Vulnerability Assessment

Sun, 27 Aug 2023 09:15:44 EDT

Vulnerabilities by Host 192.168.50.100

12	13	41	10	153
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sun Aug 27 08:09:01 2023
End time:	Sun Aug 27 09:15:43 2023

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.100
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities by Risk level

Critical

Plugin ID	Port	Protocol	Name
70728	80	tcp	Apache PHP-CGI Remote Code Execution
51988	1524	tcp	Bind Shell Backdoor Detection
32314	22	tcp	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
32321	25	tcp	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
32321	5432	tcp	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
11356	2049	udp	NFS Exported Share Information Disclosure
20007	25	tcp	SSL Version 2 and 3 Protocol Detection
20007	5432	tcp	SSL Version 2 and 3 Protocol Detection
33850	0	tcp	Unix Operating System Unsupported Version Detection
46882	6697	tcp	UnrealIRCd Backdoor Detection
61708	5900	tcp	VNC Server 'password' Password
125855	80	tcp	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

High

Plugin ID	Port	Protocol	Name
39465	80	tcp	CGI Generic Command Execution
39469	80	tcp	CGI Generic Remote File Inclusion
42424	80	tcp	CGI Generic SQL Injection (blind)
136769	53	udp	ISC BIND Service Downgrade / Reflected DoS
42256	2049	tcp	NFS Shares World Readable
59088	80	tcp	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
42873	25	tcp	SSL Medium Strength Cipher Suites Supported (SWEET32)
42873	5432	tcp	SSL Medium Strength Cipher Suites Supported (SWEET32)
90509	445	tcp	Samba Badlock Vulnerability

Plugin ID	Port	Protocol	Name
19704	80	tcp	TWiki 'rev' Parameter Arbitrary Command Execution
36171	80	tcp	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
10205	513	tcp	rlogin Service Detection
10245	514	tcp	rsh Service Detection

Medium

Plugin ID	Port	Protocol	Name
11411	80	tcp	Backup Files Disclosure
40984	80	tcp	Browsable Web Directories
44136	80	tcp	CGI Generic Cookie Injection Scripting
49067	80	tcp	CGI Generic HTML Injections (quick test)
42872	80	tcp	CGI Generic Local File Inclusion (2nd pass)
39467	80	tcp	CGI Generic Path Traversal
46195	80	tcp	CGI Generic Path Traversal (extended test)
47831	80	tcp	CGI Generic XSS (comprehensive test)
55903	80	tcp	CGI Generic XSS (extended patterns)
39466	80	tcp	CGI Generic XSS (quick test)
11213	80	tcp	HTTP TRACE / TRACK Methods Allowed
139915	53	udp	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
136808	53	udp	ISC BIND Denial of Service
46803	80	tcp	PHP expose_php Information Disclosure
57608	445	tcp	SMB Signing not required
52611	25	tcp	SMTP Service STARTTLS Plaintext Command Injection
90317	22	tcp	SSH Weak Algorithms Supported
31705	25	tcp	SSL Anonymous Cipher Suites Supported
51192	25	tcp	SSL Certificate Cannot Be Trusted
51192	5432	tcp	SSL Certificate Cannot Be Trusted
15901	25	tcp	SSL Certificate Expiry

Plugin ID	Port	Protocol	Name
15901	5432	tcp	SSL Certificate Expiry
45411	25	tcp	SSL Certificate with Wrong Hostname
45411	5432	tcp	SSL Certificate with Wrong Hostname
89058	25	tcp	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
65821	25	tcp	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
65821	5432	tcp	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
57582	25	tcp	SSL Self-Signed Certificate
57582	5432	tcp	SSL Self-Signed Certificate
26928	25	tcp	SSL Weak Cipher Suites Supported
81606	25	tcp	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
58751	25	tcp	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
104743	25	tcp	TLS Version 1.0 Protocol Detection
104743	5432	tcp	TLS Version 1.0 Protocol Detection
42263	23	tcp	Unencrypted Telnet Server
57640	80	tcp	Web Application Information Disclosure
85582	80	tcp	Web Application Potentially Vulnerable to Clickjacking
11229	80	tcp	Web Server info.php / phpinfo.php Detection
51425	80	tcp	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
36083	80	tcp	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)
49142	80	tcp	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)

Low

Plugin ID	Port	Protocol	Name
10407	6000	tcp	X Server Detection
26194	80	tcp	Web Server Transmits Cleartext Credentials
42057	80	tcp	Web Server Allows Password Auto-Completion
70658	22	tcp	SSH Server CBC Mode Ciphers Enabled

Plugin ID	Port	Protocol	Name
71049	22	tcp	SSH Weak MAC Algorithms Enabled
78479	25	tcp	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
78479	5432	tcp	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
83738	25	tcp	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
83875	25	tcp	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
153953	22	tcp	SSH Weak Key Exchange Algorithms Enabled

Info

Please see InfoDetails.pdf.

Critical Vulnerabilities Detail

70728 Apache PHPCGI Remote Code Execution

Synopsis

The remote web server contains a version of PHP that allows arbitrary code execution.

Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass commandline arguments as part of a query string to the PHPCGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

Solution

Upgrade to PHP 5.3.13 / 5.4.3 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)

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

BID	53388
CVE	CVE20121823
CVE	CVE20122311
CVE	CVE20122335
CVE	CVE20122336
XREF	CERT:520827
XREF	EDBID:29290
XREF	EDBID:29316
XREF	CISAKNOWNEXPLOITED:2022/04/15

Exploitable With

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

Plugin Information

Published: 2013/11/01, Modified: 2023/04/25

Plugin Output

tcp/80/www

```
Nessus was able to verify the issue exists using the following request : snip POST
/cgibin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D
%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%6
1%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67
%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E HTTP/1.1Host: 192.168.50.100AcceptCharset: iso88591,utf8;q=0.9,*;q=0.1AcceptLanguage:
enContentType: application/xwwwformurlencodedConnection: KeepAliveContentLength: 115UserAgent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)Pragma:
nocacheAccept: image/gif, image/xxbitmap, image/jpeg, image/pjpeg, image/png, */*<?php echo "ContentType:text/html\r\n\r\n"; echo
'php_cgi_remote_code_execution1693141200'; system('id'); die; ?> snip
```

51988 Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

Description

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

Solution

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

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

tcp/1524/wild_shell

```
Nessus was able to execute the command "id" using thefollowing request :This produced the following truncated output (limited to 10 lines) : snip
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)root@metasploitable:/# snip
```

32314 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

See Also

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

Solution

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

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE20080166
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 regenerated.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE20080166
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 regenerated.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE20080166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

