

Metasploitable Vulnerabilities

Report generated by Nessus™

Sat, 02 Sep 2023 22:59:48 CEST

TABLI	OF CONTENTS
Vulnerabilities by Host	
• 192.168.50.3	4



8	5	23	8	126
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

Netbios Name: METASPLOITABLE IP: 192.168.50.3

MAC Address: 08:00:27:BC:3B:1B

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

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

VPR Score

9.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

XREF CISA-KNOWN-EXPLOITED:2022/03/17

XREF CEA-ID:CEA-2020-0021

Plugin Information

Published: 2020/03/24, Modified: 2023/07/17

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....1
```

```
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..
                                                          .en-US, en; q=0.5.
        OE 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00
0x0070: A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45
                                                            ....O...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 0x00C0: 7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D
                                                            max-age=0....Mo
                                                            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
t...!javax.servl
                                                            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 0x0170: 74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65
                                                            ..."javax.servle
                                                            t.include.servle
0x0180: 74 5F 70 61 74 68 00 00 00 00 FF
                                                            t_path....
This produced the following truncated output (limite [...]
```

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

VPR Score

7.4

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

VPR Score

7.4

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

VPR Score

7.4

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/postgresal

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

VPR Score

5.9

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: 2023/08/30

Plugin Output

udp/2049/rpc-nfs

The following NFS shares could be mounted :

+ /media

```
+ Contents of /media:
- .
- ..
- cdrom
- cdrom0
- floppy
- floppy0
```

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

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: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/25/smtp

	rver supports at 1	east one cipner	£ •		
Low Strength Ciphers (<= 64	-bit key)				
Name	Code	KEX	Auth	Encryption	N
EXP-RC2-CBC-MD5 export		RSA(512)	RSA	RC2-CBC(40)	
EXP-RC4-MD5 export		RSA(512)	RSA	RC4(40)	M
Medium Strength Ciphers (> 6	64-bit and < 112-b	it key, or 3DES	5)		
Name	Code	KEX	Auth	Encryption	
DES-CBC3-MD5		RSA		3DES-CBC(168)	
High Strength Ciphers (>= 1	12-bit key)				
Name	Code	KEX	Auth	Encryption	_ I
RC4-MD5		RSA	RSA	RC4 (128)	- I
e fields above are :					
{Tenable ciphername} {Cipher ID code} Kex={key exchange}					
Auth={authentication} Encrypt={symmetric encryptic MAC={message authentication {export flag}	code}				
<pre>Encrypt={symmetric encryptic MAC={message authentication</pre>	rver supports at l				
Encrypt={symmetric encryption MAC={message authentication {export flag} SSLv3 is enabled and the semplanation: TLS 1.0 and SSL 3	rver supports at 1				
Encrypt={symmetric encryption MAC={message authentication {export flag} SSLv3 is enabled and the serval and s	rver supports at 13.0 cipher suites : -bit key) Code	may be used wit	th SSLv3		
Encrypt={symmetric encryption MAC={message authentication {export flag} SSLv3 is enabled and the second and th	rver supports at 13.0 cipher suites : -bit key)	may be used wit	eh SSLv3	Encryption DES-CBC(40)	<u>M</u>

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

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: 2005/10/12, Modified: 2022/04/04

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
                                                             RSA
                                                                     3DES-CBC(168)
   DES-CBC3-SHA
                                                            RSA 3DES-CBC(168)
                                                RSA
 High Strength Ciphers (>= 112-bit key)
                                                            Auth Encryption
   Name
                               Code
                                               KEX
                                                                                           MAC
   DHE-RSA-AES128-SHA
                                                             RSA
                                                                    AES-CBC(128)
                                                DH
   DHE-RSA-AES256-SHA
                                                DH
                                                             RSA AES-CBC(256)
  AES128-SHA
                                                RSA
                                                            RSA AES-CBC(128)
 SHA1
                                                             RSA
                                                                    AES-CBC(256)
   AES256-SHA
                                                RSA
                                                             RSA
                                                                    RC4 (128)
   RC4 - SHA
                                                RSA
 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}
```

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: 2023/07/07

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

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)
VPR Score
5.2
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

