



## DC-1

Mon, 27 Oct 2025 04:56:24 UTC

### TABLE OF CONTENTS

#### Vulnerabilities by Host

- 192.168.1.7

#### Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

#### 192.168.1.7

2

2

7

4

82

CRITICAL

HIGH

MEDIUM

LOW

INFO

#### Scan Information

Start time: Mon Oct 27 04:47:24 2025

End time: Mon Oct 27 04:56:23 2025

#### Host Information

IP: 192.168.1.7

MAC Address: 00:0C:29:4D:FE:F2

OS: Linux Kernel 3.2.0-6-486 on Debian 7.11

#### Vulnerabilities

##### 201366 - Debian Linux SEoL (7.x)

#### Synopsis

An unsupported version of Debian Linux is installed on the remote host.

#### Description

According to its version, Debian Linux is 7.x. It is, therefore, no longer maintained by its vendor or provider.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://www.debian.org/News/2016/20160425>

#### Solution

Upgrade to a version of Debian Linux 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: 2024/07/03, Modified: 2025/03/26

**Plugin Output**

tcp/0

```
OS : Debian GNU/Linux 7 (wheezy)
Security End of Life : April 25, 2016
Time since Security End of Life (Est.) : >= 9 years
```

**58987 - PHP Unsupported Version Detection****Synopsis**

The remote host contains an unsupported version of a web application scripting language.

**Description**

According to its version, the installation of PHP on the remote host is no longer supported.

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

**See Also**

<http://php.net/eol.php>  
<https://wiki.php.net/rfc/releaseprocess>

**Solution**

Upgrade to a version of PHP that is currently supported.

**Risk Factor**

Critical

**CVSS v3.0 Base Score**

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

**CVSS v2.0 Base Score**

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

**References**

XREF IAVA:0001-A-0581

**Plugin Information**

Published: 2012/05/04, Modified: 2024/11/22

**Plugin Output**

tcp/80/www

```
Source : X-Powered-By: PHP/5.4.45-0+deb7u14
Installed version : 5.4.45-0+deb7u14
End of support date : 2015/09/03
Announcement : http://php.net/supported-versions.php
Supported versions : 8.1.x / 8.2.x / 8.3.x
```

**78515 - Drupal Database Abstraction API SQLi****Synopsis**

The remote web server is running a PHP application that is affected by a SQL injection vulnerability.

**Description**

The remote web server is running a version of Drupal that is affected by a SQL injection vulnerability due to a flaw in the Drupal database abstraction API, which allows a remote attacker to use specially crafted requests that can result in arbitrary SQL execution. This may lead to privilege escalation, arbitrary PHP execution, or remote code execution.

## See Also

<https://www.drupal.org/SA-CORE-2014-005>  
<https://www.drupal.org/project/drupal/releases/7.32>

## Solution

Upgrade to version 7.32 or later.

## Risk Factor

High

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

BID	70595
CVE	CVE-2014-3704
XREF	EDB-ID:34984
XREF	EDB-ID:34992
XREF	EDB-ID:34993
XREF	EDB-ID:35150

## Exploitable With

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

## Plugin Information

Published: 2014/10/16, Modified: 2022/04/11

## Plugin Output

tcp/80/www

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

```
POST /?q=node&destination=node HTTP/1.1
Host: 192.168.1.7
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: 117
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, /*
name[0];SELECT+@version;#=0;&name[0]=nessus&pass=nessus&test2=test&form_build_id=&form_id=user_login_block&op=Log+in
```

This produced the following truncated output (limited to 5 lines) :

```
----- snip -----
>Warning</em>: mb_strlen() expects parameter 1 to be string, array given in <em class="placeholder">drupal_strlen()</em> (line <em
class="placeholder">478</em> of <em class="placeholder">/var/www/includes/unicode.inc</em>).</li>
<li><em class="placeholder">Warning</em>: addcslashes() expects parameter 1 to be string, array given in <em
class="placeholder">DatabaseConnection-&gt;escapeLike()</em> (line <em class="placeholder">981</em> of <em
class="placeholder">/var/www/includes/database/database.inc</em>).</li>
<li>Sorry, unrecognized username or password. <a href="/user/password?
name[0%3BSELECT%20%40%40version%3B%23]=0%3B&amp;name[0]=nessus">Have you forgotten your password?</a></li>
</ul>
</div>
[...]
----- snip -----
```

118233 - MySQL 5.5.x < 5.5.62 Multiple Vulnerabilities (October 2018 CPU)

## Synopsis

The remote database server is affected by multiple vulnerabilities.

## Description

The version of MySQL running on the remote host is 5.5.x prior to 5.5.62. It is, therefore, affected by multiple vulnerabilities as noted in the October 2018 Critical Patch Update advisory. Please consult the CVRF details for the applicable CVEs for additional information.