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

Plugin Output

tcp/5432/postgresql

11356 NFS Exported Share Information Disclosure

Synopsis

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

Description

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

Solution

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

Risk Factor

Critical

CVSS v2.0 Base Score

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

References

CVE	CVE19990170
CVE	CVE19990211
CVE	CVE19990554

Exploitable With

Metasploit (true)

Plugin Information

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

Plugin Output

udp/2049/rpcnfs

```
The following NFS shares could be mounted :+ /+ Contents of / :  . .. bin boot cdrom dev etc home initrd initrd.img lib lost+found media mnt nohup.out opt proc root
sbin srv sys tmp usr var vmlinuz
```

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 maninthemiddle 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/paperssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/sslpoodle.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

```
 SSLv2 is enabled and the server supports at least one cipher.Low Strength Ciphers (<= 64bit key)Name Code KEX Auth Encryption MAC     EXPRC2CBCMD5 RSA(512) RSA
RC2CBC(40) MD5 exportEXPRC4MD5 RSA(512) RSA RC4(40) MD5 exportMedium Strength Ciphers (> 64bit and < 112bit key, or 3DES)Name Code KEX Auth Encryption MAC
DESCBC3MD5 RSA RSA 3DESCBC(168) MD5High Strength Ciphers (>= 112bit key)Name Code KEX Auth Encryption MAC     RC4MD5 RSA RSA RC4(128) MD5The fields above are :{Tenable
ciphername}{Cipher ID code}Kex={key exchange}Auth={authentication}Encrypt={symmetric encryption method}MAC={message authentication code}{export flag} SSLv3 is enabled
and the server supports at least one cipher.Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3Low Strength Ciphers (<= 64bit key)Name Code KEX Auth
Encryption MAC     EXPEDHRSADESCBCSHA DH(512) RSA DESCBC(40) SHA1 exportEDHRSADESCBCSHA DH RSA DESCBC(56) SHA1EXPADHDESCBCSHA DH(512) None DESCBC(40) SHA1
exportEXPADHRC4MD5 DH(512) None RC4(40) MD5 exportADHDESCBCSHA DH None DESCBC(56) SHA1EXPDESCBCSHA RSA(512) RSA DESCBC(40) SHA1 exportEXPRC2CBCMD5 RSA(512) RSA
RC2CBC(40) MD5 exportEXPRC4MD5 RSA(512) RSA RC4(40) MD5 exportDESCBCSHA RSA RSA DESCBC(56) SHA1Medium Strength Ciphers (> 64bit and < 112bit key, or 3DES)Name Code KEX
Auth Encryption MAC     EDHRSADESCBC3SHA DH RSA 3DESCBC(168) SHA1ADHDESCBC3SHA DH None 3DESCBC(168) SHA1DESCBC3SHA RSA RSA 3DESCBC(168) SHA1High Strength Ciphers (>=
112bit key)Name Code KEX Auth Encryption MAC     DHERSAAES128SHA DH RSA AESCBC(128) SHA1DHERSAAES256SHA DH RSA AESCBC(256) SHA1ADHAES128SHA DH None AESCBC(128)
SHA1ADHAES256SHA DH None AESCBC(256) SHA1ADHRC4MD5 DH None RC4(128) MD5AES128SHA RSA RSA AESCBC(128) SHA1AES256SHA RSA RSA AESCBC(256) SHA1RC4MD5 RSA RSA RC4(128)
MD5RC4SHA RSA RSA RC4(128) SHA1The fields above are :{Tenable ciphername}{Cipher ID code}Kex={key exchange}Auth={authentication}Encrypt={symmetric encryption
method}MAC={message authentication code}{export flag}
```

20007 SSL Version 2 and 3 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: An insecure padding scheme with CBC ciphers. Insecure session renegotiation and resumption schemes.An attacker can exploit these flaws to conduct maninthemiddle 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/paperssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/sslpoodle.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 SSLv3Medium Strength Ciphers (> 64bit and
< 112bit key, or 3DES)Name Code KEX Auth Encryption MAC     EDHRSADESCBC3SHA DH RSA 3DESCBC(168) SHA1DESCBC3SHA RSA RSA 3DESCBC(168) SHA1High Strength Ciphers (>=
112bit key)Name Code KEX Auth Encryption MAC     DHERSAAES128SHA DH RSA AESCBC(128) SHA1DHERSAAES256SHA DH RSA AESCBC(256) SHA1AES128SHA RSA RSA AESCBC(128)
SHA1AES256SHA RSA RSA AESCBC(256) SHA1RC4SHA RSA RSA RC4(128) SHA1The 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 selfreported 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:0001A0502
XREF	IAVA:0001A0648

Plugin Information

Published: 2008/08/08, Modified: 2023/07/07

Plugin Output

tcp/0

```
Ubuntu 8.04 support ended on 20110512 (Desktop) / 20130509 (Server).Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.For more information, see :
https://wiki.ubuntu.com/Releases
```

46882 UnrealIRCd Backdoor Detection

Synopsis

The remote IRC server contains a backdoor.

Description

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

See Also

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

Solution

Redownload the software, verify it using the published MD5 / SHA1 checksums, and reinstall it.

Risk Factor

Critical

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	40820
CVE	CVE20102075

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2010/06/14, Modified: 2022/04/11

Plugin Output

tcp/6697/irc

```
The remote IRC server is running as :uid=0(root) gid=0(root)
```

61708 VNC Server 'password' Password

Synopsis

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

Description

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

Solution

Secure the VNC service with a strong password.

Risk Factor

Critical

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/5900/vnc

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

125855 phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA20193)

Synopsis

The remote web server hosts a PHP application that is affected by SQLi vulnerability.

Description

According to its selfreported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the backend database, resulting in the disclosure or manipulation of arbitrary data.Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's selfreported version number.

See Also

http://www.nessus.org/u?c9d7fc8c

Solution

Upgrade to phpMyAdmin version 4.8.6 or later.Alternatively, apply the patches referenced in the vendor advisories.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	108617
CVE	CVE201911768

Plugin Information

Published: 2019/06/13, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
URL : http://192.168.50.100/phpMyAdminInstalled version : 3.1.1Fixed version : 4.8.6
```

High Vulnerabilities Detail

39465 CGI Generic Command Execution

Synopsis

Arbitrary code may be run on the remote server.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to execute arbitrary commands on the remote host.

See Also

https://en.wikipedia.org/wiki/Code_injection
http://projects.webappsec.org/w/page/13246950/OS%20Commanding

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address command execution flaws.

Risk Factor

High

CVSS v2.0 Base Score

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

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:77
XREF	CWE:78
XREF	CWE:713
XREF	CWE:722
XREF	CWE:727
XREF	CWE:741
XREF	CWE:751
XREF	CWE:801
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/06/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :+ The following resources may be vulnerable to arbitrary command execution :+ The 'topic' parameter of the
/twiki/bin/view/Main/WebHome CGI :/twiki/bin/view/Main/WebHome?topic=echo%20NeS%20%20SuS output <body bgcolor="#ffffff"><a name="PageTop"></a><form name="main"
action="/twiki/bin/view/Main/echo%20NeS%20SuS"><table width="100%" border="0" cellpadding="3" cellspacing="0"><tr>Clicking directly on these URLs should exhibit the
issue :(you will probably need to read the HTML source)http://192.168.50.100/twiki/bin/view/Main/WebHome?topic=echo%20NeS%20%20SuS
```

39469 CGI Generic Remote File Inclusion

Synopsis

Arbitrary code may be run on the remote server.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.