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

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

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

Description

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

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

See Also

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

https://sweet32.info

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

6.1

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

tcp/25/smtp

Medium Strength Ciphers (> 64-k	oit and	< 112	-bit :	key, or 3DES)			
Name	Code			KEX	Auth	Encryption	MAC
DES-CBC3-MD5		0x00,		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 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)

VPR Score

6.1

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

tcp/5432/postgresql

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

        Code
        KEX
        Auth
        Encryption

        0x00, 0x16
        DH
        RSA
        3DES-CBC(168)

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

VPR Score

6.7

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

VPR Score
6.7

CVSS v2.0 Base Score

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

References

CVF CVF-1999-0651

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/08/30, Modified: 2022/04/11

Plugin Output

tcp/513/rlogin

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)
VPR Score
4.0
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-2010-0386 CVE XREF CERT:288308 XREF CERT:867593 XREF CWE:16 XRFF CWF: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 /Nessus252121670.html HTTP/1.1
Connection: Close
Host: 192.168.50.3
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: Sat, 02 Sep 2023 20:53:36 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 /Nessus252121670.html HTTP/1.1
```

```
Connection: Keep-Alive
Host: 192.168.50.3
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) **VPR** Score 3.6 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

192.168.50.3

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

STIG Severity

ı

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

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 Medium CVSS v3.0 Base Score 5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) CVSS v3.0 Temporal Score 5.3 (CVSS:3.0/E:P/RL:O/RC:C) **VPR Score** 5.1 CVSS v2.0 Base Score 4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P) CVSS v2.0 Temporal Score 3.4 (CVSS2#E:POC/RL:OF/RC:C) STIG Severity

References

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

Plugin Information

Published: 2020/05/22, Modified: 2023/03/23

Plugin Output

udp/53/dns

Installed version : 9.4.2
Fixed version : 9.11.19

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: 2022/10/05

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

VPR Score

6.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.1 (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
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) **VPR** Score 3.6 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

Plugin Information

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

Plugin Output

tcp/25/smtp

Low Strength Ciphers (<= 64	-bit key)				
Name	Code	KEX	Auth	Encryption	I
EXP-ADH-DES-CBC-SHA	0x00, 0x19	DH(512)	None	DES-CBC(40)	
HA1 export EXP-ADH-RC4-MD5	0x00, 0x17	DH(512)	None	RC4(40)	
export ADH-DES-CBC-SHA HA1	0x00, 0x1A	DH	None	DES-CBC(56)	
Medium Strength Ciphers (>	64-bit and < 112-b	it key, or 3DE	S)		
Name	Code	KEX	Auth	2 2 2 3	
ADH-DES-CBC3-SHA HA1	0x00, 0x1B	DH	None	3DES-CBC(168)	
High Strength Ciphers (>= 1	12-bit key)				
Name	Code	KEX	Auth	Encryption	
ADH-AES128-SHA HA1	0x00, 0x34	 DH	None	AES-CBC(128)	
ADH-AES256-SHA HA1	0x00, 0x3A	DH	None	AES-CBC(256)	
ADH-RC4-MD5	0x00, 0x18	DH	None	RC4 (128)	
e fields above are :					
{Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryptic MAC={message authentication {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/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain/E=root@ubuntu804
```

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

base.localdomain

```
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-

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:

192.168.50.3

192.168.50.3

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:

192.168.50.3

192.168.50.3

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)

VPR Score

4.4

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)
                            Code KEX Auth Encryption
   EXP-RC2-CBC-MD5
                           0x04, 0x00, 0x80 RSA(512)
                                                     RSA
                                                            RC2-CBC(40)
     export
                          0x02, 0x00, 0x80 RSA(512) RSA RC4(40)
   EXP-RC4-MD5
                                                                                 MD5
    export
 High Strength Ciphers (>= 112-bit key)
                            KEX
                                                    Auth Encryption
   Name
                            Code
                                                                                 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)