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

## See Also

<https://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-62.html>  
<http://www.nessus.org/u?705136d8>

## Solution

Upgrade to MySQL version 5.5.62 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

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

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

CVE	CVE-2016-9843
CVE	CVE-2018-3133
CVE	CVE-2018-3174
CVE	CVE-2018-3282

## Plugin Information

Published: 2018/10/19, Modified: 2021/05/21

## Plugin Output

tcp/0

```
Path : /usr/sbin/mysqld
Installed version : 5.5.60-0+deb7u1
Fixed version : 5.5.62
```

## 136929 - JQuery 1.2 < 3.5.0 Multiple XSS

## Synopsis

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

## Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

## See Also

<https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>  
<https://security.paloaltonetworks.com/PAN-SA-2020-0007>

## Solution

Upgrade to JQuery version 3.5.0 or later.

**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)

**CVSS v3.0 Temporal Score**

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

**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**

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

**STIG Severity**

II

**References**

CVE	<a href="#">CVE-2020-11022</a>
CVE	<a href="#">CVE-2020-11023</a>
XREF	<a href="#">IAVB:2020-B-0030</a>
XREF	<a href="#">CEA-ID:CEA-2021-0004</a>
XREF	<a href="#">CEA-ID:CEA-2021-0025</a>
XREF	<a href="#">CISA-KNOWN-EXPLOITED:2025/02/13</a>

**Plugin Information**

Published: 2020/05/28, Modified: 2025/01/24

**Plugin Output**

tcp/80/www

```
URL : http://192.168.1.7/misc/jquery.js?v=1.4.4
Installed version : 1.4.4
Fixed version : 3.5.0
```

**111153 - MySQL 5.5.x < 5.5.61 Multiple Vulnerabilities (July 2018 CPU)****Synopsis**

The remote database server is affected by multiple vulnerabilities.

**Description**

The version of MySQL running on the remote host is 5.5.x prior to 5.5.61. It is, therefore, affected by multiple vulnerabilities as noted in the July 2018 Critical Patch Update advisory. Please consult the CVRF details for the applicable CVEs for additional information.

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

**See Also**

<https://dev.mysql.com/doc/relnotes/mysql/5.5/en/news-5-5-61.html>  
<http://www.nessus.org/u?50f36723>

**Solution**

Upgrade to MySQL version 5.5.61 or later.

**Risk Factor**

Medium

**CVSS v3.0 Base Score**

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

**CVSS v3.0 Temporal Score**

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

**CVSS v2.0 Base Score**

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

**CVSS v2.0 Temporal Score**

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

**References**

BID	103954
BID	104766
BID	104779
BID	104786
CVE	CVE-2018-2767
CVE	CVE-2018-3058
CVE	CVE-2018-3063
CVE	CVE-2018-3066
CVE	CVE-2018-3070
CVE	CVE-2018-3081

**Plugin Information**

Published: 2018/07/20, Modified: 2021/05/21

**Plugin Output**

tcp/0

```
Path : /usr/sbin/mysqld
Installed version : 5.5.60-0+deb7u1
Fixed version : 5.5.61
```

**138561 - MySQL Denial of Service (Jul 2020 CPU)****Synopsis**

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

**Description**

The version of MySQL running on the remote host is 5.7.29 and prior or 8.0.19 and prior. It is, therefore, affected by a vulnerability, as noted in the July 2020 Critical Patch Update advisory:

A Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.

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

**See Also**

<http://www.nessus.org/u?dc7b9bd1>

**Solution**

Refer to the vendor advisory.

**Risk Factor**

Medium

**CVSS v3.0 Base Score**

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

**CVSS v3.0 Temporal Score**

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

**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	<a href="#">CVE-2020-14567</a>
XREF	IAVA:2020-A-0321-S

**Plugin Information**

Published: 2020/07/16, Modified: 2023/11/01

**Plugin Output**

tcp/0

```
Path : /usr/sbin/mysqld
Installed version : 5.5.60-0+deb7u1
Fixed version : 5.7.30
```

**142591 - PHP < 7.3.24 Multiple Vulnerabilities****Synopsis**

The version of PHP running on the remote web server is affected by multiple vulnerabilities.

**Description**

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.24. It is, therefore affected by multiple vulnerabilities.

**See Also**

<https://www.php.net/ChangeLog-7.php#7.3.24>

**Solution**

Upgrade to PHP version 7.3.24 or later.

**Risk Factor**

Medium

**CVSS v3.0 Base Score**

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

**CVSS v2.0 Base Score**

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

**STIG Severity**

I

**References**

XREF	IAVA:2020-A-0510-S
------	--------------------

**Plugin Information**

Published: 2020/11/06, Modified: 2025/05/26

**Plugin Output**

tcp/80/www

```
URL : http://192.168.1.7/ (5.4.45-0+deb7u14 under X-Powered-By: PHP/5.4.45-0+deb7u14)
Installed version : 5.4.45-0+deb7u14
Fixed version : 7.3.24
```

**152853 - PHP < 7.3.28 Email Header Injection**

## Synopsis

The version of PHP running on the remote web server is affected by an email header injection vulnerability.

## Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.28. It is, therefore affected by an email header injection vulnerability, due to a failure to properly handle CR-LF sequences in header fields. An unauthenticated, remote attacker can exploit this, by inserting line feed characters into email headers, to gain full control of email header content.

## See Also

<https://www.php.net/ChangeLog-7.php#7.3.28>

## Solution

Upgrade to PHP version 7.3.28 or later.

## 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: 2021/08/26, Modified: 2025/05/26

## Plugin Output

tcp/80/www

```
URL : http://192.168.1.7/ (5.4.45-0+deb7u14 under X-Powered-By: PHP/5.4.45-0+deb7u14)
Installed version : 5.4.45-0+deb7u14
Fixed version : 7.3.28
```

## 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
```

## 121479 - web.config File Information Disclosure

### Synopsis

The remote web server hosts an application that is affected by an information disclosure vulnerability.

### Description

An information disclosure vulnerability exists in the remote web server due to the disclosure of the web.config file. An unauthenticated, remote attacker can exploit this, via a simple GET request, to disclose potentially sensitive configuration information.

### Solution

Ensure proper restrictions are in place, or remove the web.config file if the file is not required.

### 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: 2019/01/30, Modified: 2020/04/27

### Plugin Output

tcp/80/www

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

```
GET /web.config HTTP/1.1
Host: 192.168.1.7
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, */*
```

This produced the following truncated output (limited to 5 lines) :

```
----- snip -----
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
<system.webServer>
<!-- Don't show directory listings for URLs which map to a directory. -->
<directoryBrowse enabled="false" />
[...]
----- snip -----
```

## 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

## CVSS v2.0 Base Score

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

## References

CVE	<a href="#">CVE-1999-0524</a>
XREF	<a href="#">CWE:200</a>

## Plugin Information

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

## Plugin Output

icmp/0

The difference between the local and remote clocks is -19795 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)

## 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	<a href="#">32319</a>
CVE	<a href="#">CVE-2008-5161</a>
XREF	<a href="#">CERT:958563</a>
XREF	<a href="#">CWE:200</a>

## 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
hmac-sha2-256-96
hmac-sha2-512-96
```

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

```
hmac-md5
hmac-md5-96
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96
```

**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: 2025/03/31

**Plugin Output**

tcp/0

The Linux distribution detected was :

- Debian 7.0 (wheezy)
- Debian unstable (sid)
- Debian testing (wheezy)

**141394 - Apache HTTP Server Installed (Linux)****Synopsis**

The remote host has Apache HTTP Server software installed.

**Description**

Apache HTTP Server is installed on the remote Linux host.

**See Also**

<https://httpd.apache.org/>

**Solution**

n/a

**Risk Factor**

None

**References**

XREF IAVT:0001-T-0530

**Plugin Information**

Published: 2020/10/12, Modified: 2025/08/19

**Plugin Output**

tcp/0

```
Nessus detected 4 installs of Apache:  
Path : /usr/lib/apache2/mpm-worker/apache2  
Version : 2.2.22  
Running : no  
  
Configs found :  
  
Loaded modules :  
  
Path : /usr/lib/apache2/mpm-event/apache2  
Version : 2.2.22  
Running : no  
  
Configs found :  
  
Loaded modules :  
  
Path : /usr/lib/apache2/mpm-prefork/apache2  
Version : 2.2.22  
Running : no  
  
Configs found :  
  
Loaded modules :  
  
Path : /usr/lib/apache2/mpm-itk/apache2  
Version : 2.2.22  
Running : no  
  
Configs found :  
  
Loaded modules :
```

**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://192.168.1.7/  
Version : 2.2.99  
Source : Server: Apache/2.2.22 (Debian)  
backported : 1  
os : ConvertedDebian
```

**34098 - BIOS Info (SSH)****Synopsis**

BIOS info could be read.

**Description**

Using SMBIOS and UEFI, it was possible to get BIOS info.

**Solution**

N/A

**Risk Factor**

None

**Plugin Information**

Published: 2008/09/08, Modified: 2024/02/12

**Plugin Output**

tcp/0