See Also

https://en.wikipedia.org/wiki/Remote_File_Inclusion
http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

Risk Factor

High

CVSS v2.0 Base Score

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

References

XREF	CWE:73	XREF	CWE:78
XREF	CWE:98		
XREF	CWE:434		
XREF	CWE:473		
XREF	CWE:632		
XREF	CWE:714		
XREF	CWE:727		
XREF	CWE:801		
XREF	CWE:928		
XREF	CWE:929		

Plugin Information

Published: 2009/06/19, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :+ The following resources may be vulnerable to web code injection :+ The 'page' parameter of the /mutillidae/ CGI
:/mutillidae/?page=http://yL0Yh2Ol.example.com/ output <b>Warning</b>: include() [<a href='function.include'>function.in [...]<br /><b>Warning</b>:
include(http://yL0Yh2Ol.example.com/) [<a href='function.include'>function.include</a>]: failed to open stream: no suitable wrapper could be found in
<b>/var/www/mutillidae/index.php</b> on line <b>469</b><br /><br /><b>Warning</b>: include() [<a href='function.include'>function.in [...]+ The 'page' parameter of the
/mutillidae/index.php CGI :/mutillidae/index.php?page=http://yL0Yh2Ol.example.com/ output <b>Warning</b>: include() [<a href='function.include'>function.in [...]<br
/><b>Warning</b>: include(http://yL0Yh2Ol.example.com/) [<a href='function.include'>function.include</a>]: failed to open stream: no suitable wrapper could be found in
<b>/var/www/mutillidae/index.php</b> on line <b>469</b><br /><br /><b>Warning</b>: include() [<a href='function.include'>function.in [...]Clicking directly on these
URLs should exhibit the issue :(you will probably need to read the HTML
source)http://192.168.50.100/mutillidae/?page=http://yL0Yh2Ol.example.com/http://192.168.50.100/mutillidae/index.php?page=http://yL0Yh2Ol.example.com/Using the POST
HTTP method, Nessus found that :+ The following resources may be vulnerable to web code injection :/mutillidae/index.php
[do=togglehints&page=http://yL0Yh2Ol.example.com/&username=anonymous] output <b>Warning</b>: include() [<a href='function.include'>function.in [...]<br
/><b>Warning</b>: include(http://yL0Yh2Ol.example.com/) [<a href='function.include'>function.include</a>]: failed to open stream: no suitable wrapper could be found in
<b>/var/www/mutillidae/index.php</b> on line <b>469</b><br /><br /><b>Warning</b>: include() [<a href='function.include'>function.in [...]
```

42424 CGI Generic SQL Injection (blind)

Synopsis

A CGI application hosted on the remote web server is potentially prone to SQL injection attack.

Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database. An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system. Note that this script is experimental and may be prone to false positives.

See Also

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://www.nessus.org/u?ed792cf5
http://www.nessus.org/u?11ab1866

Solution

Modify the affected CGI scripts so that they properly escape arguments.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:20
XREF	CWE:77
XREF	CWE:89
XREF	CWE:91
XREF	CWE:203
XREF	CWE:643
XREF	CWE:713
XREF	CWE:722
XREF	CWE:727
XREF	CWE:751
XREF	CWE:801
XREF	CWE:810
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/11/06, Modified: 2022/10/28

Plugin Output

tcp/80/www

```
Using the POST HTTP method, Nessus found that :+ The following resources may be vulnerable to blind SQL injection :+ The 'page' parameter of the /mutillidae/index.php
CGI :/mutillidae/index.php [username=anonymous&do=togglehints&page=home.phpzzanonymous&do=togglehints&page=home.phpyy] output <a
href="./index.php?page=login.php">Login/Register</a></td><td><a href="./index.php?do=togglehints&page=home.php">Toggle Hints</a></td><td><a
href="./index.php?do=togglesecurity&page=home.php">Toggle Security</a></td><td><a href="setupdatabase.php">Reset DB</a></td><td><a
href="./index.php?page=showlog.php">View Log</a></td> vs <a href="./index.php?page=login.php">Login/Register</a></td><td><a
href="./index.php?do=togglehints&page=home.phpyy">Toggle Hints</a></td><td><a href="./index.php?do=togglesecurity&page=home.phpyy">Toggle Security</a></td><td><a
href="setupdatabase.php">Reset DB</a></td><td><a href="./index.php?page=showlog.php">View Log</a></td>/mutillidae/index.php
[username=anonymous&do=togglehints&page=home.phpzzanonymous&do=togglehints&page=home.phpyy] {2} output <a
href="./index.php?page=login.php">Login/Register</a></td><td><a href="./index.php?do=togglehints&page=home.php">Toggle Hints</a></td><td><a
href="./index.php?do=togglesecurity&page=home.php">Toggle Security</a></td><td><a href="setupdatabase.php">Reset DB</a></td><td><a
href="./index.php?page=showlog.php">View Log</a></td> vs <a href="./index.php?page=login.php">Login/Register</a></td><td><a
href="./index.php?do=togglehints&page=home.phpyy">Toggle Hints</a></td><td><a href="./index.php?do=togglesecurity&page=home.phpyy">Toggle Security</a></td><td><a
href="setupdatabase.php">Reset DB</a></td><td><a href="./index.php?page=showlog.php">View Log</a></td>
```

136769 ISC BIND Service Downgrade / Reflected DoS

Synopsis

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

Description

According to its selfreported 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/cve20208616

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE20208616
XREF	IAVA:2020A0217S

Plugin Information

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

Plugin Output

udp/53/dns

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

42256 NFS Shares World Readable

Synopsis

The remote NFS server exports worldreadable shares.

Description

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

See Also

http://www.tldp.org/HOWTO/NFSHOWTO/security.html

Solution

Place the appropriate restrictions on all NFS shares.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/2049/rpcnfs

