

A DNS server is listening on the remote host.

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/53/dns

11002 - DNS Server Detection -

Synopsis

A DNS server is listening on the remote host.

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

udp/53/dns

72779 - DNS Server Version Detection -

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0937

Plugin Information

Published: 2014/03/03, Modified: 2020/09/22

Plugin Output

tcp/53/dns

```
DNS server answer for "version.bind" (over TCP) :

9.4.2
```

35371 - DNS Server hostname.bind Map Hostname Disclosure -

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information

Published: 2009/01/15, Modified: 2011/09/14

Plugin Output

udp/53/dns

```
The remote host name is :

metasploitable
```

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 : 95
```

10092 - FTP Server Detection -

Synopsis

An FTP server is listening on a remote port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220 (vsFTPd 2.3.4)
```

10092 - FTP Server Detection -

Synopsis

An FTP server is listening on a remote port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2121/ftp

```
The remote FTP banner is :

220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.16.11.5]
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.2.8 (Ubuntu) DAV/2
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/8180/www

```
The remote web server type is :

Apache-Coyote/1.1
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

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

Date: Thu, 18 Nov 2021 20:54:25 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

```
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

_ _ _ _ _ _ ____
 _ __ ___ ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8180/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Headers :

Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 18 Nov 2021 20:54:24 GMT
Connection: close

Response Body :

<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>Apache Tomcat/5.5</title>
<style type="text/css">
/*<![CDATA[*/
body {
color: #000000;
background-color: #FFFFFF;
font-family: Arial, "Times New Roman", Times, serif;
margin: 10px 0px;
}

img {
border: none;
}

a:link, a:visited {
color: blue
}

th {
font-family: Verdana, "Times New Roman", Times, serif;
font-size: 110%;
font-weight: normal;
font-style: italic;
background: #D2A41C;
text-align: left;
}

td {
```

```
color: #000000;
font-family: Arial, Helvetica, sans-serif;
}

td.menu {
background: #FFDC75;
}

.center {
text-align: center;
}

.code {
color: #000000;
font-family: "Courier New", Courier, monospace;
font-size: 110%;
margin-left: 2.5em;
}

#banner {
margin-bottom: 12px;
}

p#congrats {
margin-top: 0;
font-weight: bold;
text-align: center;
}

p#footer {
text-align: right;
font-size: 80%;
}
/*]]>*/
</style>
</head>

<body>

<!-- Header -->
<table id="banner" width="100%">
<tr>
<td align="left" style="width:130px">
<a href="http://tomcat.apache.org/">
<img src="tomcat.gif" height="92" width="130" alt="The Mighty Tomcat - MEOW!"/>
</a>
</td>
<td align="left" valign="top"><b>Apache Tomcat/5.5</b></td>
<td align="right">
<a href="http://www.apache.org/">
<img src="asf-logo-wide.gif" height="51" width="537" alt="The Apache Software Foundation"/>
</a>
</td>
</tr>
</table>

<table>
<tr>

<!-- Table of Contents -->
<td valign="top">
<table width="100%" border="1" cellspacing="0" cellpadding="3">
<tr>
<th>Administration</th>
</tr>
<tr>
<td class="menu">
<a href="manager/status">Status</a><br/>
<a href="admin">Tomcat Administration</a><br/>
<a href="manager/html">Tomcat Manager</a><br/>
 
</td>
</tr>
</table>

<br />
<table width="100%" border="1" cellspacing="0" cellpadding="3">
<tr>
<th>Documentation</th>
</tr>
<tr>
<td class="menu">
<a href="RELEASE-NOTES.txt">Release Notes</a><br/>
<a href="tomcat-docs/changelog.html">Change Log</a><br/>
<a href="tomcat-docs">Tomcat Documentation</a><br/>  
 
</td>
</tr>
</table>

<br/>
<table width="100%" border="1" cellspacing="0" cellpadding="3">
<tr>
<th>Tomcat Online</th>
</tr>
<tr>
<td class="menu">
<a href="http://tomcat.apache.org/">Home Page</a><br/>
<a href="http://tomcat.apache.org/faq/">FAQ</a><br/>
<a href="http://tomcat.apache.org/bugreport.html">Bug Database</a><br/>
<a href="http://issues.apache.org/bugzilla/buglist.cgi?
bug_status=UNCONFIRMED&amp;bug_status=NEW&amp;bug_status=ASSIGNED&amp;bug_status=REOPENED&amp;bug_status=RESOLVED&amp;resolution=LATER&amp;resolution=REMIND&amp;re
--&amp;bugidtype=include&amp;product=Tomcat+5&amp;cmdtype=doit&amp;order=Importance">Open Bugs</a><br/>
<a href="http://mail-archives.apache.org/mod_mbox/tomcat-users/">Users Mailing List</a><br/>
<a href="http://mail-archives.apache.org/mod_mbox/tomcat-dev/">Developers Mailing List</a><br/>
<a href="irc://irc.freenode.net/#tomcat">IRC</a><br/>
 
</td>
</tr>
</table>

<br/>
<table width="100%" border="1" cellspacing="0" cellpadding="3">
<tr>
<th>Examples</th>
</tr>
<tr>
<td class="menu">
<a href="jsp-examples/">JSP Examples</a><br/>
<a href="servlets-examples/">Servlet Examples</a><br/>
<a href="webdav/">WebDAV capabilities</a><br/>
 
</td>
</tr>
</table>

<br/>
<table width="100%" border="1" cellspacing="0" cellpadding="3">
<tr>
<th>Miscellaneous</th>
</tr>
<tr>
<td class="menu">
<a href="http://java.sun.com/products/jsp">Sun's Java Server Pages Site</a><br/>
```

```
<a href="http://java.sun.com/products/servlet">Sun's Servlet Site</a><br/>
 
</td>
</tr>
</table>
</td>

<td style="width:20px"> </td>

<!-- Body -->
<td align="left" valign="top">
<p id="congrats">If you're seeing this page via a web browser, it means you've setup Tomcat successfully.
Congratulations!</p>

<p>As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:</p>
<p class="code">$CATALINA_HOME/webapps/ROOT/index.jsp</p>

<p>where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't
think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an
administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the <a
href="tomcat-docs">Tomcat Documentation</a> for more detailed setup and administration information than is found in the
INSTALL file.</p>

<p><b>NOTE:</b> This page is precompiled. If you change it, this page will not change since
it was compiled into a servlet at build time.
(See <tt>$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml</tt> as to how it was mapped.)
</p>

<p><b>NOTE: For security reasons, using the administration webapp
is restricted to users with role "admin". The manager webapp
is restricted to users with role "manager".</b>
Users are defined in <code>$CATALINA_HOME/conf/tomcat-users.xml</code>.</p>

<p>Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive
documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web
applications.</p>

<p>Tomcat mailing lists are available at the Tomcat project web site:</p>

<ul>
<li><b><a href="mailto:users@tomcat.apache.org">users@tomcat.apache.org</a></b> for general questions related to
configuring and using Tomcat</li>
<li><b><a href="mailto:dev@tomcat.apache.org">dev@tomcat.apache.org</a></b> for developers working on Tomcat</li>
</ul>

<p>Thanks for using Tomcat!</p>

<p id="footer"><img src="tomcat-power.gif" width="77" height="80" alt="Powered by Tomcat"/><br/>
 

Copyright &copy; 1999-2005 Apache Software Foundation<br/>
All Rights Reserved
</p>
</td>

</tr>
</table>

</body>
</html>
```

10114 - ICMP Timestamp Request Remote Date Disclosure -

Synopsis

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

Description

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

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

Solution

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

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -13772 seconds.
```

11156 - IRC Daemon Version Detection -

Synopsis

The remote host is an IRC server.

Description

This plugin determines the version of the IRC daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/19, Modified: 2016/01/08

Plugin Output

tcp/6667/irc

```
The IRC server version is : Unreal3.2.8.1. FhiXOoE [*=2309]
```

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure -

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
Here is the browse list of the remote host :

METASPLOITABLE ( os : 0.0 )
SERVER2-31 ( os : 0.0 )
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure -

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Unix
The remote native LAN manager is : Samba 3.0.20-Debian
The remote SMB Domain Name is : METASPLOITABLE
```

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: 2021/02/11

Plugin Output

tcp/139/smb

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

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: 2021/02/11

Plugin Output

tcp/445/cifs

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

100871 - Microsoft Windows SMB Versions Supported (remote check) -

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
SMBv1
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) -

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 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: 2020/03/11

Plugin Output

tcp/445/cifs

```
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
```

10719 - MySQL Server Detection -

Synopsis

A database server is listening on the remote port.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0802

Plugin Information

Published: 2001/08/13, Modified: 2021/05/10

Plugin Output

tcp/3306/mysql

```
Version : 5.0.51a-3ubuntu5
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
CLIENT_LONG_FLAG (Get all column flags)
CLIENT_CONNECT_WITH_DB (One can specify db on connect)
CLIENT_COMPRESS (Can use compression protocol)
CLIENT_PROTOCOL_41 (New 4.1 protocol)
CLIENT_SSL (Switch to SSL after handshake)
CLIENT_TRANSACTIONS (Client knows about transactions)
CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

10437 - NFS Share Export List

Synopsis

The remote NFS server exports a list of shares.

Description

This plugin retrieves the list of NFS exported shares.

See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Solution

Ensure each share is intended to be exported.

Risk Factor

None

Plugin Information

Published: 2000/06/07, Modified: 2019/10/04

Plugin Output

tcp/2049/rpc-nfs

```
Here is the export list of 172.16.11.5 :
/ *
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/21/ftp

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/23/telnet

```
Port 23/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/53/dns

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/111/rpc-portmapper

```
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: 2021/09/16

Plugin Output

tcp/139/smb

```
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: 2021/09/16

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/512/rexecd

```
Port 512/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/513/rlogin

```
Port 513/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/514/rsh

```
Port 514/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/1099/rmi_registry

```
Port 1099/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/1524/wild_shell

```
Port 1524/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2049/rpc-nfs

```
Port 2049/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2121/ftp

```
Port 2121/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3306/mysql

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3632

```
Port 3632/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave

unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/5432/postgresql

```
Port 5432/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/5900/vnc

```
Port 5900/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/6000/x11

```
Port 6000/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/6667/irc

```
Port 6667/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8009/ajp13

```
Port 8009/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8180/www

```
Port 8180/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8787

```
Port 8787/tcp was found to be open
```

19506 - Nessus Scan Information -

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2021/09/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.0.1
Nessus build : 20287
Plugin feed version : 202111191213
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : My scan
Scan policy used : Basic Network Scan
Scanner IP : 172.16.1.200
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 23.374 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2021/11/19 9:00 Pacific Standard Time
Scan duration : 390 sec
```

11936 - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2021/09/27

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Confidence level : 95
Method : HTTP

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SSH:SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SinFP:
P1:B10113:F0x12:W5840:O0204ffff:M1460:
P2:B10113:F0x12:W5792:O0204ffff0402080affffffff4445414401030305:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:190002_7_p=2121R
SMTP:!:220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
SSLcert:!:i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple
Affairss/CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple Affairs
ed093088706603bfd5dc237399b498da2d4d31c6
i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple Affairss/CN:ubuntu804-
base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple Affairs
ed093088706603bfd5dc237399b498da2d4d31c6


The remote host is running Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
```

117886 - OS Security Patch Assessment Not Available -

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.
This does not necessarily indicate a problem with the scan.
Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

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

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

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

Plugin Output

tcp/0

```
The following issues were reported :

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

10919 - Open Port Re-check -

Synopsis

Previously open ports are now closed.

Description

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

There are several possible reasons for this :

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

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

This might be an availability problem related to the following :

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

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

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

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

Solution

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2021/07/23

Plugin Output

tcp/0

```
Port 5432 was detected as being open but is now closed
Port 25 was detected as being open but is now closed
```

50845 - OpenSSL Detection -

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

50845 - OpenSSL Detection -

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

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

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

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/5432/postgresql

48243 - PHP Version Detection -

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2020/09/22

Plugin Output

tcp/80/www

```
Nessus was able to identify the following PHP version information :

Version : 5.2.4-2ubuntu5.10
Source : X-Powered-By: PHP/5.2.4-2ubuntu5.10
```

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: 2021/11/09

Plugin Output

tcp/0

```
. You need to take the following 4 actions :

[ Apache Tomcat AJP Connector Request Injection (Ghostcat) (134862) ]

+ Action to take : Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100,
8.5.51, 9.0.31 or later.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS (139915) ]

+ Action to take : Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Samba Badlock Vulnerability (90509) ]

+ Action to take : Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.


[ UnrealIRCd Backdoor Detection (46882) ]

+ Action to take : Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.
```

118224 - PostgreSQL STARTTLS Support -

Synopsis

The remote service supports encrypting traffic.

Description

The remote PostgreSQL server supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.

See Also

https://www.postgresql.org/docs/9.2/protocol-flow.html#AEN96066
https://www.postgresql.org/docs/9.2/protocol-message-formats.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/10/19, Modified: 2021/02/24

Plugin Output

tcp/5432/postgresql

```
Here is the PostgreSQL's SSL certificate that Nessus
was able to collect after sending a pre-login packet :

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

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
15 6E 8D 30 38 F6 CA 2E 75


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

26024 - PostgreSQL Server Detection -

Synopsis

A database service is listening on the remote host.

Description

The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

See Also

https://www.postgresql.org/

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2007/09/14, Modified: 2020/11/10

Plugin Output

tcp/5432/postgresql

22227 - RMI Registry Detection -

Synopsis

An RMI registry is listening on the remote host.

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

See Also

https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html
http://www.nessus.org/u?b6fd7659

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/08/16, Modified: 2020/02/24

Plugin Output

tcp/1099/rmi_registry
tcp/1099/rmi_registry

```
Valid response recieved for port 1099:
0x00: 51 AC ED 00 05 77 0F 01 20 8A 4F A0 00 00 01 7D Q....w.. .O....}
0x10: 34 D3 4B 60 80 02 75 72 00 13 5B 4C 6A 61 76 61 4.K`..ur..[Ljava
```

```
0x20: 2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56 .lang.String;..V
0x30: E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00 ...{G...pxp....
```

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/rpc-portmapper

```
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/rpc-portmapper

```
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/2049/rpc-nfs

```
The following RPC services are available on TCP port 2049 :

- program: 100003 (nfs), version: 2
- program: 100003 (nfs), version: 3
- program: 100003 (nfs), version: 4
```

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/2049/rpc-nfs

```
The following RPC services are available on UDP port 2049 :

- program: 100003 (nfs), version: 2
- program: 100003 (nfs), version: 3
- program: 100003 (nfs), version: 4
```

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/38359/rpc-nlockmgr

```
The following RPC services are available on UDP port 38359 :

- program: 100021 (nlockmgr), version: 1
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4
```

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/38405/rpc-status

```
The following RPC services are available on TCP port 38405 :

- 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/46023/rpc-mountd

```
The following RPC services are available on UDP port 46023 :

- program: 100005 (mountd), version: 1
- program: 100005 (mountd), version: 2
- program: 100005 (mountd), version: 3
```

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/46987/rpc-nlockmgr

```
The following RPC services are available on TCP port 46987 :

- program: 100021 (nlockmgr), version: 1
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4
```

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/58818/rpc-mountd

```
The following RPC services are available on TCP port 58818 :

- program: 100005 (mountd), version: 1
- program: 100005 (mountd), version: 2
- program: 100005 (mountd), version: 3
```

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/58915/rpc-status

```
The following RPC services are available on UDP port 58915 :

- 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/rpc-portmapper

10223 - RPC portmapper Service Detection -

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

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

Solution

n/a

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0632

Plugin Information

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

Plugin Output

udp/111/rpc-portmapper

10263 - SMTP Server Detection -

Synopsis

An SMTP server is listening on the remote port.

Description

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

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

Solution

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

Risk Factor

None

References

XREF IAVT:0001-T-0932

Plugin Information

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

Plugin Output

tcp/25/smtp

```
Remote SMTP server banner :

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

42088 - SMTP Service STARTTLS Command Support -

Synopsis

The remote mail service supports encrypting traffic.

Description

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

See Also

https://en.wikipedia.org/wiki/STARTTLS
https://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

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

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

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain
```

```
Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
15 6E 8D 30 38 F6 CA 2E 75

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

70657 - SSH Algorithms and Languages Supported -

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1

The server supports the following options for server_host_key_algorithms :

ssh-dss
ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

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

The server supports the following options for encryption_algorithms_server_to_client :

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

The server supports the following options for mac_algorithms_client_to_server :

hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

none
zlib@openssh.com
```

```
The server supports the following options for compression_algorithms_server_to_client :

none
zlib@openssh.com
```

149334 - SSH Password Authentication Accepted -

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported -

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

- 1.99
- 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled -

Synopsis

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

Description

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2021/09/23

Plugin Output

tcp/22/ssh

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

hmac-sha1
hmac-sha1-96

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

hmac-sha1
hmac-sha1-96
```

10267 - SSH Server Type and Version Information -

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

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

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SSH supported authentication : publickey,password
```

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

```
This port supports SSLv2/SSLv3/TLSv1.0.
```

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/5432/postgresql

```
This port supports 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: 2021/03/09

Plugin Output

tcp/25/smtp

```
The host name known by Nessus is :

metasploitable

The Common Name in the certificate is :

ubuntu804-base.localdomain
```

45410 - SSL Certificate 'commonName' Mismatch -

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/5432/postgresql

```
The host name known by Nessus is :

metasploitable

The Common Name in the certificate is :

ubuntu804-base.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: 2021/02/03

Plugin Output

tcp/25/smtp

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D 4D 31 C6
MD5 Fingerprint: DC D9 AD 90 6C 8F 2F 73 74 AF 38 3B 25 40 88 28


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDWzCCAsQCCQD6+TpMf7a5zDANBgkqhkiG9w0BAQUFADCB8TELMAkGA1UEBhMCWFgxKjAoBgNVBAgTIVRoZXJlIGlzIG5vIHN1Y2ggdGhpbmcgb3V0c2lkZSBVUzETMBEGA1UEBxMKRXZlcnl3aGVyZTEOMAwGA1l
-----END CERTIFICATE-----
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/5432/postgresql

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D 4D 31 C6
MD5 Fingerprint: DC D9 AD 90 6C 8F 2F 73 74 AF 38 3B 25 40 88 28


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDWzCCAsQCQD6+TpMf7a5zDANBgkqhkiG9w0BAQUFADCB8TELMAkGA1UEBhMCWFgxKjAoBgNVBAgTIVRoZXJlIGlzIG5vIHN1Y2ggdGhpbmcgb3V0c2lkZSBVUzETMBEGA1UEBxMKRXZlcnl3aGVyZTEOMAwGA1l
-----END CERTIFICATE-----
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

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

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-RC2-CBC-MD5 0x04, 0x00, 0x80 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1

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

```
Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
DES-CBC3-MD5 0x07, 0x00, 0xC0 RSA RSA 3DES-CBC(168) MD5
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1

The fields above are :

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

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/5432/postgresql

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

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

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1

The fields above are :

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

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

```
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)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1

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

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1


SSL Version : SSLv3
Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1

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

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1


SSL Version : SSLv2
Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EXP-RC2-CBC-MD5 0x04, 0x00, 0x80 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x02, 0x00, 0x80 RSA(512) RSA RC4(40) MD5 export

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

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DES-CBC3-MD5 0x07, 0x00, 0xC0 RSA RSA 3DES-CBC(168) MD5

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
RC4-MD5 0x01, 0x00, 0x80 RSA RSA RC4(128) MD5

The fields above are :

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

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

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/5432/postgresql

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

SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1


SSL Version : SSLv3
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

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

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

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

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1

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

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1

The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/5432/postgresql

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

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

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1

The fields above are :

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

51891 - SSL Session Resume Supported -

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/25/smtp

```
This port supports resuming SSLv3 sessions.
```

25240 - Samba Server Detection -

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

https://www.samba.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

104887 - Samba Version -

Synopsis

It was possible to obtain the samba version from the remote operating system.

Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/11/30, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote Samba Version is : Samba 3.0.20-Debian
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) -

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/21/ftp

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/22/ssh

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/23/telnet

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/25/smtp

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/80/www

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/1524/wild_shell

```
A shell server (Metasploitable) is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/2121/ftp

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/5900/vnc

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/8180/www

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

17975 - Service Detection (GET request) -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0935

Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

Plugin Output

tcp/6667/irc

```
An IRC daemon is listening on this port.
```

11153 - Service Detection (HELP Request) -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3306/mysql

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

25220 - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

11819 - TFTP Daemon Detection -

Synopsis

A TFTP server is listening on the remote port.