```
Version : None  
Vendor : VMware, Inc.  
Release Date : 11/12/2020  
Secure boot : disabled
```

**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](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

Local checks have been enabled.

**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](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

Local checks have been enabled.

**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: 2025/07/14

## Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:debian:debian\_linux:7 -> Debian Linux

Following application CPE's matched on the remote system :

cpe:/a:apache:http\_server:2.2.22 -> Apache Software Foundation Apache HTTP Server  
cpe:/a:apache:http\_server:2.2.99 -> Apache Software Foundation Apache HTTP Server  
cpe:/a:drupal:drupal:7 -> Drupal  
cpe:/a:exiv2:libexiv2:0.23  
cpe:/a:gnupg:libgcrypt:1.5.0 -> GnuPG Libgcrypt  
cpe:/a:haxx:curl:7.26.0 -> Haxx Curl  
cpe:/a:haxx:libcurl:7.26.0 -> Haxx libcurl  
cpe:/a:jquery:jquery:1.4.4 -> jQuery  
cpe:/a:mysql:mysql:5.5.60-0%2bdeb7u1\_ -> MySQL MySQL  
cpe:/a:openbsd:openssh:6.0 -> OpenBSD OpenSSH  
cpe:/a:openbsd:openssh:6.0p1 -> OpenBSD OpenSSH  
cpe:/a:openssl:openssl:1.0.0 -> OpenSSL Project OpenSSL  
cpe:/a:openssl:openssl:1.0.1d -> OpenSSL Project OpenSSL  
cpe:/a:openssl:openssl:1.0.1t -> OpenSSL Project OpenSSL  
cpe:/a:php:php:5.4.45 -> PHP PHP  
cpe:/a:php:php:5.4.45-0%2bdeb7u14 -> PHP PHP  
cpe:/a:tukaani:xz:5.1.1 -> Tukaani XZ  
cpe:/a:vim:vim:7.3 -> Vim

182774 - Curl Installed (Linux / Unix)

## Synopsis

Curl is installed on the remote Linux / Unix host.

## Description

Curl (also known as curl and cURL) is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

## See Also

<https://curl.se/>

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2023/10/09, Modified: 2025/07/28

## Plugin Output

tcp/0

Path : /usr/bin/curl  
Version : 7.26.0  
Associated Package : curl 7.26.0-1  
Managed by OS : True

## 55472 - Device Hostname

### Synopsis

It was possible to determine the remote system hostname.

### Description

This plugin reports a device's hostname collected via SSH or WMI.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/06/30, Modified: 2025/07/28

### Plugin Output

tcp/0

```
Hostname : DC-1
DC-1 (hostname command)
```

## 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: 2025/03/12

### Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 100
```

## 18638 - Drupal Software Detection

### Synopsis

A content management system is running on the remote web server.

### Description

Drupal, an open source content management system written in PHP, is running on the remote web server.

### See Also

<https://www.drupal.org/>

### Solution

Ensure that the use of this software aligns with your organization's security and acceptable use policies.

### Risk Factor

None

## References

XREF IAVT:0001-T-0586

## Plugin Information

Published: 2005/07/07, Modified: 2023/05/24

## Plugin Output

tcp/80/www

URL : <http://192.168.1.7/>  
Version : 7

## 25203 - Enumerate IPv4 Interfaces via SSH

### Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

### Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

### Solution

Disable any unused IPv4 interfaces.

### Risk Factor

None

## Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

## Plugin Output

tcp/0

The following IPv4 addresses are set on the remote host :

- 192.168.1.7 (on interface eth0)
- 127.0.0.1 (on interface lo)

## 25202 - Enumerate IPv6 Interfaces via SSH

### Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

### Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

### Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

### Risk Factor

None

## Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

## Plugin Output

tcp/0

The following IPv6 interfaces are set on the remote host :

```
- fe80::20c:29ff:fe4d:fef2 (on interface eth0)
- ::1 (on interface lo)
```

### 33276 - Enumerate MAC Addresses via SSH

#### Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

#### Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

#### Solution

Disable any unused interfaces.

#### Risk Factor

None

#### Plugin Information

Published: 2008/06/30, Modified: 2022/12/20

#### Plugin Output

tcp/0

The following MAC address exists on the remote host :

```
- 00:0c:29:4d:fe:f2 (interface eth0)
```

### 170170 - Enumerate the Network Interface configuration via SSH

#### Synopsis

Nessus was able to parse the Network Interface data on the remote host.

#### Description

Nessus was able to parse the Network Interface data on the remote host.

#### Solution

n/a

#### Risk Factor

None

#### Plugin Information

Published: 2023/01/19, Modified: 2025/02/11

#### Plugin Output

tcp/0

```
lo:
IPv4:
- Address : 127.0.0.1
Netmask : 255.0.0.0
IPv6:
- Address : ::1
Prefixlen : 128
Scope : host
eth0:
MAC : 00:0c:29:4d:fe:f2
IPv4:
- Address : 192.168.1.7
Netmask : 255.255.255.0
Broadcast : 192.168.1.255
IPv6:
- Address : fe80::20c:29ff:fe4d:fef2
Prefixlen : 64
Scope : link
```

**179200 - Enumerate the Network Routing configuration via SSH****Synopsis**

Nessus was able to retrieve network routing information from the remote host.