```
The following shares have no access restrictions :/ *
```

59088 PHP PHPCGI Query String Parameter Injection Arbitrary Code Execution

Synopsis

The remote web server contains a version of PHP that allows arbitrary code execution.

Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass commandline arguments as part of a query string to the PHPCGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

See Also

http://eindbazen.net/2012/05/phpcgiadvisorycve20121823/
http://www.php.net/archive/2012.php#id201205081
http://www.php.net/ChangeLog5.php#5.3.13
http://www.php.net/ChangeLog5.php#5.4.3
http://www.nessus.org/u?80589ce8
https://www304.ibm.com/support/docview.wss?uid=swg21620314

Solution

If using Lotus Foundations, upgrade the Lotus Foundations operating system to version 1.2.2b or later. Otherwise, upgrade to PHP 5.3.13 / 5.4.3 or later.

Risk Factor

High

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

BID	53388
CVE	CVE20121823
CVE	CVE20122311
XREF	CERT:520827
XREF	EDBID:18834
XREF	CISAKNOWNEXPLOITED:2022/04/15

Exploitable With

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

Plugin Information

Published: 2012/05/14, Modified: 2022/03/28

Plugin Output

tcp/80/www

```
Nessus was able to verify the issue exists using the following request : snip POST
/dvwa/dvwa/includes/DBMS/DBMS.php?d+allow_url_include%3don+d+safe_mode%3doff+d+suhosin.simulation%3don+d+open_basedir%3doff+d+auto_prepend_file%3dphp%3a//input+n
HTTP/1.1Host: 192.168.50.100AcceptCharset: iso88591,utf8;q=0.9,*;q=0.1AcceptLanguage: enContentType: application/xwwwformurlencodedConnection: KeepAliveContentLength:
82UserAgent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)Pragma: nocacheAccept: image/gif, image/xxbitmap, image/jpeg, image/pjpeg, image/png,
*/*<?php echo 'php_cgi_query_string_code_execution1693141200'; system('id'); die; ?> snip
```

42873 SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

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

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE20162183

Plugin Information

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

Plugin Output

tcp/25/smtp

```
Medium Strength Ciphers (> 64bit and < 112bit key, or 3DES)Name Code KEX Auth Encryption MAC     DESCBC3MD5 0x07, 0x00, 0xC0 RSA RSA 3DESCBC(168) MD5EDHRSADESCBC3SHA
0x00, 0x16 DH RSA 3DESCBC(168) SHA1ADHDESCBC3SHA 0x00, 0x1B DH None 3DESCBC(168) SHA1DESCBC3SHA 0x00, 0x0A RSA RSA 3DESCBC(168) SHA1The fields above are :{Tenable
ciphername}{Cipher ID code}Kex={key exchange}Auth={authentication}Encrypt={symmetric encryption method}MAC={message authentication code}{export flag}
```

42873 SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

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

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE20162183

Plugin Information

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

Plugin Output

tcp/5432/postgresql

```
Medium Strength Ciphers (> 64bit and < 112bit key, or 3DES)Name Code KEX Auth Encryption MAC     EDHRSADESCBC3SHA 0x00, 0x16 DH RSA 3DESCBC(168) SHA1DESCBC3SHA 0x00,
0x0A RSA RSA 3DESCBC(168) SHA1The 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 maninthemiddle 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/CVE20162118.html

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	86002
CVE	CVE20162118
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.
```

19704 TWiki 'rev' Parameter Arbitrary Command Execution

Synopsis

The remote web server hosts a CGI application that is affected by an arbitrary command execution vulnerability.

Description

The version of TWiki running on the remote host allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id.

See Also

http://www.nessus.org/u?c70904f3

Solution

Apply the appropriate hotfix referenced in the vendor advisory.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	14834
CVE	CVE20052877

Exploitable With

Metasploit (true)

Plugin Information

Published: 2005/09/15, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Nessus was able to execute the command "id" using thefollowing request :http://192.168.50.100/twiki/bin/view/Main/TWikiUsers?rev=2%20%7cid%7c%7cecho%20This produced
the following truncated output (limited to 2 lines) : snip uid=33(wwwdata) gid=33(wwwdata) groups=33(wwwdata) snip
```

36171 phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA20094)

Synopsis

The remote web server contains a PHP application that is affected by a code execution vulnerability.

Description

The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize usersupplied input before using it to generate a config file for the application. This version is affected by the following vulnerabilities : The setup script inserts the unsanitized verbose server name into a Cstyle comment during config file generation. An attacker can save arbitrary data to the generated config file by altering the value of the 'textconfig' parameter during a POST request to config.php.An unauthenticated, remote attacker can exploit these issues to execute arbitrary PHP code.

See Also

https://www.tenable.com/security/research/tra200902
http://www.phpmyadmin.net/home_page/security/PMASA20094.php

Solution

Upgrade to phpMyAdmin 3.1.3.2. Alternatively, apply the patches referenced in the project's advisory.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	34526
CVE	CVE20091285
XREF	TRA:TRA200902
XREF	SECUNIA:34727
XREF	CWE:94

Plugin Information

Published: 2009/04/16, Modified: 2022/04/11

Plugin Output

tcp/80/www

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 maninthemiddle 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 filewrite access into full logins through the .rhosts or rhosts.equiv files.

Solution

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

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE19990651

Exploitable With

Metasploit (true)

Plugin Information

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

Plugin Output

tcp/513/rlogin

10245 rsh Service Detection

Synopsis

The rsh service is running on the remote host.

Description

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

Solution

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

Risk Factor

High

CVSS v2.0 Base Score

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

References

CVE	CVE19990651

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/08/22, Modified: 2022/04/11

Plugin Output

tcp/514/rsh

Medium Vulnerabilities Detail

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**11411**
Port	80
Protocol	tcp
Synopsis	It is possible to retrieve file backups from the remote web server.
Description	By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.
Solution	Ensure the files do not contain any sensitive information, such ascredentials to connect to a database, and delete or protect thosefiles that should not be accessible.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**40984**
Port	80
Protocol	tcp
Synopsis	Some directories on the remote web server are browsable.
Description	Multiple Nessus plugins identified directories on the web serverthat are browsable.
Solution	Make sure that browsable directories do not leak confidentialinformation or give access to sensitive resources. Additionally, useaccess restrictions or disable directory indexing for any that do.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**44136**
Port	80
Protocol	tcp
Synopsis	The remote web server is prone to cookie injection attacks.