Description

The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and diskless hosts to retrieve their configuration. It can also be used by worms to propagate.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 2003/08/13, Modified: 2019/11/22

Plugin Output

udp/69/tftp

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided -

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2021/08/30

Plugin Output

tcp/0

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

10281 - Telnet Server Detection -

Synopsis

A Telnet server is listening on the remote port.

Description

The remote host is running a Telnet server, a remote terminal server.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2020/06/12

Plugin Output

tcp/23/telnet

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
 _ _ _ _ _ _ ____
 _ __ ___ ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
------------------------------ snip ------------------------------
```

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 172.16.1.200 to 172.16.11.5 :
172.16.1.200
172.16.1.1
172.16.11.5

Hop Count: 2
```

11154 - Unknown Service Detection: Banner Retrieval -

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/07/24

Plugin Output

tcp/8787

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

Port : 8787
Type : get_http
Banner :
0x0000: 00 00 00 03 04 08 46 00 00 03 A1 04 08 6F 3A 16 ......F......o:.
0x0010: 44 52 62 3A 3A 44 52 62 43 6F 6E 6E 45 72 72 6F DRb::DRbConnErro
0x0020: 72 07 3A 07 62 74 5B 17 22 2F 2F 75 73 72 2F 6C r.:.bt[."//usr/l
0x0030: 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F ib/ruby/1.8/drb/
0x0040: 64 72 62 2E 72 62 3A 35 37 33 3A 69 6E 20 60 6C drb.rb:573:in `l
0x0050: 6F 61 64 27 22 37 2F 75 73 72 2F 6C 69 62 2F 72 oad'"7/usr/lib/r
0x0060: 75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2E uby/1.8/drb/drb.
0x0070: 72 62 3A 36 31 32 3A 69 6E 20 60 72 65 63 76 5F rb:612:in `recv_
0x0080: 72 65 71 75 65 73 74 27 22 37 2F 75 73 72 2F 6C request'"7/usr/l
0x0090: 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F ib/ruby/1.8/drb/
0x00A0: 64 72 62 2E 72 62 3A 39 31 31 3A 69 6E 20 60 72 drb.rb:911:in `r
0x00B0: 65 63 76 5F 72 65 71 75 65 73 74 27 22 3C 2F 75 ecv_request'"</u
0x00C0: 73 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F sr/lib/ruby/1.8/
0x00D0: 64 72 62 2F 64 72 62 2E 72 62 3A 31 35 33 30 3A drb/drb.rb:1530:
0x00E0: 69 6E 20 60 69 6E 69 74 5F 77 69 74 68 5F 63 6C in `init_with_cl
0x00F0: 69 65 6E 74 27 22 39 2F 75 73 72 2F 6C 69 62 2F ient'"9/usr/lib/
0x0100: 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 ruby/1.8/drb/drb
0x0110: 2E 72 62 3A 31 35 34 32 3A 69 6E 20 60 73 65 74 .rb:1542:in `set
0x0120: 75 70 5F 6D 65 73 73 61 67 65 27 22 33 2F 75 73 up_message'"3/us
0x0130: 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 r/lib/ruby/1.8/d
0x0140: 72 62 2F 64 72 62 2E 72 62 3A 31 34 39 34 3A 69 rb/drb.rb:1494:i
0x0150: 6E 20 60 70 65 72 66 6F 72 6D 27 22 35 2F 75 73 n `perform'"5/us
```

```
0x0160: 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 r/lib/ruby/1.8/d
0x0170: 72 62 2F 64 72 62 2E 72 62 3A 31 35 38 39 3A 69 rb/drb.rb:1589:i
0x0180: 6E 20 60 6D 61 69 6E 5F 6C 6F 6F 70 27 22 30 2F n `main_loop'"0/
0x0190: 75 73 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 usr/lib/ruby/1.8
0x01A0: 2F 64 72 62 2F 64 72 62 2E 72 62 3A 31 35 38 35 /drb/drb.rb:1585
0x01B0: 3A 69 6E 20 60 6C 6F 6F 70 27 22 35 2F 75 73 72 :in `loop'"5/usr
0x01C0: 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 /lib/ruby/1.8/dr
0x01D0: 62 2F 64 72 62 2E 72 62 3A 31 35 38 35 3A 69 6E b/drb.rb:1585:in
0x01E0: 20 60 6D 61 69 6E 5F 6C 6F 6F 70 27 22 31 2F 75 `main_loop'"1/u
0x01F0: 73 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F sr/lib/ruby/1.8/
0x0200: 64 72 62 2F 64 72 62 2E 72 62 3A 31 35 38 31 3A drb/drb.rb:1581:
0x0210: 69 6E 20 60 73 74 61 72 74 27 22 35 2F 75 73 72 in `start'"5/usr
0x0220: 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 /lib/ruby/1.8/dr
0x0230: 62 2F 64 72 62 2E 72 62 3A 31 35 38 31 3A 69 6E b/drb.rb:1581:in
0x0240: 20 60 6D 61 69 6E 5F 6C 6F 6F 70 27 22 2F 2F 75 `main_loop'"//u
0x0250: 73 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F sr/lib/ruby/1.8/
0x0260: 64 72 62 2F 64 72 62 2E 72 62 3A 31 34 33 30 3A drb/drb.rb:1430:
0x0270: 69 6E 20 60 72 75 6E 27 22 31 2F 75 73 72 2F 6C in `run'"1/usr/l
0x0280: 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F ib/ruby/1.8/drb/
0x0290: 64 72 62 2E 72 62 3A 31 34 32 37 3A 69 6E 20 60 drb.rb:1427:in `
0x02A0: 73 74 61 72 74 27 22 2F 2F 75 73 72 2F 6C 69 62 start'"//usr/lib
0x02B0: 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 /ruby/1.8/drb/dr
0x02C0: 62 2E 72 62 3A 31 34 32 37 3A 69 6E 20 60 72 75 b.rb:1427:in `ru
0x02D0: 6E 27 22 36 2F 75 73 72 2F 6C 69 62 2F 72 75 62 n'"6/usr/lib/rub
0x02E0: 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2E 72 62 y/1.8/drb/drb.rb
0x02F0: 3A 31 33 34 37 3A 69 6E 20 60 69 6E 69 74 69 61 :1347:in `initia
0x0300: 6C 69 7A 65 27 22 2F 2F 75 73 72 2F 6C 69 62 2F lize'"//usr/lib/
0x0310: 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 ruby/1.8/drb/drb
0x0320: 2E 72 62 3A 31 36 32 37 3A 69 6E 20 60 6E 65 77 .rb:1627:in `new
0x0330: 27 22 39 2F 75 73 72 2F 6C 69 62 2F 72 75 62 79 '"9/usr/lib/ruby
0x0340: 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2E 72 62 3A /1.8/drb/drb.rb:
0x0350: 31 36 32 37 3A 69 6E 20 60 73 74 61 72 74 5F 73 1627:in `start_s
0x0360: 65 72 76 69 63 65 27 22 25 2F 75 73 72 2F 73 62 ervice'"%/usr/sb
0x0370: 69 6E 2F 64 72 75 62 79 5F 74 69 6D 65 73 65 72 in/druby_timeser
0x0380: 76 65 72 2E 72 62 3A 31 32 3A 09 6D 65 73 67 22 ver.rb:12:.mesg"
0x0390: 20 74 6F 6F 20 6C 61 72 67 65 20 70 61 63 6B 65 too large packe
0x03A0: 74 20 31 31 39 35 37 32 35 38 35 36 t 1195725856
```

19288 - VNC Server Security Type Detection -

Synopsis

A VNC server is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types'.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/07/22, Modified: 2021/07/13

Plugin Output

tcp/5900/vnc

```
\nThe remote VNC server chose security type #2 (VNC authentication)
```

65792 - VNC Server Unencrypted Communication Detection -

Synopsis

A VNC server with one or more unencrypted 'security-types' is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/03, Modified: 2014/03/12

Plugin Output

tcp/5900/vnc

```
The remote VNC server supports the following security type
which does not perform full data communication encryption :

2 (VNC authentication)
```

10342 - VNC Software Detection -

Synopsis

The remote host is running a remote display software (VNC).

Description

The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.

See Also

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

Solution

Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port.

Risk Factor

None

Plugin Information

Published: 2000/03/07, Modified: 2017/06/12

Plugin Output

tcp/5900/vnc

```
The highest RFB protocol version supported by the server is :

3.3
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2021/11/12

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

20108 - Web Server / Application favicon.ico Vendor Fingerprinting

Synopsis

The remote web server contains a graphic image that is prone to information disclosure.

Description

The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

Solution

Remove the 'favicon.ico' file or create a custom one for your site.

Risk Factor

None

Plugin Information

Published: 2005/10/28, Modified: 2020/06/12

Plugin Output

tcp/8180/www

```
MD5 fingerprint : 4644f2d45601037b8423d45e13194c93
Web server : Apache Tomcat or Alfresco Community
```

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/8180/www

```
The default welcome page is from Tomcat.
```

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/80/www

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: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 5 NetBIOS names have been gathered :

METASPLOITABLE = Computer name
METASPLOITABLE = Messenger Service
METASPLOITABLE = File Server Service
WORKGROUP = Workgroup / Domain name
WORKGROUP = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

52703 - vsftpd Detection

Synopsis

An FTP server is listening on the remote port.

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

http://vsftpd.beasts.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/03/17, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
Source : 220 (vsFTPd 2.3.4)
Version : 2.3.4
```

172.16.11.8

4	6	19	0	80
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Fri Nov 19 09:00:27 2021
End time:	Fri Nov 19 09:07:00 2021

Host Information

Netbios Name:	S08
IP:	172.16.11.8
MAC Address:	00:50:56:AE:47:3F
OS:	Microsoft Windows Server 2008 Standard Service Pack 1

Vulnerabilities

40887 - MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (EDUCATEDSCHOLAR) (uncredentialed check) -

Synopsis

Arbitrary code may be executed on the remote host through the SMB port

Description

The remote host is running a version of Microsoft Windows Vista or Windows Server 2008 that contains a vulnerability in its SMBv2 implementation. An attacker can exploit this flaw to disable the remote host or to execute arbitrary code on it.

EDUCATEDSCHOLAR is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers.

See Also

http://www.nessus.org/u?0f72ec72
http://www.nessus.org/u?3e7748a1

Solution

Microsoft has released a patch for Windows Vista and Windows Server 2008.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	36299
BID	36594
CVE	CVE-2009-2532
CVE	CVE-2009-3103
MSKB	975497
XREF	MSFT:MS09-050
XREF	CERT:135940
XREF	EDB-ID:9594
XREF	EDB-ID:10005
XREF	EDB-ID:12524
XREF	EDB-ID:14674
XREF	EDB-ID:16363
XREF	CWE:94
XREF	CWE:399

Exploitable With

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

Plugin Information

Published: 2009/09/08, Modified: 2019/11/26

Plugin Output

tcp/445/cifs

```
Sent:
0000009dff534d4272000000001853c801000000000000000000000000000000000000007a0002
54454e41424c455f4e4554574f524b5f534543555249545900024c414e4d414e312e30000257696e
646f777320666f7220576f726b67726f7570732e316100024c4d312e325830303200024c414e
4d414e322e3100024e54204c4d20302e31320002534d4220322e3030320002534d4220322e3f3f3f
00

Received:
ff534d42720000000d0000c0010000000100000000000000000000000000000007a000254454e41
424c455f4e4554574f524b5f534543555249545900024c4109000000000000002
```

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 web server if it is no longer needed. Otherwise, upgrade to a supported 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 v2.0 Base Score

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

References

XREF	IAVA:0001-A-0617

Plugin Information

Published: 2008/10/21, Modified: 2021/11/17

Plugin Output

tcp/80/www

```
Product : Microsoft IIS 7.0
Server response header : Microsoft-IIS/7.0
Support ended : 2020-01-14
Supported versions : Microsoft IIS 8.5 / 8.0
Additional information : http://www.nessus.org/u?376a720e
```

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 web server if it is no longer needed. Otherwise, upgrade to a supported 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 v2.0 Base Score

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

References

XREF IAVA:0001-A-0617

Plugin Information

Published: 2008/10/21, Modified: 2021/11/17

Plugin Output

tcp/443/www

```
Product : Microsoft IIS 7.0
Server response header : Microsoft-IIS/7.0
Support ended : 2020-01-14
Supported versions : Microsoft IIS 8.5 / 8.0
Additional information : http://www.nessus.org/u?376a720e
```

108797 - Unsupported Windows OS (remote) -

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

https://support.microsoft.com/en-us/lifecycle

Solution

Upgrade to a supported service pack or operating system

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0501

Plugin Information

Published: 2018/04/03, Modified: 2020/09/22

Plugin Output

tcp/0

```
The following Windows version is installed and not supported:

Microsoft Windows Server 2008 Standard Service Pack 1
```

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) -

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

http://www.nessus.org/u?68fc8eff
http://www.nessus.org/u?321523eb
http://www.nessus.org/u?065561d0
http://www.nessus.org/u?d9f569cf
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
http://www.nessus.org/u?b9d9ebf9
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3
https://github.com/stamparm/EternalRocks/
http://www.nessus.org/u?59db5b5b

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212
MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065

Exploitable With

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

Plugin Information

Published: 2017/03/20, Modified: 2020/10/15

Plugin Output

tcp/445/cifs

```
Sent:
00000054ff534d4225000000001803c800000000000000000000000049866320100000110000000
00ffffffff000000000000000000000005400000054000200230000001100005c00500049005000
45005c0000000000

Received:
ff534d4225050200c09803c8000000000000000000000000498663201000001000000
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm -

Synopsis

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

Description

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

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

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

See Also

https://tools.ietf.org/html/rfc3279
http://www.nessus.org/u?9bb87bf2
http://www.nessus.org/u?e120eea1
http://www.nessus.org/u?5d894816
http://www.nessus.org/u?51db68aa
http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	11849
BID	33065

CVE CVE-2004-2761
XREF CERT:836068
XREF CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2020/04/27

Plugin Output

tcp/443/www

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

|-Subject : CN=WIN-6CLCZAW0GON
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : Apr 04 16:09:50 2016 GMT
|-Valid To : Apr 04 00:00:00 2026 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 SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

Published: 2009/01/05, Modified: 2020/04/27

Plugin Output

tcp/3389/msrdp

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

|-Subject : CN=s08
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : Oct 05 16:02:50 2021 GMT
|-Valid To : Apr 06 16:02:50 2022 GMT
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

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

Description

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

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

Plugin Output

tcp/443/www

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

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
DES-CBC3-MD5 0x07, 0x00, 0xC0 RSA RSA 3DES-CBC(168) MD5
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

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

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

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

Description

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

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

Plugin Output

tcp/3389/msrdp

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

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

The fields above are :

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

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 1.2 (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 v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/443/www

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

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

Name Code KEX Auth Encryption MAC
---------------------------------- ---------- --- ---- --------------------- ---
DES-CBC3-MD5 RSA RSA 3DES-CBC(168) MD5

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------------------- ---------- --- ---- --------------------- ---
RC4-MD5 RSA RSA RC4(128) MD5

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={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


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

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

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA ECDH RSA AES-CBC(256) SHA1
AES128-SHA RSA RSA AES-CBC(128) SHA1
AES256-SHA RSA RSA AES-CBC(256) SHA1
RC4-MD5 RSA RSA RC4(128) MD5
RC4-SHA RSA RSA RC4(128) SHA1

The fields above are :

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

10061 - Echo Service Detection -

Synopsis

An echo service is running on the remote host.

Description

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

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

Solution

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

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

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

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

- Under Windows systems, set the following registry key to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho

Then launch cmd.exe and type :

net stop simptcp net start simptcp

To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0103
CVE	CVE-1999-0635

Plugin Information

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

Plugin Output

tcp/7/echo

10061 - Echo Service Detection -

Synopsis

An echo service is running on the remote host.

Description

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

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

Solution

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

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

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

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

- Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho

Then launch cmd.exe and type :

net stop simptcp net start simptcp

To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0103
CVE	CVE-1999-0635

Plugin Information

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

Plugin Output

udp/7

63643 - MS13-006: Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220) (uncredentialed check) -

Synopsis

The remote host is affected by a security feature bypass vulnerability.

Description

The remote host contains a flaw in the handling of SSL version 3 (SSLv3) and TLS (Transport Layer Security) protocols. An attacker can inject specially crafted content into an SSL/TLS session, which could allow an attacker to bypass security features of SSLv3 and TLS protocols in order to intercept communications.

Note that this plugin only tests Microsoft IIS HTTPS and TLS-capable FTP servers, which are known to use MS13-006 update files. Other SSL/TLS implementations may also be affected. To test all SSL/TLS services Nessus finds, configure the 'Report paranoia' preference setting to 'Paranoid (more false alarms).'

See Also

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2013/ms13-006

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, and 2012.

For other SSL/TLS implementations, contact the vendor for updates.

Risk Factor

Medium

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

BID	57144
CVE	CVE-2013-0013
MSKB	2785220
XREF	MSFT:MS13-006
XREF	IAVB:2013-B-0003

Plugin Information

Published: 2013/01/22, Modified: 2021/10/25

Plugin Output

tcp/443/www

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) -

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

http://www.nessus.org/u?52ade1e9
http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

BID	86002
CVE	CVE-2016-0128
MSKB	3148527
MSKB	3149090
MSKB	3147461
MSKB	3147458
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

Plugin Information

Published: 2016/04/13, Modified: 2019/07/23

Plugin Output

tcp/49155/dce-rpc

10198 - Quote of the Day (QOTD) Service Detection -

Synopsis

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

Description

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

Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17.
When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).

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

Solution

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0103

Plugin Information

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

Plugin Output

tcp/17/qotd

10198 - Quote of the Day (QOTD) Service Detection -

Synopsis

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

Description

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

Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17.
When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).