VPR Score

3.6

CVSS v2.0 Base Score

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

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)
                                                         Auth Encryption
                               Code KEX
                               Code
   Name
                                                                                         MAC
                                                           RSA
                              0x02, 0x00, 0x80 RSA(512)
   EXP-RC4-MD5
                                                                    RC4(40)
                                                                                         MD5
     export
   EXP-ADH-RC4-MD5
                             0 \times 00, 0 \times 17
                                                           None RC4(40)
                                             DH(512)
                                                                                         MD5
     export
   EXP-RC4-MD5
                             0x00, 0x03 RSA(512)
                                                           RSA RC4(40)
                                                                                         MD5
    export
 High Strength Ciphers (>= 112-bit key)
                               KEX
                                                         Auth Encryption
   Name
                               Code
                                                                                         MAC
                                                          RSA
                              0x01, 0x00, 0x80 RSA
   RC4-MD5
                                                                    RC4 (128)
                                                                                         MD5
                                                         None RC4 (128)
RSA RC4 (128)
RSA RC4 (128)
                              0x00, 0x18 DH
0x00, 0x04 RSA
0x00, 0x05 RSA
   ADH-RC4-MD5
                                                                                         MD5
   RC4-MD5
   RC4 - SHA
 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)

VPR Score

3.6

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)
                                                        Auth Encryption
                                          KEX
                               Code
   Name
                                                                                         MAC
                                                           RSA RC4 (128)
   RC4 - SHA
                              0x00, 0x05
                                             RSA
SHA1
The fields above are :
 {Tenable ciphername}
 {Cipher ID code}
 Kex={key exchange}
 Auth={authentication}
 Encrypt={symmetric encryption method}
 MAC={message authentication code}
 {export flag}
```

57582 - SSL Self-Signed Certificate

Synopsis

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

Description

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/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:

 $|\mbox{-Subject: C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain} \\$

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 v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/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:

 $|\mbox{-Subject: C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-base.localdomain} \\$

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

ere is the list of weak SSL c		pported	by the remo	ote server :		
Low Strength Ciphers (<= 64-)	oit key)					
Name	Code		KEX	Auth	2 1	
EXP-RC2-CBC-MD5 export	0x04,	0x00,	0x80 RSA(512	2) RSA	RC2-CBC(40)	MD
EXP-RC4-MD5 export	0x02,	0x00,	0x80 RSA(512	2) RSA	RC4 (40)	MD
EXP-EDH-RSA-DES-CBC-SHA SHA1 export	0x00,	0x14	DH(512)) RSA	DES-CBC(40)	
EDH-RSA-DES-CBC-SHA HA1	0x00,	0x15	DH	RSA	DES-CBC(56)	
EXP-ADH-DES-CBC-SHA HA1 export	0x00,	0x19	DH(512)) None	DES-CBC(40)	
EXP-ADH-RC4-MD5	0x00,	0x17	DH(512)) None	RC4(40)	MD
export ADH-DES-CBC-SHA HA1	0x00,	0x1A	DH	None	DES-CBC(56)	
EXP-DES-CBC-SHA	0x00,	0x08	RSA(512	2) RSA	DES-CBC(40)	
EXP-RC2-CBC-MD5	0x00,	0x06	RSA (512	2) RSA	RC2-CBC(40)	MD
export EXP-RC4-MD5	0x00,	0x03	RSA (512	2) RSA	RC4(40)	MD
export DES-CBC-SHA HA1	0x00,	0x09	RSA	RSA	DES-CBC(56)	
ne fields above are :						
{Tenable ciphername} {Cipher ID code}						
Kex={key exchange}						
<pre>Auth={authentication} Encrypt={symmetric encryptio:</pre>	n mothodl					
MAC={message authentication						
{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

VPR Score

4.5

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

Plugin Output

tcp/25/smtp

```
EXPORT_RSA cipher suites supported by the remote server :
 Low Strength Ciphers (<= 64-bit key)
                                           KEX Auth Encryption
                             Code
   Name
                                                                                    MAC
                             . . . . . . . . . . .
                                                                ______
                                                       RSA DES-CBC(40)
  EXP-DES-CBC-SHA
                            0x00, 0x08
                                           RSA(512)
 SHA1 export
  EXP-RC2-CBC-MD5
                                                              RC2-CBC(40)
                           0x00, 0x06
                                                                                  MD5
                                          RSA(512)
                                                       RSA
     export
                            0x00, 0x03
                                                              RC4(40)
                                                                                    MD5
   EXP-RC4-MD5
                                           RSA(512)
                                                       RSA
     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)

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/25/smtp

 ${\tt TLSv1}$ is enabled and the server supports at least one cipher.