Description	The remote web server hosts at least one CGI script that fails toadequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to inject arbitrarycookies. Depending on the structure of the web application, it may bepossible to launch a 'session fixation' attack using this mechanism. Please note that : - Nessus did not check if the session fixation attack is feasible. - This is not the only vector of session fixation.
Solution	Restrict access to the vulnerable application. Contact the vendorfor a patch or upgrade.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	**HTTP TRACE / TRACK Methods Allowed**
Plugin ID	**49067**
Port	80
Protocol	tcp
Synopsis	The remote web server may be prone to HTML injections.
Description	The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML to be executed in a user's browser within the security context of the affected site.The remote web server may be vulnerable to IFRAME injections or cross-site scripting attacks : - IFRAME injections allow 'virtual defacement' that might scare or anger gullible users. Such injections are sometimes implemented for 'phishing' attacks. - XSS are extensively tested by four other scripts. - Some applications (e.g. web forums) authorize a subset of HTML without any ill effect. In this case, ignore this warning.
Solution	Either restrict access to the vulnerable application or contact thevendor for an update.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	**HTTP TRACE / TRACK Methods Allowed**
Plugin ID	**42872**
Port	80
Protocol	tcp
Synopsis	Arbitrary code may be run on this server.
Description	The remote web server hosts CGI scripts that fail to adequatelysanitize request strings. By leveraging this issue, an attacker maybe able to include a local file and disclose its contents, or evenexecute arbitrary code on the remote host.
Solution	Restrict access to the vulnerable application. Contact the vendorfor a patch or upgrade.
Risk Factor	Medium
CVSS v2.0 Base Score	68

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**39467**
Port	80
Protocol	tcp
Synopsis	Arbitrary files may be accessed or executed on the remote host.
Description	The remote web server hosts CGI scripts that fail to adequately sanitizerequest strings and are affected by directory traversal or local filesinclusion vulnerabilities.By leveraging this issue, an attacker may be able to read arbitraryfiles on the web server or execute commands.
Solution	Restrict access to the vulnerable application. Contact thevendor for a patch or upgrade to address path traversal flaws.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**46195**
Port	80
Protocol	tcp
Synopsis	Arbitrary files may be accessed or executed on the remote host.
Description	The remote web server hosts CGI scripts that fail to adequatelysanitize request strings and are affected by directory traversal orlocal file inclusion vulnerabilities.By leveraging this issue, an attacker may be able to read arbitraryfiles on the web server or execute commands.
Solution	Either restrict access to the vulnerable application or contact thevendor for an update.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**47831**
Port	80
Protocol	tcp
Synopsis	The remote web server is prone to cross-site scripting attacks.
Description	The remote web server hosts CGI scripts that fail to adequatelysanitize request strings of malicious JavaScript. By leveraging thisissue, an attacker may be able to cause arbitrary HTML and script codeto be executed in a user's browser within the security context of theaffected site. These XSS are likely to be 'non-persistent' or'reflected'.
Solution	Restrict access to the vulnerable application. Contact the vendorfor a patch or upgrade.
Risk Factor	Medium

CVSS v2.0 Base Score	43

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**55903**
Port	80
Protocol	tcp
Synopsis	The remote web server is prone to cross-site scripting attacks.
Description	The remote web server hosts one or more CGI scripts that fail toadequately sanitize request strings with malicious JavaScript. Byleveraging this issue, an attacker may be able to cause arbitrary HTMLand script code to be executed in a user's browser within the securitycontext of the affected site. These XSS vulnerabilities are likely tobe 'non-persistent' or 'reflected'.
Solution	Restrict access to the vulnerable application. Contact the vendorfor a patch or upgrade.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**39466**
Port	80
Protocol	tcp
Synopsis	The remote web server is prone to cross-site scripting attacks.
Description	The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script codeto be executed in a user's browser within the security context of theaffected site.These XSS are likely to be 'non persistent' or 'reflected'.
Solution	Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**11213**
Port	80
Protocol	tcp
Synopsis	Debugging functions are enabled on the remote web server.
Description	The remote web server supports the TRACE and/or TRACK methods. TRACEand TRACK are HTTP methods that are used to debug web serverconnections.

Solution	Disable these HTTP methods. Refer to the plugin output for more information.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**139915**
Port	53
Protocol	udp
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 denialof 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 aTSIG-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.
Solution	Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.
Risk Factor	Medium
CVSS v2.0 Base Score	40

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**136808**
Port	53
Protocol	udp
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 aspecially-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 versionnumber.
Solution	Upgrade to the patched release most closely related to your current version of BIND.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**46803**
Port	80
Protocol	tcp
Synopsis	The configuration of PHP on the remote host allows disclosure ofsensitive information.
Description	The PHP install on the remote server is configured in a way thatallows disclosure of potentially sensitive information to an attackerthrough a special URL. Such a URL triggers an Easter egg built intoPHP itself. Other such Easter eggs likely exist, but Nessus has not checked forthem.
Solution	In the PHP configuration file, php.ini, set the value for'expose_php' to 'Off' to disable this behavior. Restart the webserver daemon to put this change into effect.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**57608**
Port	445
Protocol	tcp
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 attacksagainst the SMB server.
Solution	Enforce message signing in the host's configuration. On Windows, thisis found in the policy setting 'Microsoft network server: Digitallysign communications (always)'. On Samba, the setting is called 'serversigning'. See the 'see also' links for further details.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**52611**
Port	25
Protocol	tcp
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 STARTTLSimplementation that could allow a remote, unauthenticated attacker toinject commands during the plaintext protocol phase that will beexecuted during the ciphertext protocol phase. Successful exploitation could allow an attacker to steal a victim'semail or associated SASL (Simple Authentication and Security Layer)credentials.

Solution	Contact the vendor to see if an update is available.
Risk Factor	Medium
CVSS v2.0 Base Score	40

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**90317**
Port	22
Protocol	tcp
Synopsis	The remote SSH server is configured to allow weak encryptionalgorithms or no algorithm at all.
Description	Nessus has detected that the remote SSH server is configured to usethe Arcfour stream cipher or no cipher at all. RFC 4253 advisesagainst using Arcfour due to an issue with weak keys.
Solution	Contact the vendor or consult product documentation to remove the weakciphers.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**31705**
Port	25
Protocol	tcp
Synopsis	The remote service supports the use of anonymous SSL ciphers.
Description	The remote host supports the use of anonymous SSL ciphers. While thisenables an administrator to set up a service that encrypts trafficwithout having to generate and configure SSL certificates, it offersno way to verify the remote host's identity and renders the servicevulnerable to a man-in-the-middle attack.Note: This is considerably easier to exploit if the attacker is on thesame physical network.
Solution	Reconfigure the affected application if possible to avoid use of weakciphers.
Risk Factor	Low
CVSS v2.0 Base Score	26

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**51192**
Port	25
Protocol	tcp
Synopsis	The SSL certificate for this service cannot be trusted.