**Description**

Nessus was able to retrieve network routing information the remote host.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2023/08/02, Modified: 2023/08/02

**Plugin Output**

tcp/0

```
Gateway Routes:  
eth0:  
  ipv4_gateways:  
    192.168.1.1:  
      subnets:  
        - 0.0.0.0/0  
Interface Routes:  
eth0:  
  ipv4_subnets:  
    - 192.168.1.0/24  
  ipv6_subnets:  
    - fe80::/64
```

**168980 - Enumerate the PATH Variables****Synopsis**

Enumerates the PATH variable of the current scan user.

**Description**

Enumerates the PATH variables of the current scan user.

**Solution**

Ensure that directories listed here are in line with corporate policy.

**Risk Factor**

None

**Plugin Information**

Published: 2022/12/21, Modified: 2025/07/28

**Plugin Output**

tcp/0

Nessus has enumerated the path of the current scan user :

```
/usr/local/bin  
/usr/bin  
/bin  
/usr/bin/X11  
/usr/games
```

**35716 - Ethernet Card Manufacturer Detection****Synopsis**

The manufacturer can be identified from the Ethernet OUI.

**Description**

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUs are registered by IEEE.

## See Also

<https://standards.ieee.org/faqs/regauth.html>  
<http://www.nessus.org/u?794673b4>

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

## Plugin Output

tcp/0

The following card manufacturers were identified :

00:0C:29:4D:FE:F2 : VMware, Inc.

## 86420 - Ethernet MAC Addresses

### Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

### Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

### Solution

n/a

### Risk Factor

None

## Plugin Information

Published: 2015/10/16, Modified: 2025/06/10

## Plugin Output

tcp/0

The following is a consolidated list of detected MAC addresses:

- 00:0C:29:4D:FE:F2

## 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

**Plugin Information**

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

**Plugin Output**

tcp/80/www

The remote web server type is :

Apache/2.2.22 (Debian)

**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: Mon, 27 Oct 2025 10:19:37 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.45-0+deb7u14
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Last-Modified: Mon, 27 Oct 2025 10:19:37 +0000
Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0
ETag: "1761560377"
Content-Language: en
X-Generator: Drupal 7 (http://drupal.org)
Vary: Accept-Encoding
Content-Length: 7564
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

Response Body :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RDFa 1.0//EN"
"http://www.w3.org/MarkUp/DTD/xhtml-rdfa-1.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RDFa 1.0" dir="ltr"
xmlns:content="http://pur1.org/rss/1.0/modules/content/"
xmlns:dc="http://purl.org/dc/terms/"
xmlns:foaf="http://xmlns.com/foaf/0.1/"
xmlns:og="http://ogp.me/ns#"
xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
xmlns:sioc="http://rdfs.org/sioc/ns#"
xmlns:sioc="http://rdfs.org/sioc/types#"
xmlns:skos="http://www.w3.org/2004/02/skos/core#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema#">

<head profile="http://www.w3.org/1999/xhtml/vocab">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="http://192.168.1.7/misc/favicon.ico" type="image/vnd.microsoft.icon" />
<meta name="Generator" content="Drupal 7 (http://drupal.org)" />
<title>Welcome to Drupal Site | Drupal Site</title>
```

```

<style type="text/css" media="all">@import url("http://192.168.1.7/modules/system/system.base.css?pn6csl");
@import url("http://192.168.1.7/modules/system/system.menus.css?pn6csl");
@import url("http://192.168.1.7/modules/system/system.messages.css?pn6csl");
@import url("http://192.168.1.7/modules/system/system.theme.css?pn6csl");</style>
<style type="text/css" media="all">@import url("http://192.168.1.7/modules/field/theme/field.css?pn6csl");
@import url("http://192.168.1.7/modules/node/node.css?pn6csl");
@import url("http://192.168.1.7/modules/search/search.css?pn6csl");
@import url("http://192.168.1.7/modules/user/user.css?pn6csl");
@import url("http://192.168.1.7/sites/all/modules/views/css/views.css?pn6csl");</style>
<style type="text/css" media="all">@import url("http://192.168.1.7/sites/all/modules/ctools/css/ctools.css?pn6csl");</style>
<style type="text/css" media="all">@import url("http://192.168.1.7/themes/bartik/css/layout.css?pn6csl");
@import url("http://192.168.1.7/themes/bartik/css/style.css?pn6csl");
@import url("http://192.168.1.7/themes/bartik/css/colors.css?pn6csl");</style>
<style type="text/css" media="print">@import url("http://192.168.1.7/themes/bartik/css/print.css?pn6csl");</style>

<!--[if lte IE 7]>
<link type="text/css" rel="stylesheet" href="http://192.168.1.7/themes/bartik/css/ie.css?pn6csl" media="all" />
<![endif]-->