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF CWE:327

Plugin Information

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

Plugin Output

tcp/5432/postgresql

 $\ensuremath{\operatorname{TLSv1}}$ 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

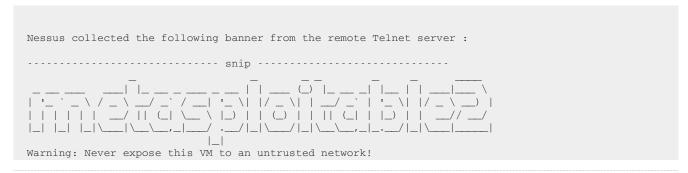
5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

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

Plugin Output

tcp/23/telnet



70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

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

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

Solution

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

Risk Factor

Low

VPR Score

2.5

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 32319

CVE CVE-2008-5161

XREF CERT:958563

XREF CWE:200

Plugin Information

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

Plugin Output

tcp/22/ssh

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :
 3des-cbc
 aes128-cbc
 aes192-cbc
 aes256-cbc
 blowfish-cbc
 cast128-cbc
 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

192.168.50.3

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

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Description The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections. See Also https://weakdh.org/ Solution Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater. Risk Factor low CVSS v3.0 Base Score 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N) CVSS v3.0 Temporal Score 3.2 (CVSS:3.0/E:U/RL:O/RC:C) **VPR** Score 4.5 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 1.9 (CVSS2#E:U/RL:OF/RC:C) References BID 74733

CVE CVE-2015-4000

XREF CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/05/28, Modified: 2022/12/05

Plugin Output

tcp/25/smtp

```
Vulnerable connection combinations:

SSL/TLS version : SSLv3
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

SSL/TLS version : TLSv1.0
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)
```

83738 - SSL/TLS EXPORT DHE <= 512-bit Export Cipher Suites Supported (Logjam

Synopsis
The remote host supports a set of weak ciphers.
Description
The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.
A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.
See Also
https://weakdh.org/
Solution
Reconfigure the service to remove support for EXPORT_DHE cipher suites.
Risk Factor
Low
CVSS v3.0 Base Score
3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)
CVSS v3.0 Temporal Score
3.2 (CVSS:3.0/E:U/RL:O/RC:C)
VPR Score
4.5
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

XREF CEA-ID:CEA-2021-0004

Plugin Information

Published: 2015/05/21, Modified: 2022/12/05

Plugin Output

tcp/25/smtp

```
EXPORT_DHE cipher suites supported by the remote server :
 Low Strength Ciphers (<= 64-bit key)
                                                            Auth Encryption
RSA DES-CBC(40)
                                               KEX
                                                                                          MAC
  EXP-EDH-RSA-DES-CBC-SHA
                              0x00, 0x14
                                             DH(512)
 SHA1 export
  EXP-ADH-DES-CBC-SHA
                              0x00, 0x19
                                              DH(512)
                                                            None DES-CBC(40)
        export
                              0x00, 0x17
                                                            None RC4 (40)
  EXP-ADH-RC4-MD5
                                              DH(512)
                                                                                          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

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

CVSS v3.0 Temporal Score

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

VPR Score

5.3

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

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

References

BID 70574

CVE CVE-2014-3566 XREF CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2023/06/23

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

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

CVSS v3.0 Temporal Score

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

VPR Score

5.3

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

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

References

BID 70574

CVE CVE-2014-3566 XREF CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2023/06/23

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.

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.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2022/03/21

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

Plugin Information

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

Plugin Output

tcp/80/www

URL : http://192.168.50.3/ Version : 2.2.99

: Server: Apache/2.2.8 (Ubuntu) DAV/2 Source

backported : 1

modules : DAV/2
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/2121/ftp
Give Nessus gradentials 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: 2022/04/11
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 gradentials 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: 2023/07/27

Plugin Output

tcp/0

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

cpe:/o:canonical:ubuntu_linux:8.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system:

cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server cpe:/a:apache:http_server:2.2.99 -> Apache Software Foundation Apache HTTP Server cpe:/a:isc:bind:9.4. -> ISC BIND cpe:/a:isc:bind:9.4.2 -> ISC BIND cpe:/a:mysql:mysql:5.0.51a-3ubuntu5 -> MySQL MySQL cpe:/a:mysql:mysql:5.0.51a-3ubuntu5 -> MySQL MySQL cpe:/a:openbsd:openssh:4.7 -> OpenBSD OpenSSH cpe:/a:php:php:5.2.4 -> PHP PHP cpe:/a:php:php:5.2.4 -2ubuntu5.10 -> PHP PHP cpe:/a:postgresql:postgresql -> PostgreSQL cpe:/a:samba:samba:3.0.20 -> Samba Samba
```