Description	The server's X.509 certificate cannot be trusted. This situation canoccur in three different ways, in which the chain of trust can bebroken, 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 thechain 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.
Solution	Purchase or generate a proper SSL certificate for this service.
Risk Factor	Medium
CVSS v2.0 Base Score	64

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**51192**
Port	5432
Protocol	tcp
Synopsis	The SSL certificate for this service cannot be trusted.
Description	The server's X.509 certificate cannot be trusted. This situation canoccur in three different ways, in which the chain of trust can bebroken, 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 thechain 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.
Solution	Purchase or generate a proper SSL certificate for this service.

Risk Factor	Medium
CVSS v2.0 Base Score	64

Name	**HTTP TRACE / TRACK Methods Allowed**
Plugin ID	**15901**
Port	25
Protocol	tcp
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 alreadyexpired.
Solution	Purchase or generate a new SSL certificate to replace the existingone.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	**HTTP TRACE / TRACK Methods Allowed**
Plugin ID	**15901**
Port	5432
Protocol	tcp
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 alreadyexpired.
Solution	Purchase or generate a new SSL certificate to replace the existingone.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	**HTTP TRACE / TRACK Methods Allowed**
Plugin ID	**45411**
Port	25
Protocol	tcp
Synopsis	The SSL certificate for this service is for a different host.
Description	The 'commonName' (CN) attribute of the SSL certificate presented forthis service is for a different machine.
Solution	Purchase or generate a proper SSL certificate for this service.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**45411**
Port	5432
Protocol	tcp
Synopsis	The SSL certificate for this service is for a different host.
Description	The 'commonName' (CN) attribute of the SSL certificate presented forthis service is for a different machine.
Solution	Purchase or generate a proper SSL certificate for this service.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**89058**
Port	25
Protocol	tcp
Synopsis	The remote host may be affected by a vulnerability that allows aremote attacker to potentially decrypt captured TLS traffic.
Description	The remote host supports SSLv2 and therefore may be affected by avulnerability that allows a cross-protocol Bleichenbacher paddingoracle attack known as DROWN (Decrypting RSA with Obsolete andWeakened eNcryption). This vulnerability exists due to a flaw in theSecure Sockets Layer Version 2 (SSLv2) implementation, and it allowscaptured TLS traffic to be decrypted. A man-in-the-middle attacker canexploit this to decrypt the TLS connection by utilizing previouslycaptured traffic and weak cryptography along with a series ofspecially crafted connections to an SSLv2 server that uses the sameprivate key.
Solution	Disable SSLv2 and export grade cryptography cipher suites. Ensure thatprivate keys are not used anywhere with server software that supportsSSLv2 connections.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**65821**
Port	25
Protocol	tcp
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 streamof bytes so that a wide

	variety of small biases are introduced intothe stream, decreasing its randomness.If plaintext is repeatedly encrypted (e.g., HTTP cookies), and anattacker is able to obtain many (i.e., tens of millions) ciphertexts,the attacker may be able to derive the plaintext.
Solution	Reconfigure the affected application, if possible, to avoid use of RC4ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browserand web server support.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	**HTTP TRACE / TRACK Methods Allowed**
Plugin ID	
Port	5432
Protocol	tcp
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 streamof bytes so that a wide variety of small biases are introduced intothe stream, decreasing its randomness.If plaintext is repeatedly encrypted (e.g., HTTP cookies), and anattacker is able to obtain many (i.e., tens of millions) ciphertexts,the attacker may be able to derive the plaintext.
Solution	Reconfigure the affected application, if possible, to avoid use of RC4ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browserand web server support.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	**HTTP TRACE / TRACK Methods Allowed**
Plugin ID	**57582**
Port	25
Protocol	tcp
Synopsis	The SSL certificate chain for this service ends in an unrecognizedself-signed certificate.
Description	The X.509 certificate chain for this service is not signed by arecognized certificate authority. If the remote host is a public hostin production, this nullifies the use of SSL as anyone could establisha man-in-the-middle attack against the remote host. Note that this plugin does not check for certificate chains that endin a certificate that is not self-signed, but is signed by anunrecognized certificate authority.
Solution	Purchase or generate a proper SSL certificate for this service.
Risk Factor	Medium
CVSS v2.0 Base Score	64

Name	**HTTP TRACE / TRACK Methods Allowed**

Plugin ID	
Port	5432
Protocol	tcp
Synopsis	The SSL certificate chain for this service ends in an unrecognizedself-signed certificate.
Description	The X.509 certificate chain for this service is not signed by arecognized certificate authority. If the remote host is a public hostin production, this nullifies the use of SSL as anyone could establisha man-in-the-middle attack against the remote host. Note that this plugin does not check for certificate chains that endin a certificate that is not self-signed, but is signed by anunrecognized certificate authority.
Solution	Purchase or generate a proper SSL certificate for this service.
Risk Factor	Medium
CVSS v2.0 Base Score	64

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**26928**
Port	25
Protocol	tcp
Synopsis	The remote service supports the use of weak SSL ciphers.
Description	The remote host supports the use of SSL ciphers that offer weakencryption.Note: This is considerably easier to exploit if the attacker is on thesame physical network.
Solution	Reconfigure the affected application, if possible to avoid the use ofweak ciphers.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**81606**
Port	25
Protocol	tcp
Synopsis	The remote host supports a set of weak ciphers.
Description	The remote host supports EXPORT_RSA cipher suites with keys less thanor equal to 512 bits. An attacker can factor a 512-bit RSA modulus ina short amount of time.A man-in-the middle attacker may be able to downgrade the session touse EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it isrecommended to remove support for weak cipher suites.
Solution	Reconfigure the service to remove support for EXPORT_RSA ciphersuites.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**58751**
Port	25
Protocol	tcp
Synopsis	It may be possible to obtain sensitive information from the remotehost with SSL/TLS-enabled services.
Description	A vulnerability exists in SSL 3.0 and TLS 1.0 that could allowinformation disclosure if an attacker intercepts encrypted trafficserved from an affected system.TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode arenot affected.This plugin tries to establish an SSL/TLS remote connection using anaffected SSL version and cipher suite and then solicits return data.If returned application data is not fragmented with an empty orone-byte record, it is likely vulnerable.OpenSSL uses empty fragments as a countermeasure unless the'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSLis initialized.Microsoft implemented one-byte fragments as a countermeasure, and thesetting can be controlled via the registry keyHKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendExtraRecord.Therefore, if multiple applications use the same SSL/TLSimplementation, some may be vulnerable while others may not be,depending on whether or not a countermeasure has been enabled.Note that this plugin detects the vulnerability in the SSLv3/TLSv1protocol implemented in the server. It does not detect the BEASTattack where it exploits the vulnerability at HTTPS client-side(i.e., Internet browser). The detection at server-side does notnecessarily mean your server is vulnerable to the BEAST attack,because the attack exploits the vulnerability at the client-side, andboth SSL/TLS clients and servers can independently employ the splitrecord countermeasure.
Solution	Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported.Configure SSL/TLS servers to only support cipher suites that do notuse block ciphers. Apply patches if available.Note that additional configuration may be required after theinstallation of the MS12-006 security update in order to enable thesplit-record countermeasure. See Microsoft KB2643584 for details.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**104743**
Port	25
Protocol	tcp
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 anumber of cryptographic design flaws. Modern implementations of TLS 1.0mitigate these problems, but newer versions of TLS like 1.2 and 1.3 aredesigned