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

Solution

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0103

Plugin Information

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

Plugin Output

udp/17/qotd

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

http://www.nessus.org/u?df39b8b3
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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

Plugin Information

Published: 2012/01/19, Modified: 2021/03/15

Plugin Output

tcp/445/cifs

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/443/www

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

|-Subject : CN=WIN-6CLCZAW0GON
|-Issuer : CN=WIN-6CLCZAW0GON
```

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/3389/msrdp

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

|-Subject : CN=s08
|-Issuer : CN=s08
```

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 SSL 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 v2.0 Base Score

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

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/443/www

```
The identities known by Nessus are :
```

```
172.16.11.8
172.16.11.8

The Common Name in the certificate is :

WIN-6CLCZAW0GON
```

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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	83733
CVE	CVE-2016-0800
XREF	CERT:583776

Plugin Information

Published: 2016/03/01, Modified: 2019/11/20

Plugin Output

tcp/443/www

```
The remote host is affected by SSL DROWN and supports the following
vulnerable cipher suites :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- --------------------- ---
RC4-MD5 0x01, 0x00, 0x80 RSA RSA RC4(128) MD5

The fields above are :

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

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

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

See Also

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/443/www

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

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
RC4-MD5 0x01, 0x00, 0x80 RSA RSA RC4(128) MD5
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

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

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

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

See Also

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

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

High Strength Ciphers (>= 112-bit key)

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

The fields above are :

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

57582 - SSL Self-Signed Certificate -

Synopsis

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

Description

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/443/www

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

|-Subject : CN=WIN-6CLCZAW0GON
```

57582 - SSL Self-Signed Certificate -

Synopsis

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

Description

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/3389/msrdp

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

|-Subject : CN=s08
```

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 v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/443/www

```
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.
```

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/443/www

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

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/3389/msrdp

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

42263 - Unencrypted Telnet Server -

Synopsis

The remote Telnet server transmits traffic in cleartext.

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2009/10/27, Modified: 2020/06/12

Plugin Output

tcp/23/telnet

```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------

No more connections are allowed to telnet server. Please try again later.
------------------------------ snip ------------------------------
```

45590 - Common Platform Enumeration (CPE) -

Synopsis

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

Description

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

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

See Also

http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2021/11/08

Plugin Output

tcp/0

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

cpe:/o:microsoft:windows_server_2008::sp1

Following application CPE's matched on the remote system :

cpe:/a:microsoft:iis:7.0 -> Microsoft Internet Information Services (IIS) 7.0
x-cpe:/a:microsoft:uddi_services:6.0.6001.18000
```

10736 - DCE Services Enumeration -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/135/epmap

```
The following DCERPC services are available locally :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : dsrole
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : securityevent

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : audit

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : LRPC-25ee7fb66a5e08e68f

Object UUID : 00736665-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Local RPC service
Named pipe : tapsrvlpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Local RPC service
Named pipe : unimdmsvc

Object UUID : 7a93abbc-ca68-4210-a846-4215f982bc52
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-3ede6b71bcf3335107

Object UUID : c4e50661-b7aa-442c-a1dc-ebdfbb4b69bb
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-3ede6b71bcf3335107

Object UUID : b2ac3109-d39d-4f5c-a7a4-3c3bd3e774fb
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-3ede6b71bcf3335107

Object UUID : cf463a82-3630-4c49-aed0-17bd545c93e0
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-3ede6b71bcf3335107

Object UUID : bc5f7930-4000-4bab-86b8-64b3f9222b71
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : OLED82D1AC553B74E428C4A0E472C3D

Object UUID : bc5f7930-4000-4bab-86b8-64b3f9222b71
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-5d524ffdcb7cda387f

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 45f52c28-7f9f-101a-b52b-08002b2efabe, version 1.0
Description : Wins Service
Windows process : wins.exe
Type : Local RPC service
Named pipe : OLE8F099131730F4F97A3ED2BBB7A65

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 45f52c28-7f9f-101a-b52b-08002b2efabe, version 1.0
Description : Wins Service
Windows process : wins.exe
Type : Local RPC service
Named pipe : LRPC-8d7a28417c4fdb323a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 811109bf-a4e1-11d1-ab54-00a0c91e9b45, version 1.0
Description : Wins Service
Windows process : wins.exe
Type : Local RPC service
Named pipe : OLE8F099131730F4F97A3ED2BBB7A65

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 811109bf-a4e1-11d1-ab54-00a0c91e9b45, version 1.0
Description : Wins Service
Windows process : wins.exe
Type : Local RPC service
Named pipe : LRPC-8d7a28417c4fdb323a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Local RPC service
Named pipe : LRPC-1194813f0c1b18120a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Annotation : Spooler base remote object endpoint
```

```
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd490425-5325-4565-b774-7e27d6c09c24, version 1.0
Description : Unknown RPC service
Annotation : Base Firewall Engine API
Type : Local RPC service
Named pipe : LRPC-3b62506bb5aa304eef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-3b62506bb5aa304eef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-3b62506bb5aa304eef

Object UUID : 3bdb59a0-d736-4d44-9074-c1ee00000001
UUID : 24019106-a203-4642-b88d-82dae9158929, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-7b8b5939481df82946

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : OLED258FBE2E4A746FB82FBB5EAB420

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : LRPC-3f3a06b25fed56269c

Object UUID : 666f7270-6c69-7365-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE7331F20B9BE3466187357EDDA6F8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE7331F20B9BE3466187357EDDA6F8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE7331F20B9BE3466187357EDDA6F8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7331F20B9BE3466187357EDDA6F8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service
Named pipe : OLE7331F20B9BE3466187357EDDA6F8

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : OLE7331F20B9BE3466187357EDDA6F8

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : SECLOGON

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7331F20B9BE3466187357EDDA6F8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : SECLOGON

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7d814569-35b3-4850-bb32-83035fcebf6e, version 1.0
Description : Unknown RPC service
Annotation : IAS RPC server
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7d814569-35b3-4850-bb32-83035fcebf6e, version 1.0
Description : Unknown RPC service
Annotation : IAS RPC server
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7d814569-35b3-4850-bb32-83035fcebf6e, version 1.0
Description : Unknown RPC service
Annotation : IAS RPC server
Type : Local RPC service
Named pipe : OLE7331F20B9BE3466187357EDDA6F8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7d814569-35b3-4850-bb32-83035fcebf6e, version 1.0
Description : Unknown RPC service
Annotation : IAS RPC server
Type : Local RPC service
Named pipe : SECLOGON

Object UUID : 6c637067-6569-746e-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-b9dd979da941b0ca57
```

```
Object UUID : 24d1f7c7-76af-4f28-9ccd-7f6cb6468601
UUID : 2eb08e3e-639f-4fba-97b1-14f878961076, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b9dd979da941b0ca57

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc6

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0176B91

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-65c3201fb68dd6c362

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0176C90

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0176C90

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 00736665-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-25ee7fb66a5e08e68f

Object UUID : 00736665-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : audit

Object UUID : 00736665-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : securityevent

Object UUID : 00736665-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00736665-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : dsrole
```

10736 - DCE Services Enumeration -

Synopsis

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

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services

running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/445/cifs

```
The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\tapsrv
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 45f52c28-7f9f-101a-b52b-08002b2efabe, version 1.0
Description : Wins Service
Windows process : wins.exe
Type : Remote RPC service
Named pipe : \pipe\WinsPipe
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 811109bf-a4e1-11d1-ab54-00a0c91e9b45, version 1.0
Description : Wins Service
Windows process : wins.exe
Type : Remote RPC service
Named pipe : \pipe\WinsPipe
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
Named pipe : \pipe\spoolss
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Annotation : Spooler base remote object endpoint
Type : Remote RPC service
Named pipe : \pipe\spoolss
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
Named pipe : \pipe\spoolss
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
Named pipe : \pipe\spoolss
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S08

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S08

Object UUID : 73736573-6f69-656e-6e76-000000000000
```

```
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7d814569-35b3-4850-bb32-83035fcebf6e, version 1.0
Description : Unknown RPC service
Annotation : IAS RPC server
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7d814569-35b3-4850-bb32-83035fcebf6e, version 1.0
Description : Unknown RPC service
Annotation : IAS RPC server
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\S08

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\S08

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\S08

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\S08

Object UUID : 00736665-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\S08

Object UUID : 00736665-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\S08
```

10736 - DCE Services Enumeration -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/49152/dce-rpc

```
The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 172.16.11.8
```

10736 - DCE Services Enumeration -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/49153/dce-rpc

```
The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 172.16.11.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 172.16.11.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 172.16.11.8
```

10736 - DCE Services Enumeration -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/49154/dce-rpc

```
The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 172.16.11.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49154
IP : 172.16.11.8

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49154
IP : 172.16.11.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 172.16.11.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7d814569-35b3-4850-bb32-83035fcebf6e, version 1.0
Description : Unknown RPC service
Annotation : IAS RPC server
Type : Remote RPC service
TCP Port : 49154
IP : 172.16.11.8
```

10736 - DCE Services Enumeration -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/49155/dce-rpc

```
The following DCERPC services are available on TCP port 49155 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 172.16.11.8
```

10736 - DCE Services Enumeration -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/49156/dce-rpc

```
The following DCERPC services are available on TCP port 49156 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
TCP Port : 49156
IP : 172.16.11.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Annotation : Spooler base remote object endpoint
Type : Remote RPC service
TCP Port : 49156
IP : 172.16.11.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
TCP Port : 49156
IP : 172.16.11.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Remote RPC service
TCP Port : 49156
IP : 172.16.11.8
```

10736 - DCE Services Enumeration -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/49157/dce-rpc

```
The following DCERPC services are available on TCP port 49157 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
```

```
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49157
IP : 172.16.11.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Remote RPC service
TCP Port : 49157
IP : 172.16.11.8
```

10736 - DCE Services Enumeration -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/49174/dce-rpc

```
The following DCERPC services are available on TCP port 49174 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 45f52c28-7f9f-101a-b52b-08002b2efabe, version 1.0
Description : Wins Service
Windows process : wins.exe
Type : Remote RPC service
TCP Port : 49174
IP : 172.16.11.8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 811109bf-a4e1-11d1-ab54-00a0c91e9b45, version 1.0
Description : Wins Service
Windows process : wins.exe
Type : Remote RPC service
TCP Port : 49174
IP : 172.16.11.8
```

10736 - DCE Services Enumeration -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/49175/dce-rpc

```
The following DCERPC services are available on TCP port 49175 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49175
IP : 172.16.11.8
```

10052 - Daytime Service Detection -

Synopsis

A daytime service is running on the remote host.

Description

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

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

Solution

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

- On Windows systems, set the following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Next, launch cmd.exe and type :

net stop simptcp net start simptcp This will restart the service.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/13/daytime

10052 - Daytime Service Detection -

Synopsis

A daytime service is running on the remote host.

Description

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

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

Solution

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

- On Windows systems, set the following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Next, launch cmd.exe and type :

net stop simptcp net start simptcp This will restart the service.

Risk Factor

None

Plugin Information

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

Plugin Output

udp/13/daytime

132634 - Deprecated SSLv2 Connection Attempts -

Synopsis

Secure Connections, using a deprecated protocol were attempted as part of the scan

Description

This plugin enumerates and reports any SSLv2 connections which were attempted as part of a scan. This protocol has been deemed prohibited since 2011 because of security vulnerabilities and most major ssl libraries such as openssl, nss, mbed and wolfssl do not provide this functionality in their latest versions. This protocol has been deprecated in Nessus 8.9 and later.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/01/06, Modified: 2020/01/06

Plugin Output

tcp/0

```
Nessus attempted the following SSLv2 connection(s) as part of this scan:

Plugin ID: 34947
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 35556
Timestamp: 2021-11-19 17:05:25
Port: 443

Plugin ID: 11393
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 20337
Timestamp: 2021-11-19 17:05:25
Port: 443

Plugin ID: 18047
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 85380
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 34946
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 20968
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 21220
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 20893
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 10844
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 29306
Timestamp: 2021-11-19 17:05:25
Port: 443

Plugin ID: 97610
Timestamp: 2021-11-19 17:05:26
Port: 443
```

```
Plugin ID: 25458
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 102918
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 38208
Timestamp: 2021-11-19 17:05:25
Port: 443

Plugin ID: 121479
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 18540
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 15910
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 25546
Timestamp: 2021-11-19 17:05:25
Port: 443

Plugin ID: 73203
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 39590
Timestamp: 2021-11-19 17:05:25
Port: 443

Plugin ID: 33928
Timestamp: 2021-11-19 17:05:25
Port: 443

Plugin ID: 11008
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 23780
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 38199
Timestamp: 2021-11-19 17:05:26
Port: 443

Plugin ID: 19781
Timestamp: 2021-11-19 17:05:25
Port: 443

Plugin ID: 27818
Timestamp: 2021-11-19 17:05:25
Port: 443
```

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 : 99
```

11367 - Discard Service Detection -

Synopsis

A discard service is running on the remote host.

Description

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

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

Solution

- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry key to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/9/discard

35716 - Ethernet Card Manufacturer Detection -

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

https://standards.ieee.org/faqs/regauth.html
http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:50:56:AE:47:3F : VMware, Inc.
```

86420 - Ethernet MAC Addresses -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
- 00:50:56:AE:47:3F
```

84502 - HSTS Missing From HTTPS Server -

Synopsis

The remote web server is not enforcing HSTS.

Description

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

See Also

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

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

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/www

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

- HTTP methods GET HEAD POST TRACE OPTIONS 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/www

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

- HTTP methods GET HEAD POST TRACE OPTIONS are allowed on :

/
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/80/www

```
The remote web server type is :

Microsoft-IIS/7.0
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/443/www

```
The remote web server type is :

Microsoft-IIS/7.0
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :

Content-Type: text/html
Last-Modified: Mon, 04 Apr 2016 16:36:45 GMT
Accept-Ranges: bytes
ETag: "7b44d2d908ed11:0"
Server: Microsoft-IIS/7.0
X-Powered-By: ASP.NET
Date: Fri, 19 Nov 2021 12:50:32 GMT
Content-Length: 133

Response Body :

Welcome to the Unsecured Web Page<br>
<br>

Do you wish to go secure?<br>
<a href="https://172.16.11.8/admin">Secure Page</a><br>
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :

Content-Type: text/html
Last-Modified: Mon, 04 Apr 2016 16:36:45 GMT
Accept-Ranges: bytes
ETag: "7b44d2d908ed11:0"
Server: Microsoft-IIS/7.0
X-Powered-By: ASP.NET
Date: Fri, 19 Nov 2021 12:50:32 GMT
Content-Length: 133

Response Body :

Welcome to the Unsecured Web Page<br>
<br>

Do you wish to go secure?<br>
```

```
<a href="https://172.16.11.8/admin">Secure Page</a><br>
```

10114 - ICMP Timestamp Request Remote Date Disclosure -

Synopsis

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

Description

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

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

Solution

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

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

icmp/0

```
The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is 14284 seconds.
```

85381 - Microsoft UDDI Services Detection -

Synopsis

Microsoft UDDI Services is running on the remote host.

Description

The remote web server is running Microsoft Universal Description, Discovery, and Integration (UDDI) Services, a web application that enables discovery of XML web services.

See Also

https://msdn.microsoft.com/en-us/library/Cc730814.aspx

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/08/13, Modified: 2021/10/19

Plugin Output

tcp/80/www

```
URL : http://172.16.11.8/uddipublic
Version : 6.0.6001.18000
```

85381 - Microsoft UDDI Services Detection -

Synopsis

Microsoft UDDI Services is running on the remote host.

Description

The remote web server is running Microsoft Universal Description, Discovery, and Integration (UDDI) Services, a web application that enables discovery of XML web services.

See Also

https://msdn.microsoft.com/en-us/library/Cc730814.aspx

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/08/13, Modified: 2021/10/19

Plugin Output

tcp/443/www

```
URL : https://172.16.11.8/uddipublic
Version : 6.0.6001.18000
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure -

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows Server (R) 2008 Standard 6001 Service Pack 1
The remote native LAN manager is : Windows Server (R) 2008 Standard 6.0
The remote SMB Domain Name is : S08
```

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry -

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0506

Plugin Information

Published: 2007/10/04, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
Could not connect to the registry because:
Could not connect to \winreg
```

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: 2021/02/11

Plugin Output

tcp/139/smb

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

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: 2021/02/11

Plugin Output

tcp/445/cifs

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

100871 - Microsoft Windows SMB Versions Supported (remote check) -

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
SMBv1
SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) -

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 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: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_ _introduced in windows version_
2.0.2 Windows 2008

The remote host does NOT support the following SMB dialects :
_version_ _introduced in windows version_
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: 2021/09/16

Plugin Output

tcp/7/echo

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/9/discard

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/13/daytime

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/17/qotd

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/19/chargen

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/23/telnet

```
Port 23/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/42

```
Port 42/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/135/epmap

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave

unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/139/smb

```
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: 2021/09/16

Plugin Output

tcp/443/www

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

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

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

19506 - Nessus Scan Information -

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2021/09/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.0.1
Nessus build : 20287
Plugin feed version : 202111191213
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : My scan
Scan policy used : Basic Network Scan
Scanner IP : 172.16.1.200
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 23.374 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/11/19 9:00 Pacific Standard Time
Scan duration : 391 sec
```

24786 - Nessus Windows Scan Not Performed with Admin Privileges -

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

References

XREF IAVB:0001-B-0505

Plugin Information

Published: 2007/03/12, Modified: 2020/09/22

Plugin Output

tcp/0

```
It was not possible to connect to '\\S08\ADMIN$' with the supplied credentials.
```

11936 - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2021/09/27

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2008 Standard Service Pack 1
Confidence level : 99
Method : MSRPC

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

HTTP:Server: Microsoft-IIS/7.0

SinFP:!:
P1:B11113:F0x12:W8192:O0204ffff:M1460:
P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:190002_7_p=443R
SSLcert:!:i/CN:WIN-6CLCZAW0GONs/CN:WIN-6CLCZAW0GON
aa474fe6bac083e3021a45e54d39fc7892a95cb5
i/CN:s08s/CN:s08
f257ca6b8ec9d60a5624ef84fd72cf5fd7782afa


The remote host is running Microsoft Windows Server 2008 Standard Service Pack 1
```

117886 - OS Security Patch Assessment Not Available -

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.
This does not necessarily indicate a problem with the scan.
Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

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

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

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

Plugin Output

tcp/0

```
The following issues were reported :

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

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

```
This port supports SSLv2/SSLv3/TLSv1.0.
```

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

```
This port supports 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: 2021/03/09

Plugin Output

tcp/443/www

```
The host name known by Nessus is :

s08

The Common Name in the certificate is :

win-6clczaw0gon
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

```
Subject Name:

Common Name: WIN-6CLCZAW0GON

Issuer Name:

Common Name: WIN-6CLCZAW0GON

Serial Number: 23 0C 82 69 C2 E8 A8 80 44 07 1B E3 4C AA C2 F0

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Apr 04 16:09:50 2016 GMT
Not Valid After: Apr 04 00:00:00 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 DA 55 C0 16 A3 D5 4E 8C 76 5B 33 53 F9 75 46 94 FC 6A 1D
4F F1 0C 99 E2 AB 84 81 4E 67 EF EB 96 A5 23 28 9F 26 C1 B1
E4 E5 35 DB 4D 12 C4 71 79 AB 52 B7 2F 51 05 6E 0A 1A 44 3F
8E C6 FA D5 7D CB 8D 1A 5C E5 BD 3E E8 8E 75 0D CB A4 BB 4B
E4 52 B3 BE 3F 43 7E 96 33 FA E1 16 95 F0 0E 80 16 18 FF BE
EE 62 33 5B B6 1B 68 A1 04 D4 5A 0F 8C 0A EC C1 B3 37 2C EA
86 54 54 82 9D 0C EB 65 01 70 81 07 C9 E2 D4 18 C2 A6 C5 5B
13 BE 0C EF 36 75 FE 55 CD 02 AD D5 B7 9B E2 B8 37 DD A4 CE
A3 4F 0F 4A 7A 1A 85 8A 2F 44 F6 59 14 B5 90 99 23 20 9B 11
E3 FB 45 21 E2 5D A7 E7 21 D4 3A 0D 70 00 FF A4 95 7D BE 15
D8 A3 5E 01 EA E1 B0 8F 45 02 65 D9 90 E4 F9 38 4C E3 7C 34
3E D9 27 73 C7 2F 2E 36 C1 D6 C0 A2 07 24 FA E7 92 1C EC 64
B7 B7 D9 93 47 06 63 3C 34 7C 01 B3 28 94 2A 50 77
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 97 E5 76 82 95 99 A0 57 D6 4D 3F 58 B9 82 5B 2B 7F 69 23
A7 3A C3 D2 51 9A B3 D2 5A 83 FE AC 4D 10 99 C3 DC B3 F3 6F
9B 9D 5A DB 00 88 7F 38 27 81 D2 DE B6 71 EB 4B 73 C5 44 08
8C 77 96 B8 F7 C1 5F 0D D0 D6 17 22 B0 AC 34 79 60 17 87 7A
2D 99 A9 49 F8 A4 93 12 FE 16 19 AF 01 A3 7E 23 DD 99 BD A4
5C C4 03 DA 08 68 6C 49 60 CF 44 EE D3 E9 28 2F FF 69 B5 92
3B EB DC 87 8C 43 48 F0 16 BC 45 8C 93 66 F0 17 65 D7 D3 7C
B4 D2 F0 C3 80 19 D3 BA BD F4 F1 E4 1B 4B 97 27 1B 4C 14 8C
AD E1 74 19 1E F6 4F D9 F7 84 57 F4 B2 3A 4C 7E 3A 4A 72 AE
E7 D0 94 CD B9 4C 15 5D 3A CE A2 16 5E B7 4A 75 79 04 CA BC
E9 09 76 17 47 83 09 9B AE 64 01 64 22 75 31 08 04 17 4C B1
C7 83 9D 19 78 F7 9D 96 9F 83 4F B5 A7 A0 2B 87 B2 E0 12 B6
E3 A7 D7 03 4D B4 C3 28 61 AC 85 12 AD AC 47 CC CA

Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment
```

```
Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Fingerprints :

SHA-256 Fingerprint: 84 98 77 88 A8 9F 8A 93 2D A2 BB 21 EC 1E B5 95 5A B3 74 0F
F9 78 2C BD E1 86 51 7B EF A3 E6 39
SHA-1 Fingerprint: AA 47 4F E6 BA C0 83 E3 02 1A 45 E5 4D 39 FC 78 92 A9 5C B5
MD5 Fingerprint: 0F E6 B6 17 DC 37 27 E7 00 15 CB D5 88 FA 3D C1


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIC4jCCAcqgAwIBAgIQIwyCacLoqIBEBxvjTKrC8DANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9XSU4tNkNMQ1pBVzBHT04wHhcNMTYwNDA0MTYwOTUwWhcNMjYwNDA0MDAwMDAwWjAaMRgwFgYDVQQDEw9XSU4
-----END CERTIFICATE-----
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: s08

Issuer Name:

Common Name: s08

Serial Number: E0 AC 27 88 54 0D 50 B8 47 66 E9 65 7E 30 78 C9

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 05 16:02:50 2021 GMT
Not Valid After: Apr 06 16:02:50 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B7 0F 80 CB 65 8D 37 E0 88 28 B8 77 A1 61 35 2D F5 E9 A6
88 EC A7 F2 F0 AC B9 95 41 C6 8F 2B 69 2A C0 8B 7A 99 3A 6F
0A C4 20 B2 D5 0E 79 7F 21 A6 3B BB 7B 2E CA AA A1 C2 49 CD
32 F8 B8 03 4B D9 E0 77 56 2E 1E 97 55 F8 7F C7 68 2A 1B 1A
32 58 F7 5D FC 52 32 09 58 D4 A6 65 46 93 E6 80 1B 03 A4 29
FB 84 20 78 C1 39 0E 5A 91 88 68 A7 E6 F8 95 20 B8 16 79 3D
A3 B0 87 A4 AC D9 ED E4 5E 12 3A 2B 04 C9 EC EE C1 C9 57 63
96 84 75 40 01 32 49 2A BB 3C E8 12 12 74 A7 C4 F1 CD B8 82
BC 06 B2 5C 05 BD 8F 84 11 75 AD DD 2B 9B 4B BF AE C5 42 A7
DF 69 E9 29 D5 B7 05 2E 2E 93 24 92 5D 63 52 58 DF DE E9 E7
3A 6A D0 86 70 A7 7D 00 AA EE 27 8E 00 82 46 35 94 7B 59 2F
EF 1C B4 31 CB 12 DA BD D9 66 14 B5 D4 10 9F F0 46 EC E5 05
97 88 B8 A9 0E 46 FF F1 FC D2 AB 88 E7 D8 12 48 8D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 40 32 E7 F6 10 E7 1C 8B 53 03 32 4D 03 A1 3E 9B EA 9C 95
4B C5 E7 50 E1 34 86 17 53 D0 19 AE 65 0F 24 66 EC A9 95 4A
14 CD 53 C9 77 C9 D7 05 43 26 5D CC 73 A7 38 11 FF 72 D6 62
AB 70 2E 47 DE 8E C4 E5 FC 77 4D 6B 4E 12 F0 F6 88 81 D4 BC
97 30 5D 48 5B 65 A9 D9 E1 62 84 35 AE AC E5 84 B2 4F 3F 33
09 22 53 A6 6E 8E DF C6 86 1A 53 3F 3D E8 37 59 BC 65 B3 E9
13 D2 48 68 B5 16 FB BE 6B 90 23 97 27 A9 A6 C3 29 78 22 98
3E 20 94 ED 35 09 A4 F8 7C 26 FB 0B F9 42 48 B6 AC AA BF B2
E0 11 F2 4E 12 EE 18 A8 2B 0C 35 8D 50 DF 60 11 30 AB 85 C0
6C F5 C5 61 54 62 D7 3F 55 5C 80 E7 85 A6 70 20 E2 B6 4A 40
7B BB 79 A7 7C 01 F3 1F B2 54 C5 1A 7D C5 66 28 A0 E2 5E 1D
C0 A1 6B E5 94 46 BD 6F 3F 4A 94 22 DD 4D 90 0D 1D CF ED DB
F2 3F 35 CA 41 BB 27 31 0A 58 03 7E A9 10 4A D1 4F

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment


Fingerprints :

SHA-256 Fingerprint: 60 7A 5D 9B 76 63 68 77 3C 8F A0 E2 5A 02 CD EC 58 32 3A 91
B0 37 FE F8 D8 7E 7A 3A CE 95 F4 33
SHA-1 Fingerprint: F2 57 CA 6B 8E C9 D6 0A 56 24 EF 84 FD 72 CF 5F D7 78 2A FA
MD5 Fingerprint: 3A 8E 57 55 0B 18 E2 78 B3 46 B9 35 7E EC F2 E1


PEM certificate :

-----BEGIN CERTIFICATE-----
MIICyjCCAbKgAwIBAgIQ4KwniFQNULhHZullfjB4yTANBgkqhkiG9w0BAQUFADAOMQwwCgYDVQQDEwNzMDgwHhcNMjExMDA1MTYwMjUwWhcNMjIwNDA2MTYwMjUwWjAOMQwwCgYDVQQDEwNzMDgwggEiMA0GCSqGSIb
-----END CERTIFICATE-----
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

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

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DES-CBC3-MD5 0x07, 0x00, 0xC0 RSA RSA 3DES-CBC(168) MD5
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1

The fields above are :

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

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

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

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

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

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1

The fields above are :

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

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1


SSL Version : SSLv3
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

High Strength Ciphers (>= 112-bit key)

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


SSL Version : SSLv2
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DES-CBC3-MD5 0x07, 0x00, 0xC0 RSA RSA 3DES-CBC(168) MD5

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
RC4-MD5 0x01, 0x00, 0x80 RSA RSA RC4(128) MD5

The fields above are :

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

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

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

SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
```

```
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

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

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1

The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3389/msrdp

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

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1

The fields above are :

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

51891 - SSL Session Resume Supported -

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/443/www

```
This port supports resuming SSLv3 / TLSv1 sessions.
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) -

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/7/echo

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/19/chargen

```
A chargen server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/42

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/443/www

```
A TLSv1 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.
```

17975 - Service Detection (GET request) -

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0935

Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

Plugin Output

tcp/17/qotd

```
qotd seems to be running on this port.
```

11153 - Service Detection (HELP Request) -

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/11/26

Plugin Output

tcp/13/daytime

```
Daytime is running on this port.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided -

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2021/08/30

Plugin Output

tcp/0

```
SMB was detected on port 445 but no credentials were provided.
SMB local checks were not enabled.
```

10281 - Telnet Server Detection -

Synopsis

A Telnet server is listening on the remote port.

Description

The remote host is running a Telnet server, a remote terminal server.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2020/06/12

Plugin Output

tcp/23/telnet

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------

No more connections are allowed to telnet server. Please try again later.
------------------------------ snip ------------------------------
```

64814 - Terminal Services Use SSL/TLS -

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/22, Modified: 2021/02/24

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: s08

Issuer Name:

Common Name: s08

Serial Number: E0 AC 27 88 54 0D 50 B8 47 66 E9 65 7E 30 78 C9

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 05 16:02:50 2021 GMT
Not Valid After: Apr 06 16:02:50 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B7 0F 80 CB 65 8D 37 E0 88 28 B8 77 A1 61 35 2D F5 E9 A6
88 EC A7 F2 F0 AC B9 95 41 C6 8F 2B 69 2A C0 8B 7A 99 3A 6F
0A C4 20 B2 D5 0E 79 7F 21 A6 3B BB 7B 2E CA AA A1 C2 49 CD
32 F8 B8 03 4B D9 E0 77 56 2E 1E 97 55 F8 7F C7 68 2A 1B 1A
32 58 F7 5D FC 52 32 09 58 D4 A6 65 46 93 E6 80 1B 03 A4 29
FB 84 20 78 C1 39 0E 5A 91 88 68 A7 E6 F8 95 20 B8 16 79 3D
A3 B0 87 A4 AC D9 ED E4 5E 12 3A 2B 04 C9 EC EE C1 C9 57 63
96 84 75 40 01 32 49 2A BB 3C E8 12 12 74 A7 C4 F1 CD B8 82
BC 06 B2 5C 05 BD 8F 84 11 75 AD DD 2B 9B 4B BF AE C5 42 A7
DF 69 E9 29 D5 B7 05 2E 2E 93 24 92 5D 63 52 58 DF DE E9 E7
3A 6A D0 86 70 A7 7D 00 AA EE 27 8E 00 82 46 35 94 7B 59 2F
EF 1C B4 31 CB 12 DA BD D9 66 14 B5 D4 10 9F F0 46 EC E5 05
97 88 B8 A9 0E 46 FF F1 FC D2 AB 88 E7 D8 12 48 8D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 40 32 E7 F6 10 E7 1C 8B 53 03 32 4D 03 A1 3E 9B EA 9C 95
4B C5 E7 50 E1 34 86 17 53 D0 19 AE 65 0F 24 66 EC A9 95 4A
14 CD 53 C9 77 C9 D7 05 43 26 5D CC 73 A7 38 11 FF 72 D6 62
AB 70 2E 47 DE 8E C4 E5 FC 77 4D 6B 4E 12 F0 F6 88 81 D4 BC
97 30 5D 48 5B 65 A9 D9 E1 62 84 35 AE AC E5 84 B2 4F 3F 33
09 22 53 A6 6E 8E DF C6 86 1A 53 3F 3D E8 37 59 BC 65 B3 E9
13 D2 48 68 B5 16 FB BE 6B 90 23 97 27 A9 A6 C3 29 78 22 98
3E 20 94 ED 35 09 A4 F8 7C 26 FB 0B F9 42 48 B6 AC AA BF B2
E0 11 F2 4E 12 EE 18 A8 2B 0C 35 8D 50 DF 60 11 30 AB 85 C0
6C F5 C5 61 54 62 D7 3F 55 5C 80 E7 85 A6 70 20 E2 B6 4A 40
7B BB 79 A7 7C 01 F3 1F B2 54 C5 1A 7D C5 66 28 A0 E2 5E 1D
C0 A1 6B E5 94 46 BD 6F 3F 4A 94 22 DD 4D 90 0D 1D CF ED DB
F2 3F 35 CA 41 BB 27 31 0A 58 03 7E A9 10 4A D1 4F

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment
```

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 172.16.1.200 to 172.16.11.8 :
172.16.1.200
172.16.1.1
172.16.11.8

Hop Count: 2
```

20094 - VMware Virtual Machine Detection -

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

135860 - WMI Not Available -

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2021/11/12

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

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: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 3 NetBIOS names have been gathered :

S08 = Computer name
WORKGROUP = Workgroup / Domain name
S08 = File Server Service

The remote host has the following MAC address on its adapter :

00:50:56:ae:47:3f
```

10940 - Windows Terminal Services Enabled -

Synopsis

The remote Windows host has Terminal Services enabled.

Description

Terminal Services allows a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable Terminal Services if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2020/07/08

Plugin Output

tcp/3389/msrdp

172.16.11.30

0	14	43	4	160
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Fri Nov 19 09:00:27 2021
End time:	Fri Nov 19 09:23:06 2021

Host Information

Netbios Name:	UMAIL
IP:	172.16.11.30
OS:	Linux Kernel 3.13 on Ubuntu 14.04 (trusty)

Vulnerabilities

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/110/pop3

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/143/imap

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/465/smtp

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```


42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/587/smtp

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
```

```
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/993/imap

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) -

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/995/pop3

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1
```

```
The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

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 1.2 (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 v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/25/smtp

```
- 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)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-EDH-RSA-DES-CBC-SHA DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 RSA(512) RSA RC4(40) MD5 export
DES-CBC-SHA RSA RSA DES-CBC(56) SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA DH None AES-CBC(128) SHA1
ADH-AES256-SHA DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 DH None RC4(128) MD5
ADH-SEED-SHA DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA ECDH None RC4(128) SHA1
AES128-SHA RSA RSA AES-CBC(128) SHA1
AES256-SHA RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 RSA RSA RC4(128) MD5
RC4-SHA RSA RSA RC4(128) SHA1
SEED-SHA RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 DH RSA AES-CBC(256) SHA256
```

```
DH-AES128-SHA256 DH None AES-CBC(128) SHA256
DH-AES256-SHA256 DH None AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

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 1.2 (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 v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/110/pop3

```
- 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


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA ECDH RSA RC4(128) SHA1
AES128-SHA RSA RSA AES-CBC(128) SHA1
AES256-SHA RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 RSA RSA RC4(128) MD5
RC4-SHA RSA RSA RC4(128) SHA1
SEED-SHA RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

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 1.2 (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 v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/143/imap

```
- 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


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA ECDH RSA RC4(128) SHA1
AES128-SHA RSA RSA AES-CBC(128) SHA1
AES256-SHA RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 RSA RSA RC4(128) MD5
RC4-SHA RSA RSA RC4(128) SHA1
SEED-SHA RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

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 1.2 (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 v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/465/smtp

```
- 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


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA DH None AES-CBC(128) SHA1
ADH-AES256-SHA DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 DH None RC4(128) MD5
ADH-SEED-SHA DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA ECDH None RC4(128) SHA1
AES128-SHA RSA RSA AES-CBC(128) SHA1
AES256-SHA RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 RSA RSA RC4(128) MD5
RC4-SHA RSA RSA RC4(128) SHA1
SEED-SHA RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 DH RSA AES-CBC(256) SHA256
DH-AES128-SHA256 DH None AES-CBC(128) SHA256
DH-AES256-SHA256 DH None AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

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 1.2 (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 v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/587/smtp

```
- 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


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA DH None AES-CBC(128) SHA1
ADH-AES256-SHA DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 DH None RC4(128) MD5
ADH-SEED-SHA DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA ECDH None RC4(128) SHA1
AES128-SHA RSA RSA AES-CBC(128) SHA1
AES256-SHA RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 RSA RSA RC4(128) MD5
RC4-SHA RSA RSA RC4(128) SHA1
SEED-SHA RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 DH RSA AES-CBC(256) SHA256
DH-AES128-SHA256 DH None AES-CBC(128) SHA256
DH-AES256-SHA256 DH None AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

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 1.2 (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 v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/993/imap

```
- 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


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
EDH-RSA-DES-CBC3-SHA DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
-------------------- ---------- --- ---- -------------------- ---
DHE-RSA-AES128-SHA DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA ECDH RSA RC4(128) SHA1
AES128-SHA RSA RSA AES-CBC(128) SHA1
AES256-SHA RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 RSA RSA RC4(128) MD5
RC4-SHA RSA RSA RC4(128) SHA1
SEED-SHA RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

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 1.2 (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 v2.0 Base Score

7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/995/pop3

```
- 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


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA ECDH RSA RC4(128) SHA1
AES128-SHA RSA RSA AES-CBC(128) SHA1
AES256-SHA RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 RSA RSA RC4(128) MD5
RC4-SHA RSA RSA RC4(128) SHA1
SEED-SHA RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

10595 - DNS Server Zone Transfer Information Disclosure (AXFR) -

Synopsis

The remote name server allows zone transfers

Description

The remote name server allows DNS zone transfers to be performed.

A zone transfer lets a remote attacker instantly populate a list of potential targets. In addition, companies often use a naming convention that can give hints as to a servers primary application (for instance, proxy.example.com, payroll.example.com, b2b.example.com, etc.).

As such, this information is of great use to an attacker, who may use it to gain information about the topology of the network and spot new targets.

See Also

https://en.wikipedia.org/wiki/AXFR

Solution

Limit DNS zone transfers to only the servers that need the information.

Risk Factor

Medium

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:U/RL:ND/RC:C)

References

CVE CVE-1999-0532

Plugin Information

Published: 2001/01/16, Modified: 2018/09/17

Plugin Output

tcp/53/dns

```
+ Domain "ifslab.ca":
ifslab.ca. name server ns0.ifslab.ca.
ifslab.ca.ifslab.ca. has address 172.16.100.4
ns0.ifslab.ca. has address 172.16.11.30
storage1.ifslab.ca. has address 172.16.100.4
storage2.ifslab.ca. has address 172.16.100.2
ubumail.ifslab.ca. has address 172.16.11.30
```

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

http://www.nessus.org/u?df39b8b3
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 v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Published: 2012/01/19, Modified: 2021/03/15

Plugin Output

tcp/445/cifs

90317 - SSH Weak Algorithms Supported -

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following weak server-to-client encryption algorithms are supported :

arcfour
arcfour128
arcfour256

The following weak client-to-server encryption algorithms are supported :

arcfour
arcfour128
arcfour256
```

31705 - SSL Anonymous Cipher Suites Supported -

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?3a040ada

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Low

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	28482
CVE	CVE-2007-1858

Plugin Information

Published: 2008/03/28, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DH-AES128-SHA256 0x00, 0xA6 DH None AES-GCM(128) SHA256
DH-AES256-SHA384 0x00, 0xA7 DH None AES-GCM(256) SHA384
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
DH-AES128-SHA256 0x00, 0x6C DH None AES-CBC(128) SHA256
DH-AES256-SHA256 0x00, 0x6D DH None AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

31705 - SSL Anonymous Cipher Suites Supported -

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?3a040ada

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Low

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	28482
CVE	CVE-2007-1858

Plugin Information

Published: 2008/03/28, Modified: 2021/02/03

Plugin Output

tcp/465/smtp

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DH-AES128-SHA256 0x00, 0xA6 DH None AES-GCM(128) SHA256
DH-AES256-SHA384 0x00, 0xA7 DH None AES-GCM(256) SHA384
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
```

```
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
DH-AES128-SHA256 0x00, 0x6C DH None AES-CBC(128) SHA256
DH-AES256-SHA256 0x00, 0x6D DH None AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

31705 - SSL Anonymous Cipher Suites Supported -

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?3a040ada

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Low

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	28482
CVE	CVE-2007-1858

Plugin Information

Published: 2008/03/28, Modified: 2021/02/03

Plugin Output

tcp/587/smtp

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DH-AES128-SHA256 0x00, 0xA6 DH None AES-GCM(128) SHA256
DH-AES256-SHA384 0x00, 0xA7 DH None AES-GCM(256) SHA384
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
DH-AES128-SHA256 0x00, 0x6C DH None AES-CBC(128) SHA256
DH-AES256-SHA256 0x00, 0x6D DH None AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the

certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/25/smtp

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=ON/ST=Ontario/L=Toronto/O=Security Lab/OU=Education/CN=ifslab.ca/E=root@ifslab.ca
|-Issuer : C=ON/ST=Ontario/L=Toronto/O=Security Lab/OU=Education/CN=ifslab.ca/E=root@ifslab.ca
```

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/110/pop3

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Issuer : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
```

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the

certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/143/imap

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Issuer : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
```

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/465/smtp

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=ON/ST=Ontario/L=Toronto/O=Security Lab/OU=Education/CN=ifslab.ca/E=root@ifslab.ca
|-Issuer : C=ON/ST=Ontario/L=Toronto/O=Security Lab/OU=Education/CN=ifslab.ca/E=root@ifslab.ca
```

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the

certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/587/smtp

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=ON/ST=Ontario/L=Toronto/O=Security Lab/OU=Education/CN=ifslab.ca/E=root@ifslab.ca
|-Issuer : C=ON/ST=Ontario/L=Toronto/O=Security Lab/OU=Education/CN=ifslab.ca/E=root@ifslab.ca
```

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/993/imap

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Issuer : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
```

51192 - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the

certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/995/pop3

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Issuer : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
```