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: 2022/10/12

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

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

metasploitable

udp/53/dns

The remote host name is:

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

Remote device type : general-purpose Confidence level : 95

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: 08:00:27:BC:3B:1B: PCS Systemtechnik GmbH

86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

The following is a consolidated list of detected MAC addresses:

- 08:00:27:BC:3B:1B

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

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

Solution

n/a

Risk Factor

None

References

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

Plugin Information

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

Plugin Output

tcp/21/ftp

```
The remote FTP banner is:
220 (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

References

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

Plugin Information

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

Plugin Output

tcp/2121/ftp

```
The remote FTP banner is:
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.50.3]
```

10107 - HTTP Server Type and Version

Synopsis	
A web serv	ver is running on the remote host.
Description	n
This plugir	attempts to determine the type and the version of the remote web server.
Solution	
n/a	
Risk Facto	r
None	
References	5
XREF	IAVT:0001-T-0931
Plugin Info	ormation
Published:	2000/01/04, Modified: 2020/10/30
Plugin Out	put
tcp/80/ww	w
The remo	te web server type is :
Apache/2	.2.8 (Ubuntu) DAV/2

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: Sat, 02 Sep 2023 20:53:44 GMT
 Server: Apache/2.2.8 (Ubuntu) DAV/2
 X-Powered-By: PHP/5.2.4-2ubuntu5.10
 Keep-Alive: timeout=15, max=100
 Connection: Keep-Alive
 Transfer-Encoding: chunked
 Content-Type: text/html
Response Body :
<html><head><title>Metasploitable2 - Linux</title></head><body>
```

```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

<a href="/twiki/">TWiki</a>
<a href="/phpMyAdmin/">phpMyAdmin</a>
<a href="/phpMyAdmin/">Phutillidae</a>
<a href="/dvwa/">DVWA</a>
<a href="/dvwa/">DVWA</a>

<
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

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

Description

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

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

Solution

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

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0524

XREF CWE:200

Plugin Information

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

Plugin Output

icmp/0

The remote clock is synchronized with the local clock.

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: 2022/02/01 Plugin Output tcp/445/cifs

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

METASPLOITABLE ( 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 ${\rm SMB}$: ${\rm SMBv1}$

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

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0802

Plugin Information

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

Plugin Output

tcp/3306/mysql

```
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 192.168.50.3 : /media 192.168.50.3/24

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/21/ftp

Port 21/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

Port 22/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/23/telnet

Port 23/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

Port 25/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/53/dns

Port 53/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

Port 80/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/111/rpc-portmapper

Port 111/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/139/smb

Port 139/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/445/cifs

Port 445/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/512

Port 512/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/513/rlogin

Port 513/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/514

Port 514/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/1099/rmi_registry

Port 1099/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2049/rpc-nfs

Port 2049/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2121/ftp

Port 2121/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3306/mysql

Port 3306/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3632

Port 3632/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/5432/postgresql

Port 5432/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/5900/vnc

Port 5900/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/6000/x11

Port 6000/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/6667

Port 6667/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8009/ajp13

Port 8009/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8180

Port 8180/tcp was found to be open

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

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: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.5.4
Nessus build : 20013
Plugin feed version : 202309020803
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Metasploitable Vulnerabilities
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.50.103
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 156.168 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/9/2 22:50 CEST
Scan duration: 562 sec
Scan for malware : no
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Remote operating system: Linux Kernel 2.6 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:O0204ffff0402080affffffff4445414401030307:M1460:
  P3:B00000:F0x00:W0:O0:M0
  P4:190504_7_p=2121
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
ed093088706603bfd5dc237399b498da2d4d31c6
i/CN:ubuntu804-base.localdomaini/0: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

Plugin Information

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

IAVB:0001-B-0515

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.
```

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: 2022/10/12

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.

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2023/08/08

Plugin Output

tcp/0

```
. You need to take the following 2 actions:

[ 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.
```

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: 2022/04/11

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 AO A8 14 4E
           98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 AO 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
          OC 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 OC 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: 2023/05/24
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: 2022/06/01

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 DB 89 ED A4 00 00 01 8A Q...w....

0x10: 57 AC FC 64 80 02 75 72 00 13 5B 4C 6A 61 76 61 W..d.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....
```

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

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

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
```

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
```

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/37441/rpc-mountd

```
The following RPC services are available on TCP port 37441:

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

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/42863/rpc-nlockmgr

```
The following RPC services are available on TCP port 42863:

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

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/47029/rpc-status

The following RPC services are available on UDP port 47029 :
- program: 100024 (status), version: 1

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/56389/rpc-status

The following RPC services are available on TCP port 56389:
- program: 100024 (status), version: 1

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/57136/rpc-mountd

```
The following RPC services are available on UDP port 57136:

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

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/60519/rpc-nlockmgr

```
The following RPC services are available on UDP port 60519:

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

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 AO A8 14 4E
           98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 AO 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
          OC 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 OC 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
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 :
 zlib@openssh.com
The server supports the following options for compression_algorithms_server_to_client :
 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: 2022/04/05

Plugin Output

tcp/22/ssh

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

hmac-sha1 hmac-sha1-96

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

SSH supported authentication : publickey, password

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

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/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: 2023/07/10

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 AO 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
          OC 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 OC 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 OC 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 [...]
```

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 AO 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
          OC 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 OC 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 OC 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 [...]
```

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)
                                                 KEX
                                                               Auth
                                                                       Encryption
                                                                                              MAC
   EXP-RC2-CBC-MD5
                                0x04, 0x00, 0x80 RSA(512)
                                                                       RC2-CBC(40)
     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)
```

EXP - DES - CBC - SHA	0×00 , 0×08	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-b:	it 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-b:	it key)				
Name	Code	KEX	Auth	Encryption	MAC
	[]				

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)
                                 Code
                                                 KEX
                                                               Auth
                                                                     Encryption
                                                                                               MAC
   EDH-RSA-DES-CBC3-SHA
                                0x00, 0x16
                                                                        3DES-CBC(168)
   DES-CBC3-SHA
                                 0x00, 0x0A
                                                 RSA
                                                               RSA
                                                                        3DES-CBC (168)
 High Strength Ciphers (>= 112-bit key)
                                                 KEX
                                 Code
                                                               Auth
                                                                        Encryption
                                                                                               MAC
   DHE-RSA-AES128-SHA
                                 0x00, 0x33
                                                               RSA
                                                                        AES-CBC(128)
```

DHE-RSA-AES256-SHA	0x00, 0x39	0x00, 0x39 DH	RSA	AES-CBC(256)	
SHA1					
AES128-SHA	0x00, 0x2F	0x00, 0x2F RSA	RSA	AES-CBC(128)	
SHA1					
AES256-SHA	0x00, 0x35	0x00, 0x35 RSA	RSA	AES-CBC(256)	
SHA1					
The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryptic MAC={message authentication} {export flag}					

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/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)
                                 Code
                                                  KEX
                                                                Auth
                                                                        Encryption
                                                                                                MAC
   EXP-EDH-RSA-DES-CBC-SHA
                                 0x00, 0x14
                                                  DH(512)
                                                                RSA
                                                                        DES-CBC(40)
         export
   EDH-RSA-DES-CBC-SHA
                                 0x00, 0x15
                                                                        DES-CBC(56)
                                                                RSA
   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
                                                                None
                                                                        DES-CBC(56)
   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-b	it 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 (>= 1	12-bit key)				
Name	Code	KEX	Auth	[]	

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/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)
                               Code
                                                            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)
 High Strength Ciphers (>= 112-bit key)
                                                            Auth Encryption
   Name
                               Code
                                               KEX
                                                                                           MAC
   DHE-RSA-AES128-SHA
                                0x00, 0x33
                                                DH
                                                             RSA
                                                                     AES-CBC(128)
   DHE-RSA-AES256-SHA
                               0x00, 0x39
                                                                   AES-CBC(256)
   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-b	it key, or 31	DES)		
		- 7			
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					
	440.11.1				
High Strength Ciphers (>=	112-bit key)				
Name	Code	KEX	Auth	Encryption	MAC
			[]	21101/P01011	1110