<!--[if IE 6]>
<link type="text/css" rel="stylesheet" href="http://192.168.1.7/themes/bartik/css/ie6.css?pn6csl" media="all" />
<![endif]-->
<script type="text/javascript" src="http://192.168.1.7/misc/jquery.js?v=1.4.4"></script>
<script type="text/javascript" src="http://192.168.1.7/misc/jquery.once.js?v=1.2"></script>
<script type="text/javascript" src="http://192.168.1.7/misc/drupal.js?pn6csl"></script>
<script type="text/javascript">
<!--//--><![CDATA[//><!--
jQuery.extendDrupal.settings, {"basePath": "/", "pathPrefix": "", "ajaxPageState": {"theme": "bartik", "theme_token": "Xb7Krs5gBT0cEDDXB7fREFIQ8NauWobgl4ma5GI-cFSc", "js": {"misc\jquery.js":1, "misc\jquery.once.js":1, "misc\drupal.js":1}, "css": {"modules\system\system.base.css":1, "modules\system\system.menus.css":1, "modules\system\system.messages.css":1, "modules\system\system.theme.css":1, "modules\field\theme\field.css":1, "modules\node\node.css":1, "modules\search\search.css":1, "modules\user\user.css":1, "sites\all\modules\views\css\views.css":1, "sites\all\modules\ctools\css\ctools.css":1, "themes\bartik\css\layout.css":1, "themes\bartik\css\style.css":1, "themes\bartik\css\colors.css":1, "themes\bartik\css\print.css":1, "themes\bartik\css\ie.css":1, "themes\bartik\css\ie6.css":1}}});
//--><!]]>
</script>
</head>
<body class="html front not-logged-in one-sidebar sidebar-first page-node" >
<div id="skip-link">
<a href="#main-content" class="element-invisible element-focusable">Skip to main content</a>
</div>
<div id="page-wrapper"><div id="page">

<div id="header" class="without-secondary-menu"><div class="section clearfix">
<a href="/" title="Home" rel="home" id="logo">

</a>

<div id="name-and-slogan">
<div id="site-name">
<strong>
<a href="/" title="Home" rel="home"><span>Drupal Site</span></a>
</strong>
</div>

</div> <!-- /#name-and-slogan -->

<div id="main-menu" class="navigation">
<h2 class="element-invisible">Main menu</h2><ul id="main-menu-links" class="links clearfix"><li class="menu-218 first last active">
<a href="/" class="active">Home</a></li>
</ul> </div> <!-- /#main-menu -->

</div></div> <!-- /.section, #header -->

<div id="main-wrapper" class="clearfix"><div id="main" class="clearfix">

<div id="sidebar-first" class="column sidebar"><div class="section">
<div class="region region-sidebar-first">
<div id="block-user-login" class="block block-user">

<h2>User login</h2>

<div class="content">
<form action="/node?destination=node" method="post" id="user-login-form" accept-charset="UTF-8"><div><div class="form-item form-type-textfield form-item-name">
<label for="edit-name">Username <span class="form-required" title="This field is required.">*</span></label>
<input type="text" id="edit-name" name="name" value="" size="15" maxlength="60" class="form-text required" />
</div>
<div class="form-item form-type-password form-item-pass">
<label for="edit-pass">Password <span class="form-required" title="This field is required.">*</span></label>
<input type="password" id="edit-pass" name="pass" size="15" maxlength="128" class="form-text required" />
</div>
<div class="item-list"><ul><li class="first"><a href="/user/register" title="Create a new user account.">Create new account</a></li>
<li class="last"><a href="/user/password" title="Request new password via e-mail.">Request new password</a></li>
</ul></div><input type="hidden" name="form_build_id" value="form-Xz1ZtRoz33EDkQgf2c1Xjc_WQ_2ZsdnGviXRVm7Zjk" />
<input type="hidden" name="form_id" value="user_login_block" />
<div class="form-actions form-wrapper" id="edit-actions"><input type="submit" id="edit-submit" name="op" value="Log in" class="form-submit" /></div></div></form> </div>
</div>
</div>

```

```

</div></div> <!-- /.section, #sidebar-first -->

<div id="content" class="column"><div class="section">
<a id="main-content"></a>
<h1 class="title" id="page-title">
Welcome to Drupal Site </h1>
<div class="tabs">
</div>
<div class="region region-content">
<div id="block-system-main" class="block block-system">

<div class="content">
<div id="first-time"><p>No front page content has been created yet.</p></div> </div>
</div>
</div>

</div></div> <!-- /.section, #content -->

</div></div> <!-- #main, #main-wrapper -->

<div id="footer-wrapper"><div class="section">

<div id="footer" class="clearfix">
<div class="region region-footer">
<div id="block-system-powered-by" class="block block-system">

<div class="content">
<span>Powered by <a href="http://drupal.org">Drupal</a></span> </div>
</div>
</div>
</div> <!-- #footer -->