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 SSL 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 v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/25/smtp

```
The identities known by Nessus are :

172.16.11.30
172.16.11.30

The Common Name in the certificate is :

ifslab.ca
```

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 SSL 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 v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/110/pop3

```
The identities known by Nessus are :

172.16.11.30
172.16.11.30
```

```
The Common Name in the certificate is :

mailbox
```

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 SSL 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 v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/143/imap

```
The identities known by Nessus are :

172.16.11.30
172.16.11.30

The Common Name in the certificate is :

mailbox
```

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 SSL 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 v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/465/smtp

```
The identities known by Nessus are :

172.16.11.30
172.16.11.30

The Common Name in the certificate is :

ifslab.ca
```

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 SSL 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 v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/587/smtp

```
The identities known by Nessus are :

172.16.11.30
172.16.11.30

The Common Name in the certificate is :

ifslab.ca
```

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 SSL 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 v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/993/imap

```
The identities known by Nessus are :

172.16.11.30
172.16.11.30

The Common Name in the certificate is :

mailbox
```

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 SSL 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 v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/995/pop3

```
The identities known by Nessus are :

172.16.11.30
172.16.11.30

The Common Name in the certificate is :

mailbox
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
List of RC4 cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/110/pop3

```
List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/143/imap

```
List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/465/smtp

```
List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/587/smtp

```
List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
```

```
---------------------- ---------- --- ---- ---------------------- ---
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/993/imap

```
List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```


65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) -

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/
http://www.nessus.org/u?ac7327a0
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/995/pop3

```
List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57582 - SSL Self-Signed Certificate -

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/25/smtp

```
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=ON/ST=Ontario/L=Toronto/O=Security Lab/OU=Education/CN=ifslab.ca/E=root@ifslab.ca
```

57582 - SSL Self-Signed Certificate -

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/110/pop3

```
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 : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
```

57582 - SSL Self-Signed Certificate -

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/143/imap

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
```

57582 - SSL Self-Signed Certificate -

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/465/smtp

```
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=ON/ST=Ontario/L=Toronto/O=Security Lab/OU=Education/CN=ifslab.ca/E=root@ifslab.ca
```

57582 - SSL Self-Signed Certificate -

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/587/smtp

```
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=ON/ST=Ontario/L=Toronto/O=Security Lab/OU=Education/CN=ifslab.ca/E=root@ifslab.ca
```

57582 - SSL Self-Signed Certificate -

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/993/imap

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
```

57582 - SSL Self-Signed Certificate -

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/995/pop3

```
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 : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
```

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 v2.0 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: 2021/02/03

Plugin Output

tcp/25/smtp

```
Here is the list of weak SSL ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

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 v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

References

BID 71936
CVE CVE-2015-0204
XREF CERT:243585

Plugin Information

Published: 2015/03/04, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
EXPORT_RSA cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/25/smtp

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/110/pop3

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/143/imap

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/465/smtp

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/587/smtp

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/993/imap

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/995/pop3

```
TLSv1 is enabled and the server supports at least one cipher.
```

70658 - SSH Server CBC Mode Ciphers Enabled -

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2018/07/30

Plugin Output

tcp/22/ssh

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

153953 - SSH Weak Key Exchange Algorithms Enabled -

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

http://www.nessus.org/u?b02d91cd
https://datatracker.ietf.org/doc/html/rfc8732

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2021/10/13, Modified: 2021/10/13

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

diffie-hellman-group-exchange-sha1
diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled -

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
```

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 v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 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: 2021/02/03

Plugin Output

tcp/25/smtp

```
EXPORT_DHE cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

18261 - Apache Banner Linux Distribution Disclosure -

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.
n/a

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2019/10/01

Plugin Output

tcp/0

```
The Linux distribution detected was :
- Ubuntu 14.04 (trusty)
```

48204 - Apache HTTP Server Version -

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

tcp/80/www

```
URL : http://172.16.11.30/
Version : 2.4.99
backported : 1
os : ConvertedUbuntu
```

39519 - Backported Security Patch Detection (FTP) -

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote FTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/21/ftp

```
Give Nessus credentials to perform local checks.
```

39520 - Backported Security Patch Detection (SSH) -

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

39521 - Backported Security Patch Detection (WWW) -

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80/www

```
Give Nessus credentials to perform local checks.
```

45590 - Common Platform Enumeration (CPE) -

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2021/11/08

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:canonical:ubuntu_linux:14.04

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.7 -> Apache Software Foundation Apache HTTP Server 2.4.7
cpe:/a:apache:http_server:2.4.99
cpe:/a:isc:bind:9.9.5-3ubuntu0.9-ubuntu
cpe:/a:isc:bind:9.9.5:3ubuntu0
cpe:/a:openbsd:openssh:6.6 -> OpenBSD OpenSSH 6.6
cpe:/a:samba:samba:4.3.11 -> Samba 4.3.11
```

10028 - DNS Server BIND version Directive Remote Version Detection -

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF IAVT:0001-T-0583

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

udp/53/dns

```
Version : 9.9.5-3ubuntu0.9-Ubuntu
```

11002 - DNS Server Detection -

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

https://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53/dns

11002 - DNS Server Detection -

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

https://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

udp/53/dns

72779 - DNS Server Version Detection -

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0937

Plugin Information

Published: 2014/03/03, Modified: 2020/09/22

Plugin Output

tcp/53/dns

```
DNS server answer for "version.bind" (over TCP) :

9.9.5-3ubuntu0.9-Ubuntu
```

35371 - DNS Server hostname.bind Map Hostname Disclosure -

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information

Published: 2009/01/15, Modified: 2011/09/14

Plugin Output

udp/53/dns

```
The remote host name is :

umail
```

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 : 95
```

10092 - FTP Server Detection -

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220 (vsFTPd 3.0.2)
```

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/www

```
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Tue, 26 Jan 2021 15:10:09 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Fri, 08 Nov 2019 18:12:15 GMT
ETag: "2cf6-596d9b8c725ca"
Accept-Ranges: bytes
Content-Length: 11510
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
Modified from the Debian original for Ubuntu
Last updated: 2014-03-19
See: https://launchpad.net/bugs/1288690
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Ubuntu Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}

div.main_page {
position: relative;
display: table;

width: 800px;

margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding: 0px 0px 0px 0px;

border-width: 2px;
border-color: #212738;
border-style: solid;

background-color: #FFFFFF;

text-align: center;
}

div.page_header {
height: 99px;
width: 100%;

background-color: #F5F6F7;
}

div.page_header span {
margin: 15px 0px 0px 50px;

font-size: 180%;
font-weight: bold;
}

div.page_header img {
margin: 3px 0px 0px 40px;

border: 0px 0px 0px;
}

div.table_of_contents {
clear: left;

min-width: 200px;

margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

div.table_of_contents_item {
clear: left;

width: 100%;

margin: 4px 0px 0px 0px;

background-color: #FFFFFF;

color: #000000;
text-align: left;
}

div.table_of_contents_item a {
```

```
margin: 6px 0px 0px 6px;
}

div.content_section {
margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

div.content_section_text {
padding: 4px 8px 4px 8px;

color: #000000;
font-size: 100%;
}

div.content_section_text pre {
margin: 8px 0px 8px 0px;
padding: 8px 8px 8px 8px;

border-width: 1px;
border-style: dotted;
border-color: #000000;

background-color: #F5F6F7;

font-style: italic;
}

div.content_section_text p {
margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
padding: 4px 8px 4px 16px;
}

div.section_header {
padding: 3px 6px 3px 6px;

background-color: #8E9CB2;

color: #FFFFFF;
font-weight: bold;
font-size: 112%;
text-align: center;
}

div.section_header_red {
background-color: #CD214F;
}

div.section_header_grey {
background-color: #9F9386;
}

.floating_element {
position: relative;
float: left;
}

div.table_of_contents_item a,
div.content_section_text a {
text-decoration: none;
font-weight: bold;
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
color: #000000;
}

div.table_of_contents_item a:hover {
background-color: #000000;

color: #FFFFFF;
}

div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
background-color: #DCDFE6;

color: #000000;
}

div.content_section_text a:hover {
background-color: #000000;

color: #DCDFE6;
}

div.validator {
}
</style>
</head>
<body>
<div class="main_page">
<div class="page_header floating_element">
<img src="/icons/ubuntu-logo.png" alt="Ubuntu Logo" class="floating_element"/>
<span class="floating_element">
Apache2 Ubuntu Default Page
</span>
</div>
<!-- <div class="table_of_contents floating_element">
<div class="section_header section_header_grey">
TABLE OF CONTENTS
</div>
<div class="table_of_contents_item floating_element">
<a href="#about">About</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#changes">Changes</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#scope">Scope</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#files">Config files</a>
</div>
</div>
-->
<div class="content_section floating_element">


<div class="section_header section_header_red">
<div id="about"></div>
It works!
</div>
<div class="content_section_text">
<p>
```

```
This is the default welcome page used to test the correct
operation of the Apache2 server after installation on Ubuntu systems.
It is based on the equivalent page on Debian, from which the Ubuntu Apache
packaging is derived.
If you can read this page, it means that the Apache HTTP server installed at
this site is working properly. You should <b>replace this file</b> (located at
<tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
</p>


<p>
If you are a normal user of this web site and don't know what this page is
about, this probably means that the site is currently unavailable due to
maintenance.
If the problem persists, please contact the site's administrator.
</p>

</div>
<div class="section_header">
<div id="changes"></div>
Configuration Overview
</div>
<div class="content_section_text">
<p>
Ubuntu's Apache2 default configuration is different from the
upstream default configuration, and split into several files optimized for
interaction with Ubuntu tools. The configuration system is
<b>fully documented in
/usr/share/doc/apache2/README.Debian.gz</b>. Refer to this for the full
documentation. Documentation for the web server itself can be
found by accessing the <a href="/manual">manual</a> if the <tt>apache2-doc</tt>
package was installed on this server.

</p>
<p>
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
</p>
<pre>
/etc/apache2/
|-- apache2.conf
|	`-- ports.conf
|-- mods-enabled
|	|-- *.load
|	`-- *.conf
|-- conf-enabled
|	`-- *.conf
|-- sites-enabled
|	`-- *.conf
</pre>
<ul>
<li>
<tt>apache2.conf</tt> is the main configuration
file. It puts the pieces together by including all remaining configuration
files when starting up the web server.
</li>

<li>
<tt>ports.conf</tt> is always included from the
main configuration file. It is used to determine the listening ports for
incoming connections, and this file can be customized anytime.
</li>

<li>
Configuration files in the <tt>mods-enabled/</tt>,
<tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
particular configuration snippets which manage modules, global configuration
fragments, or virtual host configurations, respectively.
</li>

<li>
They are activated by symlinking available
configuration files from their respective
*-available/ counterparts. These should be managed
by using our helpers
<tt>
<a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2enmod">a2enmod</a>,
<a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2dismod">a2dismod</a>,
</tt>
<tt>
<a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2ensite">a2ensite</a>,
<a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2dissite">a2dissite</a>,
</tt>
and
<tt>
<a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2enconf">a2enconf</a>,
<a href="http://manpages.debian.org/cgi-bin/man.cgi?query=a2disconf">a2disconf</a>
</tt>. See their respective man pages for detailed information.
</li>

<li>
The binary is called apache2. Due to the use of
environment variables, in the default configuration, apache2 needs to be
started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
<b>Calling <tt>/usr/bin/apache2</tt> directly will not work</b> with the
default configuration.
</li>
</ul>
</div>

<div class="section_header">
<div id="docroot"></div>
Document Roots
</div>

<div class="content_section_text">
<p>
By default, Ubuntu does not allow access through the web browser to
<em>any</em> file apart of those located in <tt>/var/www</tt>,
<a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html">public_html</a>
directories (when enabled) and <tt>/usr/share</tt> (for web
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
document root directory in <tt>/etc/apache2/apache2.conf</tt>.
</p>
<p>
The default Ubuntu document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www. This is different
to previous releases which provides better security out of the box.
</p>
</div>

<div class="section_header">
<div id="bugs"></div>
Reporting Problems
</div>
<div class="content_section_text">
<p>
Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
Apache2 package with Ubuntu. However, check <a
href="https://bugs.launchpad.net/ubuntu/+source/apache2">existing
bug reports</a> before reporting a new bug.
</p>
<p>
Please report bugs specific to modules (such as PHP and others)
```

```
to respective packages, not to the web server itself.
</p>
</div>




</div>
</div>
<div class="validator">
<p>
<a href="http://validator.w3.org/check?uri=referer"><img src="http://www.w3.org/Icons/valid-xhtml10" alt="Valid XHTML
1.0 Transitional" height="31" width="88" /></a>
</p>
</div>
</body>
</html>
```

10114 - ICMP Timestamp Request Remote Date Disclosure -

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS v2.0 Base Score

0.0 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

icmp/0

```
The difference between the local and remote clocks is 6801 seconds.
```

11414 - IMAP Service Banner Retrieval -

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

Plugin Output

tcp/143/imap

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED] Dovecot (Ubuntu)
ready.
```

11414 - IMAP Service Banner Retrieval -

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

Plugin Output

tcp/993/imap

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] Dovecot (Ubuntu)
ready.
```

42085 - IMAP Service STARTTLS Command Support -

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote IMAP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS
https://tools.ietf.org/html/rfc2595

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2021/02/24

Plugin Output

tcp/143/imap

```
Here is the IMAP server's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Issuer Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Serial Number: 00 FE D4 5E 15 69 D8 43 C1

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 18 19:04:48 2016 GMT
Not Valid After: Oct 18 19:04:48 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 5A C3 7D DC 10 A9 E9 02 0B F4 23 A5 44 A9 4C 54 C4 0E
1C 67 9A CE 96 8E EB 66 F3 87 70 FC 2D 42 24 E1 39 9B FD 1B
F4 BF A2 2B 89 24 2D 66 47 76 04 96 EB 17 DD A6 77 67 1F 47
46 87 B1 A9 14 EE BB 1D 85 11 4A FB 68 55 5C 92 05 C8 D3 91
48 41 6B 5C F8 51 E5 C4 0B D1 40 B8 40 FB 16 FC 5C 92 E0 63
BA DB 29 A8 35 30 25 65 A6 0B 47 DB 82 DB 5D 6C 33 E2 E9 24
DD 1F EA 06 66 67 FB 8D 7E DE 6A 38 39 BF 80 9B E0 A4 B5 29
07 9C 96 BC 1B CC 70 44 20 E3 F7 FB 8D CA 2C 6C CD BD 3D 08
92 17 07 06 4C 9C D7 9A 28 33 F9 D8 DE 5E 63 CA EF 3C 6E E3
3B 64 C5 28 8B 39 A4 F8 E6 1B C2 74 FD B5 90 79 3E 96 F9 84
BF 38 69 74 47 35 A2 7D 16 81 CC 58 EB 7F DA 92 91 BB 65 23
3A 08 01 E7 25 09 BD B8 C6 F5 39 6D EC EB 44 1A A5 70 19 7F
E5 FA 70 BD 72 B8 98 BF B2 A7 F9 CC 8D 7B 5D E8 C3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 36 88 C5 13 AA 14 89 B6 2B E0 05 C4 C8 75 2C 97 57 E8 B9
B8 C5 69 B9 E1 F3 C6 DC 6E 19 85 FE ED 2D 82 FF A3 59 36 57
01 B8 F9 4A 93 A1 29 77 09 5D C0 D1 7E F0 D1 58 03 7D F8 6C
5D 81 69 CC CB B1 B4 FF 31 8E 57 DF 3F A1 E3 36 79 99 5D 9A
9B CC F6 41 D1 EE 6D 17 7C FD CB 76 16 28 79 E9 F3 3E CC 19
B2 08 5C 05 A1 51 80 B5 FD BC AA 99 03 87 C0 FC 96 85 93 7D
1B 52 A9 0A 71 3E 59 BA 5D 55 C5 7B 35 96 5A CF 5A 75 89 00
9F 94 89 CB ED 1D 3C D2 19 FE 05 EC B2 F9 49 DB 01 0A 8E 7E
4C C9 2B DD 50 B2 C9 D9 F3 A2 3F 9C 26 88 D8 94 04 D1 E4 77
15 DE FD 62 64 40 A6 77 27 B5 54 24 63 87 F6 3B 18 12 BF E5
2D 18 78 99 68 CF DC BC E0 4C FD FC 49 96 64 B8 35 A7 B9 C7
27 DF B5 57 7C 08 C6 A7 20 CA 83 97 1C 91 63 ED 75 50 71 96
8A D1 02 77 9C 01 2B 53 7B 6F 62 21 D0 69 3F 81 C5

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Basic Constraints (2.5.29.19)
Critical: 0
CA: TRUE


------------------------------ snip ------------------------------
```

17651 - Microsoft Windows SMB : Obtains the Password Policy -

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/03/30, Modified: 2015/01/12

Plugin Output

tcp/445/cifs

```
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration -

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2019/10/04

Plugin Output

tcp/445/cifs

```
The remote host SID value is :

1-5-21-583813521-332104885-1869144122

The value of 'RestrictAnonymous' setting is : unknown
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure -

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows 6.1
The remote native LAN manager is : Samba 4.3.11-Ubuntu
The remote SMB Domain Name is : UMAIL
```

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: 2021/02/11

Plugin Output

tcp/139/smb

```
An SMB server is running on this port.
```

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: 2021/02/11

Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

60119 - Microsoft Windows SMB Share Permissions Enumeration -

Synopsis

It was possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

https://technet.microsoft.com/en-us/library/bb456988.aspx
https://technet.microsoft.com/en-us/library/cc783530.aspx

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/07/25, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
Share path : \\UMAIL\print$
Local path : C:\var\lib\samba\printers
Comment : Printer Drivers
[*] Allow ACE for Everyone: 0x001f01ff
FILE_GENERIC_READ: YES
FILE_GENERIC_WRITE: YES
FILE_GENERIC_EXECUTE: YES

Share path : \\UMAIL\IPC$
Local path : C:\tmp
Comment : IPC Service (umail server (Samba, Ubuntu))
[*] Allow ACE for Everyone: 0x001f01ff
FILE_GENERIC_READ: YES
FILE_GENERIC_WRITE: YES
FILE_GENERIC_EXECUTE: YES
```

10395 - Microsoft Windows SMB Shares Enumeration -

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2020/03/09

Plugin Output

tcp/445/cifs

```
Here are the SMB shares available on the remote host :

- print$
- IPC$
```

100871 - Microsoft Windows SMB Versions Supported (remote check) -

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
SMBv1
SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) -

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 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: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports 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: 2021/09/16

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/25/smtp

```
Port 25/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/53/dns

```
Port 53/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/110/pop3

```
Port 110/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/111/rpc-portmapper

```
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: 2021/09/16

Plugin Output

tcp/139/smb

```
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: 2021/09/16

Plugin Output

tcp/143/imap

```
Port 143/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/465/smtp

```
Port 465/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/587/smtp

```
Port 587/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/993/imap

```
Port 993/tcp was found to be open
```

11219 - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/995/pop3

```
Port 995/tcp was found to be open
```

19506 - Nessus Scan Information -

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2021/09/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.0.1
Nessus build : 20287
Plugin feed version : 202111191213
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : My scan
Scan policy used : Basic Network Scan
Scanner IP : 172.16.1.200
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 23.374 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2021/11/19 9:00 Pacific Standard Time
Scan duration : 1357 sec
```

10884 - Network Time Protocol (NTP) Server Detection -

Synopsis

An NTP server is listening on the remote host.

Description

An NTP server is listening on port 123. If not securely configured, it may provide information about its version, current date, current time, and possibly system information.