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

https://tools.ietf.org/html/rfc3749

https://tools.ietf.org/html/rfc3943

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/25/smtp

Nessus was able to confirm that the following compression method is supported by the target :

DEFLATE (0x01)

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml

https://tools.ietf.org/html/rfc3749

https://tools.ietf.org/html/rfc3943

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/5432/postgresql

Nessus was able to confirm that the following compression method is supported by the target :

DEFLATE (0x01)

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)
                                              KEX
                                                            Auth Encryption
                                                                                          MAC
   EXP-EDH-RSA-DES-CBC-SHA
                               0x00, 0x14
                                               DH(512)
                                                                    DES-CBC(40)
 SHA1 export
   EDH-RSA-DES-CBC-SHA 0x00, 0x15
                                                            RSA DES-CBC(56)
 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)
                               Code
                                               KEX
                                                            Auth
                                                                    Encryption
                                                                                          MAC
   EDH-RSA-DES-CBC3-SHA
                               0x00, 0x16
                                               DH
                                                            RSA
                                                                    3DES-CBC(168)
```

				_	-		
High	Strength	Cipners	(>=	112-D1t	кеу)		

	Name	Code	KEX	Auth	Encryption	MAC
	DHE-RSA-AES128-SHA	0x00, 0x33	DH	RSA	AES-CBC(128)	
SI	HA1					
	DHE-RSA-AES256-SHA	0x00, 0x39	DH	RSA	AES-CBC(256)	
SE	1A1					

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 ci					
Name	Code	KEX	Auth	Encryption	MAC
EDH-RSA-DES-CBC3-SHA SHA1	0x00, 0x16	DH	RSA	3DES-CBC(168)	
High Strength Ciphers (>= 11	2-bit key)				
Name	Code	KEX	Auth	Encryption	MAC
DHE-RSA-AES128-SHA SHA1	0x00, 0x33	DH	RSA	AES-CBC(128)	
DHE-RSA-AES256-SHA SHA1	0x00, 0x39	DH	RSA	AES-CBC(256)	

The fields above are :

{Tenable ciphername}
{Cipher ID code}

Kex={key exchange}

Auth={authentication}

Encrypt={symmetric encryption method}

MAC={message authentication code}
{export flag}

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.

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

- 0x13,0x01 TLS13 AES 128 GCM SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2023/07/10

ADH-DE [...]

tcp/25/smtp

oelow:							
Low Strength Ciphers (<= 64-)	oit key)						
Name	Code			KEX	Auth		MA
EXP-RC2-CBC-MD5 export		0x00,		RSA(512)	RSA	RC2-CBC(40)	MD
EXP-RC4-MD5 export	0x02,	0x00,	0x80	RSA(512)	RSA	RC4 (40)	MD
EXP-EDH-RSA-DES-CBC-SHA SHA1 export	0x00,	0x14		DH(512)	RSA	DES-CBC(40)	
EDH-RSA-DES-CBC-SHA SHA1	0x00,	0x15		DH	RSA	DES-CBC(56)	
EXP-ADH-DES-CBC-SHA SHA1 export	0x00,	0x19		DH(512)	None	DES-CBC(40)	
EXP-ADH-RC4-MD5 export	0x00,	0x17		DH(512)	None	RC4 (40)	ME
ADH-DES-CBC-SHA SHA1	0x00,	0x1A		DH	None	DES-CBC(56)	
EXP-DES-CBC-SHA SHA1 export	0x00,	0x08		RSA(512)	RSA	DES-CBC(40)	
EXP-RC2-CBC-MD5 export	0x00,	0x06		RSA(512)	RSA	RC2-CBC(40)	MI
EXP-RC4-MD5 export	0x00,	0x03		RSA(512)	RSA	RC4 (40)	MI
DES-CBC-SHA SHA1	0x00,	0x09		RSA	RSA	DES-CBC(56)	
Medium Strength Ciphers (> 64	1-bit and	< 112	-bit	key, or 3DES)		
Name	Code			KEX	Auth	Encryption	MZ
DES-CBC3-MD5 EDH-RSA-DES-CBC3-SHA	0x07,	0x00, 0x16	0xC0	RSA DH	RSA RSA	3DES-CBC(168) 3DES-CBC(168)	MI

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

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

TLSv1.3:

- 0x13,0x01 TLS13 AES 128 GCM SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TI Sv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2023/07/10

tcp/5432/postgresql

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
below:
 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)
                                          KEX
                                                       Auth Encryption
                                                                                   MAC
  Name
                            Code
  EDH-RSA-DES-CBC3-SHA
                            0x00, 0x16
                                                               3DES-CBC(168)
                                          DH
                                                       RSA
SHA1
   DES-CBC3-SHA
                           0x00, 0x0A RSA
                                                       RSA 3DES-CBC(168)
SHA1
 High Strength Ciphers (>= 112-bit key)
                                                       Auth
                                                             Encryption MAC
                                          KEX
                             Code
                                                                                   MAC
  Name
   0x00, 0x33
                                                                AES-CBC(128)
  DHE-RSA-AES128-SHA
                                            DH
                                                        RSA
   DHE-RSA-AES256-SHA
                            0x00, 0x39
                                            DH
                                                        RSA
                                                              AES-CBC(256)
SHA1
  AES128-SHA
                             0x00, 0x2F
                                            RSA
                                                        RSA AES-CBC(128)
  AES256-SHA
                             0x00, 0x35
                                            RSA
                                                       RSA
                                                              AES-CBC (256)
SHA1
                             0x00, 0x05
  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}
```