	against these flaws and should be used whenever possible.As of March 31, 2020, Endpoints that arenâ€™t enabled for TLS 1.2and 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 terminationpoints to which they connect) that can be verified as not beingsusceptible to any known exploits.
Solution	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
Risk Factor	Medium
CVSS v2.0 Base Score	61

Name	**HTTP TRACE / TRACK Methods Allowed**
Plugin ID	
Port	5432
Protocol	tcp
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 anumber of cryptographic design flaws. Modern implementations of TLS 1.0mitigate these problems, but newer versions of TLS like 1.2 and 1.3 aredesigned against these flaws and should be used whenever possible.As of March 31, 2020, Endpoints that arenâ€™t enabled for TLS 1.2and 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 terminationpoints to which they connect) that can be verified as not beingsusceptible to any known exploits.
Solution	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
Risk Factor	Medium
CVSS v2.0 Base Score	61

Name	**HTTP TRACE / TRACK Methods Allowed**
Plugin ID	**42263**
Port	23
Protocol	tcp
Synopsis	The remote Telnet server transmits traffic in cleartext.
Description	The remote host is running a Telnet server over an unencryptedchannel.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 toobtain credentials or other sensitive information and to modifytraffic exchanged between a client and server.SSH is preferred over Telnet since it protects credentials fromeavesdropping and can tunnel additional data streams such as an X11session.
Solution	Disable the Telnet service and use SSH instead.
Risk Factor	Medium

CVSS v2.0 Base Score	58

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**57640**
Port	80
Protocol	tcp
Synopsis	The remote web application discloses path information.
Description	At least one web application hosted on the remote web server disclosesthe physical path to its directories when a malformed request is sentto it.Leaking this kind of information may help an attacker fine-tuneattacks against the application and its backend.
Solution	Filter error messages containing path information.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**85582**
Port	80
Protocol	tcp
Synopsis	The remote web server may fail to mitigate a class of web applicationvulnerabilities.
Description	The remote web server does not set an X-Frame-Options response headeror a Content-Security-Policy 'frame-ancestors' response header in allcontent responses. This could potentially expose the site to aclickjacking or UI redress attack, in which an attacker can trick auser into clicking an area of the vulnerable page that is differentthan what the user perceives the page to be. This can result in a userperforming fraudulent or malicious transactions.X-Frame-Options has been proposed by Microsoft as a way to mitigateclickjacking attacks and is currently supported by all major browservendors.Content-Security-Policy (CSP) has been proposed by the W3C WebApplication Security Working Group, with increasing support amongall major browser vendors, as a way to mitigate clickjacking and otherattacks. The 'frame-ancestors' policy directive restricts whichsources can embed the protected resource.Note that while the X-Frame-Options and Content-Security-Policyresponse headers are not the only mitigations for clickjacking, theyare currently the most reliable methods that can be detected throughautomation. Therefore, this plugin may produce false positives ifother mitigation strategies (e.g., frame-busting JavaScript) aredeployed or if the page does not perform any security-sensitivetransactions.
Solution	Return the X-Frame-Options or Content-Security-Policy (with the'frame-ancestors' directive) HTTP header with the page's response.This prevents the page's content from being rendered by another sitewhen using the frame or iframe HTML tags.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**11229**
Port	80
Protocol	tcp
Synopsis	The remote web server contains a PHP script that is prone to aninformation disclosure attack.
Description	Many PHP installation tutorials instruct the user to create a PHP filethat calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessingsuch a file, a remote attacker can discover a large amount ofinformation about the remote web server, including : - The username of the user who installed PHP and if they are a SUDO user. - The IP address of the host. - The version of the operating system. - The web server version. - The root directory of the web server. - Configuration information about the remote PHP installation.
Solution	Remove the affected file(s).
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**51425**
Port	80
Protocol	tcp
Synopsis	The remote web server hosts a PHP script that is prone to a cross-site scripting attack.
Description	The version of phpMyAdmin fails to validate BBcode tags in user inputto the 'error' parameter of the 'error.php' script before using it togenerate dynamic HTML.An attacker may be able to leverage this issue to inject arbitraryHTML or script code into a user's browser to be executed within thesecurity context of the affected site. For example, this could beused to cause a page with arbitrary text and a link to an externalsite to be displayed.
Solution	Upgrade to phpMyAdmin 3.4.0-beta1 or later.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	HTTP TRACE / TRACK Methods Allowed
Plugin ID	**36083**
Port	80
Protocol	tcp
Synopsis	The remote web server contains a PHP script that is affected bymultiple issues.
escription	The version of phpMyAdmin installed on the remote host fails tosanitize user-supplied input to the 'file_path' parameter of the'bs_disp_as_mime_type.php' script

	before using it to read a file andreporting it in dynamically-generated HTML. An unauthenticated, remoteattacker may be able to leverage this issue to read arbitrary files,possibly from third-party hosts, or to inject arbitrary HTTP headersin responses sent to third-party users.Note that the application is also reportedly affected by several otherissues, although Nessus has not actually checked for them.
Solution	Upgrade to phpMyAdmin 3.1.3.1 or apply the patch referenced in theproject's advisory.
Risk Factor	Medium
CVSS v2.0 Base Score	50

Name	**HTTP TRACE / TRACK Methods Allowed**
Plugin ID	**49142**
Port	80
Protocol	tcp
Synopsis	The remote web server contains a PHP application that has a cross-site scripting vulnerability.
Description	The setup script included with the version of phpMyAdmin installed onthe remote host does not properly sanitize user-supplied input to the'verbose server name' field.A remote attacker could exploit this by tricking a user intoexecuting arbitrary script code.
Solution	Upgrade to phpMyAdmin 3.3.7 or later.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Low Vulnerabilities Detail