See Also

http://www.ntp.org

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0934

Plugin Information

Published: 2015/03/20, Modified: 2021/02/24

Plugin Output

udp/123/ntp

```
An NTP service has been discovered, listening on port 123.

No sensitive information has been disclosed.

Version : unknown
```

11936 - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2021/09/27

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
Confidence level : 95
Method : HTTP

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SSH:SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8
NTP:!:unknown
SinFP:
P1:B10113:F0x12:W29200:O0204ffff:M1460:
P2:B10113:F0x12:W28960:O0204ffff0402080affffffff4445414401030307:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:190002_7_p=993R
SMTP:!:220 umail.ifslab.ca ESMTP Postfix (Ubuntu)
SSLcert:!:i/CN:ifslab.cai/O:Security Labi/OU:Educations/CN:ifslab.cas/O:Security Labs/OU:Education
ab965420d80a20236f1b524c4b9175d3fef88ae2
i/CN:mailboxi/O:Dovecot mail serveri/OU:mailboxs/CN:mailboxs/O:Dovecot mail servers/OU:mailbox
013f3b98980a87864a94fb01abffbb64423fae64


The remote host is running Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
```

117886 - OS Security Patch Assessment Not Available -

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.
This does not necessarily indicate a problem with the scan.
Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

- Plugin : no_local_checks_credentials.nasl
Plugin ID : 110723
Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
Message :
Credentials were not provided for detected SSH service.
```

10919 - Open Port Re-check -

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2021/07/23

Plugin Output

tcp/0

```
Port 110 was detected as being open but is now closed
Port 587 was detected as being open but is now closed
Port 143 was detected as being open but is now closed
Port 25 was detected as being open but is now closed
```

50845 - OpenSSL Detection -

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/25/smtp

50845 - OpenSSL Detection -

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/110/pop3

50845 - OpenSSL Detection -

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/143/imap

50845 - OpenSSL Detection -

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/465/smtp

50845 - OpenSSL Detection -

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/587/smtp

50845 - OpenSSL Detection -

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/993/imap

50845 - OpenSSL Detection -

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/995/pop3

10185 - POP Server Detection -

Synopsis

A POP server is listening on the remote port.

Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

See Also

https://en.wikipedia.org/wiki/Post_Office_Protocol

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/110/pop3

```
Remote POP server banner :

+OK Dovecot (Ubuntu) ready.
```

10185 - POP Server Detection -

Synopsis

A POP server is listening on the remote port.

Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

See Also

https://en.wikipedia.org/wiki/Post_Office_Protocol

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/995/pop3

```
Remote POP server banner :

+OK Dovecot (Ubuntu) ready.
```

42087 - POP3 Service STLS Command Support -

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote POP3 service supports the use of the 'STLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS
https://tools.ietf.org/html/rfc2595

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2021/02/24

Plugin Output

tcp/110/pop3

```
Here is the POP3 server's SSL certificate that Nessus was able to
collect after sending a 'STLS' command :

------------------------------ snip ------------------------------
Subject Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Issuer Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Serial Number: 00 FE D4 5E 15 69 D8 43 C1

Version: 3
```

```
Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 18 19:04:48 2016 GMT
Not Valid After: Oct 18 19:04:48 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 5A C3 7D DC 10 A9 E9 02 0B F4 23 A5 44 A9 4C 54 C4 0E
1C 67 9A CE 96 8E EB 66 F3 87 70 FC 2D 42 24 E1 39 9B FD 1B
F4 BF A2 2B 89 24 2D 66 47 76 04 96 EB 17 DD A6 77 67 1F 47
46 87 B1 A9 14 EE BB 1D 85 11 4A FB 68 55 5C 92 05 C8 D3 91
48 41 6B 5C F8 51 E5 C4 0B D1 40 B8 40 FB 16 FC 5C 92 E0 63
BA DB 29 A8 35 30 25 65 A6 0B 47 DB 82 DB 5D 6C 33 E2 E9 24
DD 1F EA 06 66 67 FB 8D 7E DE 6A 38 39 BF 80 9B E0 A4 B5 29
07 9C 96 BC 1B CC 70 44 20 E3 F7 FB 8D CA 2C 6C CD BD 3D 08
92 17 07 06 4C 9C D7 9A 28 33 F9 D8 DE 5E 63 CA EF 3C 6E E3
3B 64 C5 28 8B 39 A4 F8 E6 1B C2 74 FD B5 90 79 3E 96 F9 84
BF 38 69 74 47 35 A2 7D 16 81 CC 58 EB 7F DA 92 91 BB 65 23
3A 08 01 E7 25 09 BD B8 C6 F5 39 6D EC EB 44 1A A5 70 19 7F
E5 FA 70 BD 72 B8 98 BF B2 A7 F9 CC 8D 7B 5D E8 C3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 36 88 C5 13 AA 14 89 B6 2B E0 05 C4 C8 75 2C 97 57 E8 B9
B8 C5 69 B9 E1 F3 C6 DC 6E 19 85 FE ED 2D 82 FF A3 59 36 57
01 B8 F9 4A 93 A1 29 77 09 5D C0 D1 7E F0 D1 58 03 7D F8 6C
5D 81 69 CC CB B1 B4 FF 31 8E 57 DF 3F A1 E3 36 79 99 5D 9A
9B CC F6 41 D1 EE 6D 17 7C FD CB 76 16 28 79 E9 F3 3E CC 19
B2 08 5C 05 A1 51 80 B5 FD BC AA 99 03 87 C0 FC 96 85 93 7D
1B 52 A9 0A 71 3E 59 BA 5D 55 C5 7B 35 96 5A CF 5A 75 89 00
9F 94 89 CB ED 1D 3C D2 19 FE 05 EC B2 F9 49 DB 01 0A 8E 7E
4C C9 2B DD 50 B2 C9 D9 F3 A2 3F 9C 26 88 D8 94 04 D1 E4 77
15 DE FD 62 64 40 A6 77 27 B5 54 24 63 87 F6 3B 18 12 BF E5
2D 18 78 99 68 CF DC BC E0 4C FD FC 49 96 64 B8 35 A7 B9 C7
27 DF B5 57 7C 08 C6 A7 20 CA 83 97 1C 91 63 ED 75 50 71 96
8A D1 02 77 9C 01 2B 53 7B 6F 62 21 D0 69 3F 81 C5

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Basic Constraints (2.5.29.19)
Critical: 0
CA: TRUE


------------------------------ snip ------------------------------
```

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/rpc-portmapper

```
The following RPC services are available on TCP port 111 :

- program: 100000 (portmapper), version: 4
- program: 100000 (portmapper), version: 3
- 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/rpc-portmapper

```
The following RPC services are available on UDP port 111 :

- program: 100000 (portmapper), version: 4
- program: 100000 (portmapper), version: 3
- 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/39596/rpc-status

```
The following RPC services are available on TCP port 39596 :

- 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/49719/rpc-status

```
The following RPC services are available on UDP port 49719 :

- 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/rpc-portmapper

10223 - RPC portmapper Service Detection -

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS v2.0 Base Score

0.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:N)

References

CVE CVE-1999-0632

Plugin Information

Published: 1999/08/19, Modified: 2019/10/04

Plugin Output

udp/111/rpc-portmapper

10860 - SMB Use Host SID to Enumerate Local Users -

Synopsis

Nessus was able to enumerate local users.

Description

Using the host security identifier (SID), Nessus was able to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2019/07/08

Plugin Output

tcp/445/cifs

```
- nobody (id 501, Guest account)

Note that, in addition to the Administrator, Guest, and Kerberos
accounts, Nessus has enumerated local users with IDs between
1000 and 1200. To use a different range, edit the scan policy
and change the 'Enumerate Local Users: Start UID' and/or 'End UID'
preferences under 'Assessment->Windows' and re-run the scan. Only
UIDs between 1 and 2147483647 are allowed for this range.
```

54580 - SMTP Authentication Methods -

Synopsis

The remote mail server supports authentication.

Description

The remote SMTP server advertises that it supports authentication.

See Also

https://tools.ietf.org/html/rfc4422
https://tools.ietf.org/html/rfc4954

Solution

Review the list of methods and whether they're available over an encrypted channel.

Risk Factor

None

Plugin Information

Published: 2011/05/19, Modified: 2019/03/05

Plugin Output

tcp/25/smtp

```
The following authentication methods are advertised by the SMTP
server without encryption :
LOGIN
PLAIN

The following authentication methods are advertised by the SMTP
server with encryption :
LOGIN
PLAIN
```

54580 - SMTP Authentication Methods -

Synopsis

The remote mail server supports authentication.

Description

The remote SMTP server advertises that it supports authentication.

See Also

https://tools.ietf.org/html/rfc4422
https://tools.ietf.org/html/rfc4954

Solution

Review the list of methods and whether they're available over an encrypted channel.

Risk Factor

None

Plugin Information

Published: 2011/05/19, Modified: 2019/03/05

Plugin Output

tcp/587/smtp

```
The following authentication methods are advertised by the SMTP
server with encryption :
LOGIN
PLAIN
```

10263 - SMTP Server Detection -

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/25/smtp

```
Remote SMTP server banner :

220 umail.ifslab.ca ESMTP Postfix (Ubuntu)
```

10263 - SMTP Server Detection -

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/465/smtp

```
Remote SMTP server banner :

220 umail.ifslab.ca ESMTP Postfix (Ubuntu)
```

10263 - SMTP Server Detection -

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/587/smtp

```
Remote SMTP server banner :

220 umail.ifslab.ca ESMTP Postfix (Ubuntu)
```

42088 - SMTP Service STARTTLS Command Support -

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS
https://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

Plugin Output

tcp/25/smtp

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Country: ON
State/Province: Ontario
Locality: Toronto
Organization: Security Lab
Organization Unit: Education
Common Name: ifslab.ca
Email Address: root@ifslab.ca

Issuer Name:

Country: ON
State/Province: Ontario
Locality: Toronto
Organization: Security Lab
Organization Unit: Education
Common Name: ifslab.ca
Email Address: root@ifslab.ca

Serial Number: 00 88 10 28 13 22 A5 8F C2

Version: 1

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 04 17:43:51 2019 GMT
Not Valid After: Nov 01 17:43:51 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E7 B3 A8 71 10 61 F4 EB A0 51 1F 3D 22 7D 0F 5A 9F 50 DB
98 F8 8F B3 DD F4 D1 55 97 29 66 C7 C7 DF 95 7F 77 37 23 E8
A3 2C 6A 71 A1 C1 12 43 19 74 72 89 E6 32 22 2C 8D 5F C7 E8
B4 54 DC 7E C2 9C B4 AC EC 1A 48 61 00 76 1C 39 A8 1C 6B CD
79 C4 B2 33 89 5C 8D BC CD 26 22 40 85 89 8E 2C CC 0C C7 50
4F 03 31 F5 93 68 A2 FB 75 65 D6 1B 29 AB 8F 39 4F 84 33 01
50 68 B7 4A 72 84 27 81 BC 2A 34 DE 17 4C 64 DB FA C4 30 B4
07 A3 CC 3E E4 8F 04 2C DD 7D B3 3E B8 85 A5 A7 48 B0 4D 14
9E 90 8A 9F ED 4F ED A1 D5 48 AC 05 08 AA 47 65 F5 22 03 69
C0 E9 55 73 80 7C 4C B2 C9 AD 94 86 E0 31 81 34 AC 44 D0 F5
97 F0 F6 4F BA 8A DD BA E5 1D A5 41 5F FD 58 72 19 8A A7 7F
1F 1C AB AD 1B F1 10 9F E1 EC 70 1E BB BB 7D C9 D1 07 C8 C2
F2 C6 4A 5E CC B9 92 BF 99 1D 30 61 45 56 FB A2 D1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 86 78 CC B6 03 3F 0A DE 0A 77 F9 78 09 61 14 C5 F1 1E 88
94 06 12 19 1C 12 0E 63 8E C7 B6 3C 58 6A EA F7 AD 2C C4 95
DE 5F 46 AB 94 FF 44 08 4D 1C F3 77 36 A7 A8 63 A2 3F 60 37
C9 7E 42 98 71 87 AF BD 7E BF C5 39 8B 88 E5 89 AF 46 38 30
22 B1 A2 EC 0E A6 5B 6D 8B 10 69 E1 C2 AB 33 2C CA B6 F7 2D
A3 8B 34 0D 77 54 04 8A 14 67 28 64 65 8C 31 AE A4 D5 AF 7B
B2 CD BF 6B AE 12 01 92 32 CB AE 16 4C A7 8C A8 EA 60 8C A5
3E 80 5F 25 6D 63 2F E7 BB B9 49 AF B5 FE 7F BB 39 19 30 4F
46 60 5D 8D D3 05 63 93 4B 21 AA 8A 66 61 C2 95 20 F3 55 72
B3 10 AE D3 14 C9 9B C4 4E D1 DF 70 46 44 44 85 0C 02 0F EB
82 67 C1 F7 70 32 9B AF B4 23 B3 E2 F1 15 54 7F 7F 2F F5 38
9D 34 65 77 E6 E2 54 E2 B2 5C B3 A8 2D DF 2E F9 BF AB E3 68
79 70 11 C3 A0 FD A0 80 ED A4 AA 37 82 B4 DA 30 61

------------------------------ snip ------------------------------
```

42088 - SMTP Service STARTTLS Command Support -

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS
https://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

Plugin Output

tcp/587/smtp

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Country: ON
State/Province: Ontario
Locality: Toronto
Organization: Security Lab
Organization Unit: Education
Common Name: ifslab.ca
```

```
Email Address: root@ifslab.ca

Issuer Name:

Country: ON
State/Province: Ontario
Locality: Toronto
Organization: Security Lab
Organization Unit: Education
Common Name: ifslab.ca
Email Address: root@ifslab.ca

Serial Number: 00 88 10 28 13 22 A5 8F C2

Version: 1

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 04 17:43:51 2019 GMT
Not Valid After: Nov 01 17:43:51 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E7 B3 A8 71 10 61 F4 EB A0 51 1F 3D 22 7D 0F 5A 9F 50 DB
98 F8 8F B3 DD F4 D1 55 97 29 66 C7 C7 DF 95 7F 77 37 23 E8
A3 2C 6A 71 A1 C1 12 43 19 74 72 89 E6 32 22 2C 8D 5F C7 E8
B4 54 DC 7E C2 9C B4 AC EC 1A 48 61 00 76 1C 39 A8 1C 6B CD
79 C4 B2 33 89 5C 8D BC CD 26 22 40 85 89 8E 2C CC 0C C7 50
4F 03 31 F5 93 68 A2 FB 75 65 D6 1B 29 AB 8F 39 4F 84 33 01
50 68 B7 4A 72 84 27 81 BC 2A 34 DE 17 4C 64 DB FA C4 30 B4
07 A3 CC 3E E4 8F 04 2C DD 7D B3 3E B8 85 A5 A7 48 B0 4D 14
9E 90 8A 9F ED 4F ED A1 D5 48 AC 05 08 AA 47 65 F5 22 03 69
C0 E9 55 73 80 7C 4C B2 C9 AD 94 86 E0 31 81 34 AC 44 D0 F5
97 F0 F6 4F BA 8A DD BA E5 1D A5 41 5F FD 58 72 19 8A A7 7F
1F 1C AB AD 1B F1 10 9F E1 EC 70 1E BB BB 7D C9 D1 07 C8 C2
F2 C6 4A 5E CC B9 92 BF 99 1D 30 61 45 56 FB A2 D1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 86 78 CC B6 03 3F 0A DE 0A 77 F9 78 09 61 14 C5 F1 1E 88
94 06 12 19 1C 12 0E 63 8E C7 B6 3C 58 6A EA F7 AD 2C C4 95
DE 5F 46 AB 94 FF 44 08 4D 1C F3 77 36 A7 A8 63 A2 3F 60 37
C9 7E 42 98 71 87 AF BD 7E BF C5 39 8B 88 E5 89 AF 46 38 30
22 B1 A2 EC 0E A6 5B 6D 8B 10 69 E1 C2 AB 33 2C CA B6 F7 2D
A3 8B 34 0D 77 54 04 8A 14 67 28 64 65 8C 31 AE A4 D5 AF 7B
B2 CD BF 6B AE 12 01 92 32 CB AE 16 4C A7 8C A8 EA 60 8C A5
3E 80 5F 25 6D 63 2F E7 BB B9 49 AF B5 FE 7F BB 39 19 30 4F
46 60 5D 8D D3 05 63 93 4B 21 AA 8A 66 61 C2 95 20 F3 55 72
B3 10 AE D3 14 C9 9B C4 4E D1 DF 70 46 44 44 85 0C 02 0F EB
82 67 C1 F7 70 32 9B AF B4 23 B3 E2 F1 15 54 7F 7F 2F F5 38
9D 34 65 77 E6 E2 54 E2 B2 5C B3 A8 2D DF 2E F9 BF AB E3 68
79 70 11 C3 A0 FD A0 80 ED A4 AA 37 82 B4 DA 30 61

------------------------------ snip ------------------------------
```

70657 - SSH Algorithms and Languages Supported -

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

ecdsa-sha2-nistp256
ssh-dss
ssh-ed25519
ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

3des-cbc
aes128-cbc
aes128-ctr
aes128-gcm@openssh.com
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
aes256-gcm@openssh.com
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
chacha20-poly1305@openssh.com
rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

3des-cbc
aes128-cbc
aes128-ctr
aes128-gcm@openssh.com
aes192-cbc
aes192-ctr
```

```
aes256-cbc
aes256-ctr
aes256-gcm@openssh.com
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
chacha20-poly1305@openssh.com
rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-ripemd160
hmac-ripemd160-etm@openssh.com
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-ripemd160
hmac-ripemd160-etm@openssh.com
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

none
zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

none
zlib@openssh.com
```

149334 - SSH Password Authentication Accepted -

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported -

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

- 1.99
- 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled -

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2021/09/23

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information -

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8
SSH supported authentication : publickey,password
```

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/110/pop3

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/143/imap

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/465/smtp

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/587/smtp

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/993/imap

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported -

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/995/pop3

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

45410 - SSL Certificate 'commonName' Mismatch -

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/25/smtp

```
The host name known by Nessus is :

umail

The Common Name in the certificate is :

ifslab.ca
```

45410 - SSL Certificate 'commonName' Mismatch -

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/110/pop3

```
The host name known by Nessus is :

umail

The Common Name in the certificate is :

mailbox
```

45410 - SSL Certificate 'commonName' Mismatch -

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/143/imap

```
The host name known by Nessus is :

umail

The Common Name in the certificate is :

mailbox
```

45410 - SSL Certificate 'commonName' Mismatch -

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/465/smtp

```
The host name known by Nessus is :

umail

The Common Name in the certificate is :

ifslab.ca
```

45410 - SSL Certificate 'commonName' Mismatch -

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/587/smtp

```
The host name known by Nessus is :

umail

The Common Name in the certificate is :

ifslab.ca
```

45410 - SSL Certificate 'commonName' Mismatch -

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/993/imap

```
The host name known by Nessus is :

umail

The Common Name in the certificate is :

mailbox
```