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: 2022/10/12
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.

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/21/ftp

An FTP server is running on this port.

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/22/ssh

An SSH server is running on this port.

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/23/telnet

A telnet server is running on this port.

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/25/smtp

An SMTP server is running on this port.

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/80/www

A web server is running on this port.

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/2121/ftp

An FTP server is running on this port.

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/5900/vnc

A vnc server is running on this port.

11153 - Service Detection (HELP Request)

Synopsis
The remote service could be identified.
Description
It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'
request.
Solution
n/a
Risk Factor
None
Plugin Information
Published: 2002/11/18, Modified: 2018/11/26
Plugin Output
tcp/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

Plugin Output

udp/69/tftp

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: 2022/12/28

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 Informa	ation
Published: 201	8/06/27, Modified: 2023/02/13
Plugin Output	
tcp/0	

192.168.50.3

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

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/06/26

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.50.103 to 192.168.50.3 : 192.168.50.103  
192.168.50.3  
Hop Count: 1
```

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: 2022/07/26

Plugin Output

tcp/512

```
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 : 512
Type : spontaneous
Banner:

0x00: 01 57 68 65 72 65 20 61 72 65 20 79 6F 75 3F 0A .Where are you?.

0x10:
```

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: 2022/07/26

Plugin Output

tcp/514

```
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 : 514

Type : spontaneous

Banner:

0x00: 01 67 65 74 6E 61 6D 65 69 6E 66 6F 3A 20 54 65 .getnameinfo: Te

0x10: 6D 70 6F 72 61 72 79 20 66 61 69 6C 75 72 65 20 mporary failure

0x20: 69 6E 20 6E 61 6D 65 20 72 65 73 6F 6C 75 74 69 in name resoluti
0x30: 6F 6E 0A on.
```

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: 2022/07/26

Plugin Output

tcp/6667

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: 2022/07/26

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 `1
           0x0050: 6F 61 64 27 22 37 2F 75 73 72 2F 6C 69 62 2F 72 0x0060: 75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2E
                                                                          oad'"7/usr/lib/r
                    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:
0x00C0:
                    65 63 76 5F 72 65 71 75 65 73 74 27 22 3C 2F 75
                                                                           ecv request'"</u
                    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 0x0110: 2E 72 62 3A 31 35 34 32 3A 69 6E 20 60 73 65 74
                                                                           ruby/1.8/drb/drb
                                                                           .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 [...]
```

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

 $\verb|\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: 2023/07/17

Plugin Output

tcp/445/cifs

Can't connect to the 'root\CIMV2' WMI namespace.

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 7 NetBIOS names have been gathered:

METASPLOITABLE = Computer name
METASPLOITABLE = Messenger Service
METASPLOITABLE = File Server Service
__MSBROWSE_ = Master Browser
WORKGROUP = Workgroup / Domain name
WORKGROUP = Master Browser
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