</div></div> <!-- /.section, #footer-wrapper -->

</div></div> <!-- #page, #page-wrapper -->
</body>
</html>

```

## 171410 - IP Assignment Method Detection

### Synopsis

Enumerates the IP address assignment method(static/dynamic).

### Description

Enumerates the IP address assignment method(static/dynamic).

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/02/14, Modified: 2025/07/28

### Plugin Output

tcp/0

```

+ lo
+ IPv4
- Address : 127.0.0.1
Assign Method : static
+ IPv6
- Address : ::1
Assign Method : static
+ eth0
+ IPv4
- Address : 192.168.1.7
Assign Method : static
+ IPv6
- Address : fe80::20c:29ff:fe4d:fef2
Assign Method : static

```

## 106658 - JQuery Detection

### Synopsis

file:///C:/Users/yashp/OneDrive/Desktop/DC-1\_VA Nessus.html

The web server on the remote host uses JQuery.

### Description

Nessus was able to detect JQuery on the remote host.

### See Also

<https://jquery.com/>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

### Plugin Output

tcp/80/www

URL : <http://192.168.1.7/misc/jquery.js?v=1.4.4>  
Version : 1.4.4

## 151883 - Libgcrypt Installed (Linux/UNIX)

### Synopsis

Libgcrypt is installed on this host.

### Description

Libgcrypt, a cryptography library, was found on the remote host.

### See Also

<https://gnupg.org/download/index.html>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/07/21, Modified: 2025/07/28

### Plugin Output

tcp/0

Nessus detected 2 installs of Libgcrypt:

Path : /lib/i386-linux-gnu/libgcrypt.so.11.7.0  
Version : 1.5.0

Path : /lib/i386-linux-gnu/libgcrypt.so.11  
Version : 1.5.0

## 157358 - Linux Mounted Devices

### Synopsis

Use system commands to obtain the list of mounted devices on the target machine at scan time.

### Description

Report the mounted devices information on the target machine at scan time using the following commands.  
`/bin/df -h /bin/lsblk /bin/mount -l`

This plugin only reports on the tools available on the system and omits any tool that did not return information when the command was ran.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/02/03, Modified: 2023/11/27

### Plugin Output

tcp/0

```
$ df -h
Filesystem Size Used Avail Use% Mounted on
rootfs 3.8G 1.7G 1.9G 47% /
udev 10M 0 10M 0% /dev
tmpfs 102M 228K 101M 1% /run
/dev/disk/by-uuid/98efd4b5-ef7d-4335-96c0-01fdf0f4a43b 3.8G 1.7G 1.9G 47% /
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 246M 0 246M 0% /run/shm

$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sr0 11:0 1 1024M 0 rom
sda 8:0 0 4G 0 disk
└─sda1 8:1 0 3.8G 0 part /
  ├─sda2 8:2 0 1K 0 part
  └─sda5 8:5 0 218M 0 part [SWAP]

$ mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,relatime,size=10240k,nn_inodes=128044,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=103448k,mode=755)
/dev/disk/by-uuid/98efd4b5-ef7d-4335-96c0-01fdf0f4a43b on / type ext4 (rw,relatime,errors=remount-ro,user_xattr,barrier=1,data=ordered)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /run/shm type tmpfs (rw,nosuid,nodev,noexec,relatime,size=251520k)
rpc_pipefs on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw,relatime)
```

## 193143 - Linux Time Zone Information

### Synopsis

Nessus was able to collect and report time zone information from the remote host.

### Description

Nessus was able to collect time zone information from the remote Linux host.

### Solution

None

### Risk Factor

None

### Plugin Information

Published: 2024/04/10, Modified: 2024/04/10

### Plugin Output

tcp/0

```
Via date: AEST +1000
Via /etc/timezone: Australia/Brisbane
Via /etc/localtime: AEST-10
```

## 95928 - Linux User List Enumeration

### Synopsis

Nessus was able to enumerate local users and groups on the remote Linux host.

### Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.

### Solution

None

### Risk Factor

None

### Plugin Information

Published: 2016/12/19, Modified: 2025/03/26

### Plugin Output

tcp/0

-----[ User Accounts ]-----

User : flag4  
Home folder : /home/flag4  
Start script : /bin/bash  
Groups : flag4

User : yash  
Home folder : /home/yash  
Start script : /bin/sh  
Groups : yash

User : yash1199  
Home folder : /home/yash1199  
Start script : /bin/sh  
Groups : yash1199

-----[ System Accounts ]-----

User : root  
Home folder : /root  
Start script : /bin/bash  
Groups : root

User : daemon  
Home folder : /usr/sbin  
Start script : /bin/sh  
Groups : daemon

User : bin  
Home folder : /bin  
Start script : /bin/sh  
Groups : bin

User : sys  
Home folder : /dev  
Start script : /bin/sh  
Groups : sys

User : sync  
Home folder : /bin  
Start script : /bin/sync  
Groups : nogroup

User : games  
Home folder : /usr/games  
Start script : /bin/sh  
Groups : games

User : man  
Home folder : /var/cache/man  
Start script : /bin/sh  
Groups : man

User : lp  
Home folder : /var/spool/lpd  
Start script : /bin/sh  
Groups : lp

User : mail  
Home folder : /var/mail  
Start script : /bin/sh  
Groups : mail

User : news  
Home folder : /var/spool/news  
Start script : /bin/sh