45410 - SSL Certificate 'commonName' Mismatch -

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/995/pop3

```
The host name known by Nessus is :

umail

The Common Name in the certificate is :

mailbox
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
Subject Name:

Country: ON
State/Province: Ontario
Locality: Toronto
Organization: Security Lab
Organization Unit: Education
Common Name: ifslab.ca
Email Address: root@ifslab.ca

Issuer Name:

Country: ON
State/Province: Ontario
Locality: Toronto
Organization: Security Lab
Organization Unit: Education
Common Name: ifslab.ca
Email Address: root@ifslab.ca

Serial Number: 00 88 10 28 13 22 A5 8F C2

Version: 1

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 04 17:43:51 2019 GMT
Not Valid After: Nov 01 17:43:51 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E7 B3 A8 71 10 61 F4 EB A0 51 1F 3D 22 7D 0F 5A 9F 50 DB
98 F8 8F B3 DD F4 D1 55 97 29 66 C7 C7 DF 95 7F 77 37 23 E8
A3 2C 6A 71 A1 C1 12 43 19 74 72 89 E6 32 22 2C 8D 5F C7 E8
B4 54 DC 7E C2 9C B4 AC EC 1A 48 61 00 76 1C 39 A8 1C 6B CD
79 C4 B2 33 89 5C 8D BC CD 26 22 40 85 89 8E 2C CC 0C C7 50
4F 03 31 F5 93 68 A2 FB 75 65 D6 1B 29 AB 8F 39 4F 84 33 01
50 68 B7 4A 72 84 27 81 BC 2A 34 DE 17 4C 64 DB FA C4 30 B4
07 A3 CC 3E E4 8F 04 2C DD 7D B3 3E B8 85 A5 A7 48 B0 4D 14
9E 90 8A 9F ED 4F ED A1 D5 48 AC 05 08 AA 47 65 F5 22 03 69
C0 E9 55 73 80 7C 4C B2 C9 AD 94 86 E0 31 81 34 AC 44 D0 F5
97 F0 F6 4F BA 8A DD BA E5 1D A5 41 5F FD 58 72 19 8A A7 7F
1F 1C AB AD 1B F1 10 9F E1 EC 70 1E BB BB 7D C9 D1 07 C8 C2
F2 C6 4A 5E CC B9 92 BF 99 1D 30 61 45 56 FB A2 D1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 86 78 CC B6 03 3F 0A DE 0A 77 F9 78 09 61 14 C5 F1 1E 88
94 06 12 19 1C 12 0E 63 8E C7 B6 3C 58 6A EA F7 AD 2C C4 95
DE 5F 46 AB 94 FF 44 08 4D 1C F3 77 36 A7 A8 63 A2 3F 60 37
C9 7E 42 98 71 87 AF BD 7E BF C5 39 8B 88 E5 89 AF 46 38 30
22 B1 A2 EC 0E A6 5B 6D 8B 10 69 E1 C2 AB 33 2C CA B6 F7 2D
A3 8B 34 0D 77 54 04 8A 14 67 28 64 65 8C 31 AE A4 D5 AF 7B
B2 CD BF 6B AE 12 01 92 32 CB AE 16 4C A7 8C A8 EA 60 8C A5
3E 80 5F 25 6D 63 2F E7 BB B9 49 AF B5 FE 7F BB 39 19 30 4F
46 60 5D 8D D3 05 63 93 4B 21 AA 8A 66 61 C2 95 20 F3 55 72
B3 10 AE D3 14 C9 9B C4 4E D1 DF 70 46 44 44 85 0C 02 0F EB
82 67 C1 F7 70 32 9B AF B4 23 B3 E2 F1 15 54 7F 7F 2F F5 38
9D 34 65 77 E6 E2 54 E2 B2 5C B3 A8 2D DF 2E F9 BF AB E3 68
79 70 11 C3 A0 FD A0 80 ED A4 AA 37 82 B4 DA 30 61

Fingerprints :

SHA-256 Fingerprint: AA 3F 24 D6 C9 EE 79 DF 35 DB 17 5C 00 05 70 CD 53 65 AB 2B
99 E5 00 05 1F C1 50 E4 AE 3B 6E 55
SHA-1 Fingerprint: AB 96 54 20 D8 0A 20 23 6F 1B 52 4C 4B 91 75 D3 FE F8 8A E2
MD5 Fingerprint: F7 DF AF D0 99 6E 32 E7 4A 0B 17 94 2E BB E0 1F
```

```
PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDnDCCAoQCCQCIECgTIqWPwjANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCT04xEDAOBgNVBAgMB09udGFyaW8xEDAOBgNVBAcMB1Rvcm9udG8xFTATBgNVBAoMDFNlY3VyaXR5IExhYjESMBAGA1UECwwJRWF
-----END CERTIFICATE-----
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/110/pop3

```
Subject Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Issuer Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Serial Number: 00 FE D4 5E 15 69 D8 43 C1

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 18 19:04:48 2016 GMT
Not Valid After: Oct 18 19:04:48 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 5A C3 7D DC 10 A9 E9 02 0B F4 23 A5 44 A9 4C 54 C4 0E
1C 67 9A CE 96 8E EB 66 F3 87 70 FC 2D 42 24 E1 39 9B FD 1B
F4 BF A2 2B 89 24 2D 66 47 76 04 96 EB 17 DD A6 77 67 1F 47
46 87 B1 A9 14 EE BB 1D 85 11 4A FB 68 55 5C 92 05 C8 D3 91
48 41 6B 5C F8 51 E5 C4 0B D1 40 B8 40 FB 16 FC 5C 92 E0 63
BA DB 29 A8 35 30 25 65 A6 0B 47 DB 82 DB 5D 6C 33 E2 E9 24
DD 1F EA 06 66 67 FB 8D 7E DE 6A 38 39 BF 80 9B E0 A4 B5 29
07 9C 96 BC 1B CC 70 44 20 E3 F7 FB 8D CA 2C 6C CD BD 3D 08
92 17 07 06 4C 9C D7 9A 28 33 F9 D8 DE 5E 63 CA EF 3C 6E E3
3B 64 C5 28 8B 39 A4 F8 E6 1B C2 74 FD B5 90 79 3E 96 F9 84
BF 38 69 74 47 35 A2 7D 16 81 CC 58 EB 7F DA 92 91 BB 65 23
3A 08 01 E7 25 09 BD B8 C6 F5 39 6D EC EB 44 1A A5 70 19 7F
E5 FA 70 BD 72 B8 98 BF B2 A7 F9 CC 8D 7B 5D E8 C3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 36 88 C5 13 AA 14 89 B6 2B E0 05 C4 C8 75 2C 97 57 E8 B9
B8 C5 69 B9 E1 F3 C6 DC 6E 19 85 FE ED 2D 82 FF A3 59 36 57
01 B8 F9 4A 93 A1 29 77 09 5D C0 D1 7E F0 D1 58 03 7D F8 6C
5D 81 69 CC CB B1 B4 FF 31 8E 57 DF 3F A1 E3 36 79 99 5D 9A
9B CC F6 41 D1 EE 6D 17 7C FD CB 76 16 28 79 E9 F3 3E CC 19
B2 08 5C 05 A1 51 80 B5 FD BC AA 99 03 87 C0 FC 96 85 93 7D
1B 52 A9 0A 71 3E 59 BA 5D 55 C5 7B 35 96 5A CF 5A 75 89 00
9F 94 89 CB ED 1D 3C D2 19 FE 05 EC B2 F9 49 DB 01 0A 8E 7E
4C C9 2B DD 50 B2 C9 D9 F3 A2 3F 9C 26 88 D8 94 04 D1 E4 77
15 DE FD 62 64 40 A6 77 27 B5 54 24 63 87 F6 3B 18 12 BF E5
2D 18 78 99 68 CF DC BC E0 4C FD FC 49 96 64 B8 35 A7 B9 C7
27 DF B5 57 7C 08 C6 A7 20 CA 83 97 1C 91 63 ED 75 50 71 96
8A D1 02 77 9C 01 2B 53 7B 6F 62 21 D0 69 3F 81 C5

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Basic Constraints (2.5.29.19)
Critical: 0
CA: TRUE


Fingerprints :

SHA-256 Fingerprint: 1A 95 EF 0D B9 34 8C AD 92 35 5D 57 1C 93 E2 6F D1 66 EC 4E
5E 60 6A 96 59 FA C9 FF 79 56 18 65
SHA-1 Fingerprint: 01 3F 3B 98 98 0A 87 86 4A 94 FB 01 AB FF BB 64 42 3F AE 64
MD5 Fingerprint: 12 7D E2 2C 46 93 8C 53 DB CC 39 91 C8 29 29 12


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDkTCCAnmgAwIBAgIJAP7UXhVp2EPBMA0GCSqGSIb3DQEBCwUAMF8xHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEDAOBgNVBAsMB21haWxib3gxEDAOBgNVBAMMB21haWxib3gxGzAZBgkqhkiG9w0BCQE
-----END CERTIFICATE-----
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/143/imap

```
Subject Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Issuer Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Serial Number: 00 FE D4 5E 15 69 D8 43 C1

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 18 19:04:48 2016 GMT
Not Valid After: Oct 18 19:04:48 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 5A C3 7D DC 10 A9 E9 02 0B F4 23 A5 44 A9 4C 54 C4 0E
1C 67 9A CE 96 8E EB 66 F3 87 70 FC 2D 42 24 E1 39 9B FD 1B
F4 BF A2 2B 89 24 2D 66 47 76 04 96 EB 17 DD A6 77 67 1F 47
46 87 B1 A9 14 EE BB 1D 85 11 4A FB 68 55 5C 92 05 C8 D3 91
48 41 6B 5C F8 51 E5 C4 0B D1 40 B8 40 FB 16 FC 5C 92 E0 63
BA DB 29 A8 35 30 25 65 A6 0B 47 DB 82 DB 5D 6C 33 E2 E9 24
DD 1F EA 06 66 67 FB 8D 7E DE 6A 38 39 BF 80 9B E0 A4 B5 29
07 9C 96 BC 1B CC 70 44 20 E3 F7 FB 8D CA 2C 6C CD BD 3D 08
92 17 07 06 4C 9C D7 9A 28 33 F9 D8 DE 5E 63 CA EF 3C 6E E3
3B 64 C5 28 8B 39 A4 F8 E6 1B C2 74 FD B5 90 79 3E 96 F9 84
BF 38 69 74 47 35 A2 7D 16 81 CC 58 EB 7F DA 92 91 BB 65 23
3A 08 01 E7 25 09 BD B8 C6 F5 39 6D EC EB 44 1A A5 70 19 7F
E5 FA 70 BD 72 B8 98 BF B2 A7 F9 CC 8D 7B 5D E8 C3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 36 88 C5 13 AA 14 89 B6 2B E0 05 C4 C8 75 2C 97 57 E8 B9
B8 C5 69 B9 E1 F3 C6 DC 6E 19 85 FE ED 2D 82 FF A3 59 36 57
01 B8 F9 4A 93 A1 29 77 09 5D C0 D1 7E F0 D1 58 03 7D F8 6C
5D 81 69 CC CB B1 B4 FF 31 8E 57 DF 3F A1 E3 36 79 99 5D 9A
9B CC F6 41 D1 EE 6D 17 7C FD CB 76 16 28 79 E9 F3 3E CC 19
B2 08 5C 05 A1 51 80 B5 FD BC AA 99 03 87 C0 FC 96 85 93 7D
1B 52 A9 0A 71 3E 59 BA 5D 55 C5 7B 35 96 5A CF 5A 75 89 00
9F 94 89 CB ED 1D 3C D2 19 FE 05 EC B2 F9 49 DB 01 0A 8E 7E
4C C9 2B DD 50 B2 C9 D9 F3 A2 3F 9C 26 88 D8 94 04 D1 E4 77
15 DE FD 62 64 40 A6 77 27 B5 54 24 63 87 F6 3B 18 12 BF E5
2D 18 78 99 68 CF DC BC E0 4C FD FC 49 96 64 B8 35 A7 B9 C7
27 DF B5 57 7C 08 C6 A7 20 CA 83 97 1C 91 63 ED 75 50 71 96
8A D1 02 77 9C 01 2B 53 7B 6F 62 21 D0 69 3F 81 C5

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Basic Constraints (2.5.29.19)
Critical: 0
CA: TRUE


Fingerprints :

SHA-256 Fingerprint: 1A 95 EF 0D B9 34 8C AD 92 35 5D 57 1C 93 E2 6F D1 66 EC 4E
5E 60 6A 96 59 FA C9 FF 79 56 18 65
SHA-1 Fingerprint: 01 3F 3B 98 98 0A 87 86 4A 94 FB 01 AB FF BB 64 42 3F AE 64
MD5 Fingerprint: 12 7D E2 2C 46 93 8C 53 DB CC 39 91 C8 29 29 12


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDkTCCAnmgAwIBAgIJAP7UXhVp2EPBMA0GCSqGSIb3DQEBCwUAMF8xHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEDAOBgNVBAsMB21haWxib3gxEDAOBgNVBAMMB21haWxib3gxGzAZBgkqhkiG9w0BCQE
-----END CERTIFICATE-----
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/465/smtp

```
Subject Name:

Country: ON
```

```
State/Province: Ontario
Locality: Toronto
Organization: Security Lab
Organization Unit: Education
Common Name: ifslab.ca
Email Address: root@ifslab.ca

Issuer Name:

Country: ON
State/Province: Ontario
Locality: Toronto
Organization: Security Lab
Organization Unit: Education
Common Name: ifslab.ca
Email Address: root@ifslab.ca

Serial Number: 00 88 10 28 13 22 A5 8F C2

Version: 1

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 04 17:43:51 2019 GMT
Not Valid After: Nov 01 17:43:51 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E7 B3 A8 71 10 61 F4 EB A0 51 1F 3D 22 7D 0F 5A 9F 50 DB
98 F8 8F B3 DD F4 D1 55 97 29 66 C7 C7 DF 95 7F 77 37 23 E8
A3 2C 6A 71 A1 C1 12 43 19 74 72 89 E6 32 22 2C 8D 5F C7 E8
B4 54 DC 7E C2 9C B4 AC EC 1A 48 61 00 76 1C 39 A8 1C 6B CD
79 C4 B2 33 89 5C 8D BC CD 26 22 40 85 89 8E 2C CC 0C C7 50
4F 03 31 F5 93 68 A2 FB 75 65 D6 1B 29 AB 8F 39 4F 84 33 01
50 68 B7 4A 72 84 27 81 BC 2A 34 DE 17 4C 64 DB FA C4 30 B4
07 A3 CC 3E E4 8F 04 2C DD 7D B3 3E B8 85 A5 A7 48 B0 4D 14
9E 90 8A 9F ED 4F ED A1 D5 48 AC 05 08 AA 47 65 F5 22 03 69
C0 E9 55 73 80 7C 4C B2 C9 AD 94 86 E0 31 81 34 AC 44 D0 F5
97 F0 F6 4F BA 8A DD BA E5 1D A5 41 5F FD 58 72 19 8A A7 7F
1F 1C AB AD 1B F1 10 9F E1 EC 70 1E BB BB 7D C9 D1 07 C8 C2
F2 C6 4A 5E CC B9 92 BF 99 1D 30 61 45 56 FB A2 D1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 86 78 CC B6 03 3F 0A DE 0A 77 F9 78 09 61 14 C5 F1 1E 88
94 06 12 19 1C 12 0E 63 8E C7 B6 3C 58 6A EA F7 AD 2C C4 95
DE 5F 46 AB 94 FF 44 08 4D 1C F3 77 36 A7 A8 63 A2 3F 60 37
C9 7E 42 98 71 87 AF BD 7E BF C5 39 8B 88 E5 89 AF 46 38 30
22 B1 A2 EC 0E A6 5B 6D 8B 10 69 E1 C2 AB 33 2C CA B6 F7 2D
A3 8B 34 0D 77 54 04 8A 14 67 28 64 65 8C 31 AE A4 D5 AF 7B
B2 CD BF 6B AE 12 01 92 32 CB AE 16 4C A7 8C A8 EA 60 8C A5
3E 80 5F 25 6D 63 2F E7 BB B9 49 AF B5 FE 7F BB 39 19 30 4F
46 60 5D 8D D3 05 63 93 4B 21 AA 8A 66 61 C2 95 20 F3 55 72
B3 10 AE D3 14 C9 9B C4 4E D1 DF 70 46 44 44 85 0C 02 0F EB
82 67 C1 F7 70 32 9B AF B4 23 B3 E2 F1 15 54 7F 7F 2F F5 38
9D 34 65 77 E6 E2 54 E2 B2 5C B3 A8 2D DF 2E F9 BF AB E3 68
79 70 11 C3 A0 FD A0 80 ED A4 AA 37 82 B4 DA 30 61

Fingerprints :

SHA-256 Fingerprint: AA 3F 24 D6 C9 EE 79 DF 35 DB 17 5C 00 05 70 CD 53 65 AB 2B
99 E5 00 05 1F C1 50 E4 AE 3B 6E 55
SHA-1 Fingerprint: AB 96 54 20 D8 0A 20 23 6F 1B 52 4C 4B 91 75 D3 FE F8 8A E2
MD5 Fingerprint: F7 DF AF D0 99 6E 32 E7 4A 0B 17 94 2E BB E0 1F


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDnDCCAoQCCQCIECgTIqWPwjANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCT04xEDAOBgNVBAgMB09udGFyaW8xEDAOBgNVBAcMB1Rvcm9udG8xFTATBgNVBAoMDFNlY3VyaXR5IExhYjESMBAGA1UECwwJRWF
-----END CERTIFICATE-----
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/587/smtp

```
Subject Name:

Country: ON
State/Province: Ontario
Locality: Toronto
Organization: Security Lab
Organization Unit: Education
Common Name: ifslab.ca
Email Address: root@ifslab.ca

Issuer Name:

Country: ON
State/Province: Ontario
Locality: Toronto
Organization: Security Lab
Organization Unit: Education
Common Name: ifslab.ca
Email Address: root@ifslab.ca

Serial Number: 00 88 10 28 13 22 A5 8F C2

Version: 1

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 04 17:43:51 2019 GMT
Not Valid After: Nov 01 17:43:51 2029 GMT

Public Key Info:
```

```
Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E7 B3 A8 71 10 61 F4 EB A0 51 1F 3D 22 7D 0F 5A 9F 50 DB
98 F8 8F B3 DD F4 D1 55 97 29 66 C7 C7 DF 95 7F 77 37 23 E8
A3 2C 6A 71 A1 C1 12 43 19 74 72 89 E6 32 22 2C 8D 5F C7 E8
B4 54 DC 7E C2 9C B4 AC EC 1A 48 61 00 76 1C 39 A8 1C 6B CD
79 C4 B2 33 89 5C 8D BC CD 26 22 40 85 89 8E 2C CC 0C C7 50
4F 03 31 F5 93 68 A2 FB 75 65 D6 1B 29 AB 8F 39 4F 84 33 01
50 68 B7 4A 72 84 27 81 BC 2A 34 DE 17 4C 64 DB FA C4 30 B4
07 A3 CC 3E E4 8F 04 2C DD 7D B3 3E B8 85 A5 A7 48 B0 4D 14
9E 90 8A 9F ED 4F ED A1 D5 48 AC 05 08 AA 47 65 F5 22 03 69
C0 E9 55 73 80 7C 4C B2 C9 AD 94 86 E0 31 81 34 AC 44 D0 F5
97 F0 F6 4F BA 8A DD BA E5 1D A5 41 5F FD 58 72 19 8A A7 7F
1F 1C AB AD 1B F1 10 9F E1 EC 70 1E BB BB 7D C9 D1 07 C8 C2
F2 C6 4A 5E CC B9 92 BF 99 1D 30 61 45 56 FB A2 D1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 86 78 CC B6 03 3F 0A DE 0A 77 F9 78 09 61 14 C5 F1 1E 88
94 06 12 19 1C 12 0E 63 8E C7 B6 3C 58 6A EA F7 AD 2C C4 95
DE 5F 46 AB 94 FF 44 08 4D 1C F3 77 36 A7 A8 63 A2 3F 60 37
C9 7E 42 98 71 87 AF BD 7E BF C5 39 8B 88 E5 89 AF 46 38 30
22 B1 A2 EC 0E A6 5B 6D 8B 10 69 E1 C2 AB 33 2C CA B6 F7 2D
A3 8B 34 0D 77 54 04 8A 14 67 28 64 65 8C 31 AE A4 D5 AF 7B
B2 CD BF 6B AE 12 01 92 32 CB AE 16 4C A7 8C A8 EA 60 8C A5
3E 80 5F 25 6D 63 2F E7 BB B9 49 AF B5 FE 7F BB 39 19 30 4F
46 60 5D 8D D3 05 63 93 4B 21 AA 8A 66 61 C2 95 20 F3 55 72
B3 10 AE D3 14 C9 9B C4 4E D1 DF 70 46 44 44 85 0C 02 0F EB
82 67 C1 F7 70 32 9B AF B4 23 B3 E2 F1 15 54 7F 7F 2F F5 38
9D 34 65 77 E6 E2 54 E2 B2 5C B3 A8 2D DF 2E F9 BF AB E3 68
79 70 11 C3 A0 FD A0 80 ED A4 AA 37 82 B4 DA 30 61

Fingerprints :

SHA-256 Fingerprint: AA 3F 24 D6 C9 EE 79 DF 35 DB 17 5C 00 05 70 CD 53 65 AB 2B
99 E5 00 05 1F C1 50 E4 AE 3B 6E 55
SHA-1 Fingerprint: AB 96 54 20 D8 0A 20 23 6F 1B 52 4C 4B 91 75 D3 FE F8 8A E2
MD5 Fingerprint: F7 DF AF D0 99 6E 32 E7 4A 0B 17 94 2E BB E0 1F


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDnDCCAoQCCQCIECgTIqWPwjANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCT04xEDAOBgNVBAgMB09udGFyaW8xEDAOBgNVBAcMB1Rvcm9udG8xFTATBgNVBAoMDFNlY3VyaXR5IExhYjESMBAGA1UECwwJRWP
-----END CERTIFICATE-----
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/993/imap