Name	X Server Detection
Plugin ID	10407
Port	6000
Protocol	tcp
Synopsis	An X11 server is listening on the remote host
Description	The remote host is running an X11 server. X11 is a client-serverprotocol that can be used to display graphical applications running ona given host on a remote client. Since the X11 traffic is not ciphered, it is possible for an attackerto eavesdrop on the connection.
Solution	Restrict access to this port. If the X11 client/server facility is notused, disable TCP support in X11 entirely (-nolisten tcp).
Risk Factor	Low
CVSS v2.0 Base Score	26

Name	Web Server Transmits Cleartext Credentials
Plugin ID	26194
Port	80
Protocol	tcp
Synopsis	The remote web server might transmit credentials in cleartext.
Description	The remote web server contains several HTML form fields containingan input of type 'password' which transmit their information toa remote web server in cleartext.An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.
Solution	Make sure that every sensitive form transmits content over HTTPS.
Risk Factor	Low
CVSS v2.0 Base Score	26

Name	Web Server Allows Password Auto-Completion
Plugin ID	42057
Port	80
Protocol	tcp
Synopsis	The 'autocomplete' attribute is not disabled on password fields.
Description	The remote web server contains at least one HTML form field that hasan input of type 'password' where 'autocomplete' is not set to 'off'.While this does not represent a risk to this web server per se, itdoes mean that users who use the affected forms may have theircredentials saved in their browsers, which could in turn lead to aloss of confidentiality if any of them use a shared host or if theirmachine is compromised at some point.
Solution	Add the attribute 'autocomplete=off' to these fields to preventbrowsers from caching credentials.

Risk Factor	Low
CVSS v2.0 Base Score	(vuoto)

Name	SSH Server CBC Mode Ciphers Enabled
Plugin ID	70658
Port	22
Protocol	tcp
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 messagefrom the ciphertext. Note that this plugin only checks for the options of the SSH server anddoes not check for vulnerable software versions.
Solution	Contact the vendor or consult product documentation to disable CBC modecipher encryption, and enable CTR or GCM cipher mode encryption.
Risk Factor	Low
CVSS v2.0 Base Score	26

Name	SSH Weak MAC Algorithms Enabled
Plugin ID	71049
Port	22
Protocol	tcp
Synopsis	The remote SSH server is configured to allow MD5 and 96-bit MACalgorithms.
Description	The remote SSH server is configured to allow either MD5 or 96-bit MACalgorithms, 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 and96-bit MAC algorithms.
Risk Factor	Low
CVSS v2.0 Base Score	26

Name	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Plugin ID	78479
Port	25
Protocol	tcp
Synopsis	It is possible to obtain sensitive information from the remote hostwith SSL/TLS-enabled services.

Description	The remote host is affected by a man-in-the-middle (MitM) informationdisclosure vulnerability known as POODLE. The vulnerability is due tothe way SSL 3.0 handles padding bytes when decrypting messagesencrypted using block ciphers in cipher block chaining (CBC) mode.MitM attackers can decrypt a selected byte of a cipher text in as fewas 256 tries if they are able to force a victim application torepeatedly send the same data over newly created SSL 3.0 connections.As long as a client and service both support SSLv3, a connection canbe 'rolled back' to SSLv3, even if TLSv1 or newer is supported by theclient and service.The TLS Fallback SCSV mechanism prevents 'version rollback' attackswithout impacting legacy clients; however, it can only protectconnections when the client and service support the mechanism. Sitesthat cannot disable SSLv3 immediately should enable this mechanism.This is a vulnerability in the SSLv3 specification, not in anyparticular SSL implementation. Disabling SSLv3 is the only way tocompletely mitigate the vulnerability.
Solution	Disable SSLv3.Services that must support SSLv3 should enable the TLS Fallback SCSVmechanism until SSLv3 can be disabled.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	**SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)**
Plugin ID	78479
Port	5432
Protocol	tcp
Synopsis	It is possible to obtain sensitive information from the remote hostwith SSL/TLS-enabled services.
Description	The remote host is affected by a man-in-the-middle (MitM) informationdisclosure vulnerability known as POODLE. The vulnerability is due tothe way SSL 3.0 handles padding bytes when decrypting messagesencrypted using block ciphers in cipher block chaining (CBC) mode.MitM attackers can decrypt a selected byte of a cipher text in as fewas 256 tries if they are able to force a victim application torepeatedly send the same data over newly created SSL 3.0 connections.As long as a client and service both support SSLv3, a connection canbe 'rolled back' to SSLv3, even if TLSv1 or newer is supported by theclient and service.The TLS Fallback SCSV mechanism prevents 'version rollback' attackswithout impacting legacy clients; however, it can only protectconnections when the client and service support the mechanism. Sitesthat cannot disable SSLv3 immediately should enable this mechanism.This is a vulnerability in the SSLv3 specification, not in anyparticular SSL implementation. Disabling SSLv3 is the only way tocompletely mitigate the vulnerability.
Solution	Disable SSLv3.Services that must support SSLv3 should enable the TLS Fallback SCSVmechanism until SSLv3 can be disabled.
Risk Factor	Medium
CVSS v2.0 Base Score	43

Name	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
Plugin ID	83738
Port	25
Protocol	tcp
Synopsis	The remote host supports a set of weak ciphers.
Description	The remote host supports EXPORT_DHE cipher suites with keys less thanor equal to 512 bits. Through cryptanalysis, a third party can findthe shared secret in a short amount of time.A man-in-the middle attacker may be able to downgrade the session touse EXPORT_DHE cipher suites. Thus, it is recommended to removesupport for weak cipher suites.
Solution	Reconfigure the service to remove support for EXPORT_DHE ciphersuites.
Risk Factor	Low
CVSS v2.0 Base Score	26

Name	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
Plugin ID	83875
Port	25
Protocol	tcp
Synopsis	The remote host allows SSL/TLS connections with one or moreDiffie-Hellman moduli less than or equal to 1024 bits.
Description	The remote host allows SSL/TLS connections with one or moreDiffie-Hellman moduli less than or equal to 1024 bits. Throughcryptanalysis, a third party may be able to find the shared secret ina short amount of time (depending on modulus size and attackerresources). This may allow an attacker to recover the plaintext orpotentially violate the integrity of connections.
Solution	Reconfigure the service to use a unique Diffie-Hellman moduli of 2048bits or greater.
Risk Factor	Low
CVSS v2.0 Base Score	26

Name	SSH Weak Key Exchange Algorithms Enabled
Plugin ID	153953
Port	22
Protocol	tcp
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 beenabled. This includes: diffie-hellman-group-exchange-sha1 diffie-hellman-group1-sha1 gss-gex-sha1-* gss-group1-sha1-* gss-group14-sha1-* rsa1024-sha1Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable softwareversions.
Solution	Contact the vendor or consult product documentation to disable the weak algorithms.
Risk Factor	Low
CVSS v2.0 Base Score	26