```
Subject Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Issuer Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Serial Number: 00 FE D4 5E 15 69 D8 43 C1

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 18 19:04:48 2016 GMT
Not Valid After: Oct 18 19:04:48 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 5A C3 7D DC 10 A9 E9 02 0B F4 23 A5 44 A9 4C 54 C4 0E
1C 67 9A CE 96 8E EB 66 F3 87 70 FC 2D 42 24 E1 39 9B FD 1B
F4 BF A2 2B 89 24 2D 66 47 76 04 96 EB 17 DD A6 77 67 1F 47
46 87 B1 A9 14 EE BB 1D 85 11 4A FB 68 55 5C 92 05 C8 D3 91
48 41 6B 5C F8 51 E5 C4 0B D1 40 B8 40 FB 16 FC 5C 92 E0 63
BA DB 29 A8 35 30 25 65 A6 0B 47 DB 82 DB 5D 6C 33 E2 E9 24
DD 1F EA 06 66 67 FB 8D 7E DE 6A 38 39 BF 80 9B E0 A4 B5 29
07 9C 96 BC 1B CC 70 44 20 E3 F7 FB 8D CA 2C 6C CD BD 3D 08
92 17 07 06 4C 9C D7 9A 28 33 F9 D8 DE 5E 63 CA EF 3C 6E E3
3B 64 C5 28 8B 39 A4 F8 E6 1B C2 74 FD B5 90 79 3E 96 F9 84
BF 38 69 74 47 35 A2 7D 16 81 CC 58 EB 7F DA 92 91 BB 65 23
3A 08 01 E7 25 09 BD B8 C6 F5 39 6D EC EB 44 1A A5 70 19 7F
E5 FA 70 BD 72 B8 98 BF B2 A7 F9 CC 8D 7B 5D E8 C3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 36 88 C5 13 AA 14 89 B6 2B E0 05 C4 C8 75 2C 97 57 E8 B9
B8 C5 69 B9 E1 F3 C6 DC 6E 19 85 FE ED 2D 82 FF A3 59 36 57
01 B8 F9 4A 93 A1 29 77 09 5D C0 D1 7E F0 D1 58 03 7D F8 6C
5D 81 69 CC CB B1 B4 FF 31 8E 57 DF 3F A1 E3 36 79 99 5D 9A
9B CC F6 41 D1 EE 6D 17 7C FD CB 76 16 28 79 E9 F3 3E CC 19
B2 08 5C 05 A1 51 80 B5 FD BC AA 99 03 87 C0 FC 96 85 93 7D
1B 52 A9 0A 71 3E 59 BA 5D 55 C5 7B 35 96 5A CF 5A 75 89 00
9F 94 89 CB ED 1D 3C D2 19 FE 05 EC B2 F9 49 DB 01 0A 8E 7E
4C C9 2B DD 50 B2 C9 D9 F3 A2 3F 9C 26 88 D8 94 04 D1 E4 77
15 DE FD 62 64 40 A6 77 27 B5 54 24 63 87 F6 3B 18 12 BF E5
2D 18 78 99 68 CF DC BC E0 4C FD FC 49 96 64 B8 35 A7 B9 C7
27 DF B5 57 7C 08 C6 A7 20 CA 83 97 1C 91 63 ED 75 50 71 96
8A D1 02 77 9C 01 2B 53 7B 6F 62 21 D0 69 3F 81 C5

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
```

```
Subject Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Basic Constraints (2.5.29.19)
Critical: 0
CA: TRUE


Fingerprints :

SHA-256 Fingerprint: 1A 95 EF 0D B9 34 8C AD 92 35 5D 57 1C 93 E2 6F D1 66 EC 4E
5E 60 6A 96 59 FA C9 FF 79 56 18 65
SHA-1 Fingerprint: 01 3F 3B 98 98 0A 87 86 4A 94 FB 01 AB FF BB 64 42 3F AE 64
MD5 Fingerprint: 12 7D E2 2C 46 93 8C 53 DB CC 39 91 C8 29 29 12


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDkTCCAnmgAwIBAgIJAP7UXhVp2EPBMA0GCSqGSIb3DQEBCwUAMF8xHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEDAOBgNVBAsMB21haWxib3gxEDAOBgNVBAMMB21haWxib3gxGzAZBgkqhkiG9w0BCQE
-----END CERTIFICATE-----
```

10863 - SSL Certificate Information -

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/995/pop3

```
Subject Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Issuer Name:

Organization: Dovecot mail server
Organization Unit: mailbox
Common Name: mailbox
Email Address: root@mailbox

Serial Number: 00 FE D4 5E 15 69 D8 43 C1

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 18 19:04:48 2016 GMT
Not Valid After: Oct 18 19:04:48 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 5A C3 7D DC 10 A9 E9 02 0B F4 23 A5 44 A9 4C 54 C4 0E
1C 67 9A CE 96 8E EB 66 F3 87 70 FC 2D 42 24 E1 39 9B FD 1B
F4 BF A2 2B 89 24 2D 66 47 76 04 96 EB 17 DD A6 77 67 1F 47
46 87 B1 A9 14 EE BB 1D 85 11 4A FB 68 55 5C 92 05 C8 D3 91
48 41 6B 5C F8 51 E5 C4 0B D1 40 B8 40 FB 16 FC 5C 92 E0 63
BA DB 29 A8 35 30 25 65 A6 0B 47 DB 82 DB 5D 6C 33 E2 E9 24
DD 1F EA 06 66 67 FB 8D 7E DE 6A 38 39 BF 80 9B E0 A4 B5 29
07 9C 96 BC 1B CC 70 44 20 E3 F7 FB 8D CA 2C 6C CD BD 3D 08
92 17 07 06 4C 9C D7 9A 28 33 F9 D8 DE 5E 63 CA EF 3C 6E E3
3B 64 C5 28 8B 39 A4 F8 E6 1B C2 74 FD B5 90 79 3E 96 F9 84
BF 38 69 74 47 35 A2 7D 16 81 CC 58 EB 7F DA 92 91 BB 65 23
3A 08 01 E7 25 09 BD B8 C6 F5 39 6D EC EB 44 1A A5 70 19 7F
E5 FA 70 BD 72 B8 98 BF B2 A7 F9 CC 8D 7B 5D E8 C3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 36 88 C5 13 AA 14 89 B6 2B E0 05 C4 C8 75 2C 97 57 E8 B9
B8 C5 69 B9 E1 F3 C6 DC 6E 19 85 FE ED 2D 82 FF A3 59 36 57
01 B8 F9 4A 93 A1 29 77 09 5D C0 D1 7E F0 D1 58 03 7D F8 6C
5D 81 69 CC CB B1 B4 FF 31 8E 57 DF 3F A1 E3 36 79 99 5D 9A
9B CC F6 41 D1 EE 6D 17 7C FD CB 76 16 28 79 E9 F3 3E CC 19
B2 08 5C 05 A1 51 80 B5 FD BC AA 99 03 87 C0 FC 96 85 93 7D
1B 52 A9 0A 71 3E 59 BA 5D 55 C5 7B 35 96 5A CF 5A 75 89 00
9F 94 89 CB ED 1D 3C D2 19 FE 05 EC B2 F9 49 DB 01 0A 8E 7E
4C C9 2B DD 50 B2 C9 D9 F3 A2 3F 9C 26 88 D8 94 04 D1 E4 77
15 DE FD 62 64 40 A6 77 27 B5 54 24 63 87 F6 3B 18 12 BF E5
2D 18 78 99 68 CF DC BC E0 4C FD FC 49 96 64 B8 35 A7 B9 C7
27 DF B5 57 7C 08 C6 A7 20 CA 83 97 1C 91 63 ED 75 50 71 96
8A D1 02 77 9C 01 2B 53 7B 6F 62 21 D0 69 3F 81 C5

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 4F 6B 4C 18 17 1B DC 7F 35 E1 C8 46 1C C0 8D 61 11 96 50 46


Extension: Basic Constraints (2.5.29.19)
Critical: 0
CA: TRUE


Fingerprints :

SHA-256 Fingerprint: 1A 95 EF 0D B9 34 8C AD 92 35 5D 57 1C 93 E2 6F D1 66 EC 4E
5E 60 6A 96 59 FA C9 FF 79 56 18 65
SHA-1 Fingerprint: 01 3F 3B 98 98 0A 87 86 4A 94 FB 01 AB FF BB 64 42 3F AE 64
MD5 Fingerprint: 12 7D E2 2C 46 93 8C 53 DB CC 39 91 C8 29 29 12
```

```
PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDkTCCAnmgAwIBAgIJAP7UXhVp2EPBMA0GCSqGSIb3DQEBCwUAMF8xHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEDAOBgNVBAsMB21haWxib3gxEDAOBgNVBAMMB21haWxib3gxGzAZBgkqhkiG9w0BCQE
-----END CERTIFICATE-----
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
Here is the list of SSL CBC ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
DH-AES128-SHA256 0x00, 0x6C DH None AES-CBC(128) SHA256
DH-AES256-SHA256 0x00, 0x6D DH None AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```


70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/110/pop3

```
Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/143/imap

```
Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
```

```
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/465/smtp

```
Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
DH-AES128-SHA256 0x00, 0x6C DH None AES-CBC(128) SHA256
DH-AES256-SHA256 0x00, 0x6D DH None AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```


70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/587/smtp

```
Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
DH-AES128-SHA256 0x00, 0x6C DH None AES-CBC(128) SHA256
DH-AES256-SHA256 0x00, 0x6D DH None AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/993/imap

```
Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
http://www.nessus.org/u?cc4a822a
https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/995/pop3

```
Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/25/smtp

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1
```

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
DH-AES128-SHA256 0x00, 0xA6 DH None AES-GCM(128) SHA256
DH-AES256-SHA384 0x00, 0xA7 DH None AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
DH-AES128-SHA256 0x00, 0x6C DH None AES-CBC(128) SHA256
DH-AES256-SHA256 0x00, 0x6D DH None AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256


SSL Version : TLSv11
Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : TLSv1
Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
```

```
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : SSLv3
Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1
EXP-ADH-DES-CBC-SHA 0x00, 0x19 DH(512) None DES-CBC(40) SHA1 export
EXP-ADH-RC4-MD5 0x00, 0x17 DH(512) None RC4(40) MD5 export
ADH-DES-CBC-SHA 0x00, 0x1A DH None DES-CBC(56) SHA1
EXP-DES-CBC-SHA 0x00, 0x08 RSA(512) RSA DES-CBC(40) SHA1 export
EXP-RC2-CBC-MD5 0x00, 0x06 RSA(512) RSA RC2-CBC(40) MD5 export
EXP-RC4-MD5 0x00, 0x03 RSA(512) RSA RC4(40) MD5 export
DES-CBC-SHA 0x00, 0x09 RSA RSA DES-CBC(56) SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/110/pop3

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
------------------------------ ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256


SSL Version : TLSv11
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
------------------------------ ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
------------------------------ ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : SSLv3
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
------------------------------ ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
```

```
The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/143/imap

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256


SSL Version : TLSv11
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)
```

```
Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : SSLv3
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/465/smtp

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
DH-AES128-SHA256 0x00, 0xA6 DH None AES-GCM(128) SHA256
DH-AES256-SHA384 0x00, 0xA7 DH None AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
```

```
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
DH-AES128-SHA256 0x00, 0x6C DH None AES-CBC(128) SHA256
DH-AES256-SHA256 0x00, 0x6D DH None AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256


SSL Version : TLSv11
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : SSLv3
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
```

```
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/587/smtp

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
DH-AES128-SHA256 0x00, 0xA6 DH None AES-GCM(128) SHA256
DH-AES256-SHA384 0x00, 0xA7 DH None AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
DH-AES128-SHA256 0x00, 0x6C DH None AES-CBC(128) SHA256
DH-AES256-SHA256 0x00, 0x6D DH None AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256


SSL Version : TLSv11
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
```

```
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : SSLv3
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ADH-DES-CBC3-SHA 0x00, 0x1B DH None 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
AECDH-DES-CBC3-SHA 0xC0, 0x17 ECDH None 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ADH-AES128-SHA 0x00, 0x34 DH None AES-CBC(128) SHA1
ADH-AES256-SHA 0x00, 0x3A DH None AES-CBC(256) SHA1
ADH-CAMELLIA128-SHA 0x00, 0x46 DH None Camellia-CBC(128) SHA1
ADH-CAMELLIA256-SHA 0x00, 0x89 DH None Camellia-CBC(256) SHA1
ADH-RC4-MD5 0x00, 0x18 DH None RC4(128) MD5
ADH-SEED-SHA 0x00, 0x9B DH None SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AECDH-AES128-SHA 0xC0, 0x18 ECDH None AES-CBC(128) SHA1
AECDH-AES256-SHA 0xC0, 0x19 ECDH None AES-CBC(256) SHA1
AECDH-RC4-SHA 0xC0, 0x16 ECDH None RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/993/imap

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256


SSL Version : TLSv11
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : SSLv3
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
```

```
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

21643 - SSL Cipher Suites Supported -

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/995/pop3

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256


SSL Version : TLSv11
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
```

```
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : TLSv1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
------------------------------ ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1


SSL Version : SSLv3
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
------------------------------ ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/25/smtp

```
Here is the list of SSL PFS ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EXP-EDH-RSA-DES-CBC-SHA 0x00, 0x14 DH(512) RSA DES-CBC(40) SHA1 export
EDH-RSA-DES-CBC-SHA 0x00, 0x15 DH RSA DES-CBC(56) SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
```

```
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/110/pop3

```
Here is the list of SSL PFS ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- ---------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```


57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/143/imap

```
Here is the list of SSL PFS ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/465/smtp

```
Here is the list of SSL PFS ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/587/smtp

```
Here is the list of SSL PFS ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/993/imap

```
Here is the list of SSL PFS ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384

The fields above are :

{Tenable ciphername}
```

```
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported -

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/995/pop3

```
Here is the list of SSL PFS ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
EDH-RSA-DES-CBC3-SHA 0x00, 0x16 DH RSA 3DES-CBC(168) SHA1
ECDHE-RSA-DES-CBC3-SHA 0xC0, 0x12 ECDH RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC
---------------------- ---------- --- ---- --------------------- ---
DHE-RSA-AES128-SHA256 0x00, 0x9E DH RSA AES-GCM(128) SHA256
DHE-RSA-AES256-SHA384 0x00, 0x9F DH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
DHE-RSA-AES128-SHA 0x00, 0x33 DH RSA AES-CBC(128) SHA1
DHE-RSA-AES256-SHA 0x00, 0x39 DH RSA AES-CBC(256) SHA1
DHE-RSA-CAMELLIA128-SHA 0x00, 0x45 DH RSA Camellia-CBC(128) SHA1
DHE-RSA-CAMELLIA256-SHA 0x00, 0x88 DH RSA Camellia-CBC(256) SHA1
DHE-RSA-SEED-SHA 0x00, 0x9A DH RSA SEED-CBC(128) SHA1
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
ECDHE-RSA-RC4-SHA 0xC0, 0x11 ECDH RSA RC4(128) SHA1
DHE-RSA-AES128-SHA256 0x00, 0x67 DH RSA AES-CBC(128) SHA256
DHE-RSA-AES256-SHA256 0x00, 0x6B DH RSA AES-CBC(256) SHA256
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

94761 - SSL Root Certification Authority Certificate Information -

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/110/pop3

```
The following root Certification Authority certificate was found :

|-Subject : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Issuer : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Valid From : Oct 18 19:04:48 2016 GMT
|-Valid To : Oct 18 19:04:48 2026 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information -

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/143/imap

```
The following root Certification Authority certificate was found :

|-Subject : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Issuer : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Valid From : Oct 18 19:04:48 2016 GMT
|-Valid To : Oct 18 19:04:48 2026 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information -

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/993/imap

```
The following root Certification Authority certificate was found :

|-Subject : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Issuer : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Valid From : Oct 18 19:04:48 2016 GMT
|-Valid To : Oct 18 19:04:48 2026 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information -

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/995/pop3

```
The following root Certification Authority certificate was found :

|-Subject : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Issuer : O=Dovecot mail server/OU=mailbox/CN=mailbox/E=root@mailbox
|-Valid From : Oct 18 19:04:48 2016 GMT
|-Valid To : Oct 18 19:04:48 2026 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

51891 - SSL Session Resume Supported -

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/25/smtp

```
This port supports resuming SSLv3 / TLSv1 / TLSv1 / TLSv1 sessions.
```

51891 - SSL Session Resume Supported -

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/465/smtp

```
This port supports resuming SSLv3 / TLSv1 / TLSv1 / TLSv1 sessions.
```

51891 - SSL Session Resume Supported -

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/587/smtp

```
This port supports resuming SSLv3 / TLSv1 / TLSv1 / TLSv1 sessions.
```

25240 - Samba Server Detection -

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

https://www.samba.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

104887 - Samba Version -

Synopsis

It was possible to obtain the samba version from the remote operating system.

Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/11/30, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote Samba Version is : Samba 4.3.11-Ubuntu
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) -

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/25/smtp

```
An SMTP server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/110/pop3

```
A POP3 server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/143/imap

```
An IMAP server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/465/smtp

```
A TLSv1 server answered on this port.
```

tcp/465/smtp

```
An SMTP server is running on this port through TLSv1.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/587/smtp

```
An SMTP server is running on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/993/imap

```
An IMAP server is running on this port through SSLv3.
```

tcp/993/imap

```
An SSLv3 server answered on this port.
```

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

tcp/995/pop3

```
A POP3 server is running on this port through TLSv1.
```

tcp/995/pop3

```
A TLSv1 server answered on this port.
```

25220 - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

121010 - TLS Version 1.1 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/25/smtp

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/110/pop3

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/143/imap

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/465/smtp

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/587/smtp

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/993/imap

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection -

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/995/pop3

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection -

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/25/smtp

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection -

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/110/pop3

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection -

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/143/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection -

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/465/smtp

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection -

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/587/smtp

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection -

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/993/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection -

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/995/pop3

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided -

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2021/08/30

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 172.16.1.200 to 172.16.11.30 :
172.16.1.200
172.16.1.1
172.16.11.30

Hop Count: 2
```

66293 - Unix Operating System on Extended Support -

Synopsis

The remote host is running an operating system that is on extended support.

Description

According to its version, the remote host uses a Unix or Unix-like operating system that has transitioned to an extended portion in its support life cycle. Continued access to new security updates requires payment of an additional fee and / or configuration changes to the package management tool. Without that, the host likely will be missing security updates.

Solution

Ensure that the host subscribes to the vendor's extended support plan and continues to receive security updates.

Risk Factor

None

References

XREF IAVA:0001-A-0648

Plugin Information

Published: 2013/05/02, Modified: 2021/06/09

Plugin Output

tcp/0

```
Ubuntu 14.04 support ends on 2019-04-30 (end of maintenance) / 2022-04-30 (end of extended security maintenance).
```

135860 - WMI Not Available -

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2021/11/12

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

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: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 5 NetBIOS names have been gathered :

UMAIL = Computer name
UMAIL = Messenger Service
UMAIL = File Server Service
WORKGROUP = Workgroup / Domain name
WORKGROUP = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

52703 - vsftpd Detection -

Synopsis

An FTP server is listening on the remote port.

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

http://vsftpd.beasts.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/03/17, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
Source : 220 (vsFTPd 3.0.2)
Version : 3.0.2
```