```

Groups : news

User : uucp
Home folder : /var/spool/uucp
Start script : /bin/sh
Groups : uucp

User : proxy
Home folder : /bin
Start script : /bin/sh
Groups : proxy

User : www-data
Home folder : /var/www
Start script : /bin/sh
Groups : www-data

User : backup
Home folder : /var/backups
Start script : /bin/sh
Groups : backup

User : list
Home folder : /var/list
Start script : /bin/sh
Groups : list

User : irc
Home folder : /var/run/ircd
Start script : /bin/sh
Groups : irc

User : gnats
Home folder : /var/lib/gnats
Start script : /bin/sh
Groups : gnats

User : nobody
Home folder : /nonexistent
Start script : /bin/sh
Groups : nogroup

User : libuuid
Home folder : /var/lib/libuuid
Start script : /bin/sh
Groups : libuuid

User : Debian-exim
Home folder : /var/spool/exim4
Start script : /bin/false
Groups : Debian-exim

User : statd
Home folder : /var/lib/nfs
Start script : /bin/false
Groups : nogroup

User : messagebus
Home folder : /var/run/dbus
Start script : /bin/false
Groups : messagebus

User : sshd
Home folder : /var/run/sshd
Start script : /usr/sbin/nologin
Groups : nogroup

User : mysql
Home folder : /nonexistent
Start script : /bin/false
Groups : mysql

```

-----[ Domain Accounts ]-----

## 129468 - MySQL Server Installed (Linux)

### Synopsis

MySQL Server is installed on the remote Linux host.

### Description

MySQL Server is installed on the remote Linux host.

### Solution

n/a

### Risk Factor

None

**Plugin Information**

Published: 2019/09/30, Modified: 2025/04/18

**Plugin Output**

tcp/0

```
Path : /usr/sbin/mysqld
Version : 5.5.60-0+deb7u1
```

**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: 2025/06/25

**Plugin Output**

tcp/0

Information about this scan :

```
Nessus version : 10.9.3
Nessus build : 20023
Plugin feed version : 202508200628
Scanner edition used : Nessus
```

```
ERROR: Your plugins have not been updated since 2025/8/20
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.
```

```
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : DC-1
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.9
Port scanner(s) : netstat
Port range : 65535
Ping RTT : 164.525 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes, as 'flag4' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
```

```
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/10/27 4:47 UTC
Scan duration : 522 sec
Scan for malware : no
```

## 64582 - Netstat Connection Information

### Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

### Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

### Plugin Output

tcp/0

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/22/ssh

Port 22/tcp was found to be open

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/68

Port 68/udp was found to be open

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

tcp/80/www

Port 80/tcp was found to be open

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

## Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

## See Also

<https://en.wikipedia.org/wiki/Netstat>

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

## Plugin Output

tcp/111/rpc-portmapper

Port 111/tcp was found to be open

## 14272 - Netstat Portscanner (SSH)

## Synopsis

Remote open ports can be enumerated via SSH.

## Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

## See Also

<https://en.wikipedia.org/wiki/Netstat>

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

## Plugin Output

udp/111/rpc-portmapper

Port 111/udp was found to be open

## 14272 - Netstat Portscanner (SSH)

## Synopsis

Remote open ports can be enumerated via SSH.

## Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

## See Also

<https://en.wikipedia.org/wiki/Netstat>

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

## Plugin Output

udp/704

Port 704/udp was found to be open

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

## See Also

<https://en.wikipedia.org/wiki/Netstat>

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

## Plugin Output

udp/33929/rpc-status

Port 33929/udp was found to be open

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

## See Also

<https://en.wikipedia.org/wiki/Netstat>

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

## Plugin Output

udp/33996

Port 33996/udp was found to be open

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

## See Also

<https://en.wikipedia.org/wiki/Netstat>

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

## Plugin Output

tcp/37226

Port 37226/tcp was found to be open

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

## See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/43406

Port 43406/udp was found to be open

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

### Plugin Output

udp/45720

Port 45720/udp was found to be open

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

<https://en.wikipedia.org/wiki/Netstat>

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2004/08/15, Modified: 2025/05/27

**Plugin Output**

tcp/59938/rpc-status

Port 59938/tcp was found to be open

**209654 - OS Fingerprints Detected****Synopsis**

Multiple OS fingerprints were detected.

**Description**

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2025/02/26, Modified: 2025/03/03

**Plugin Output**

tcp/0

Following OS Fingerprints were found

Remote operating system : Debian 7.0 Linux Kernel 3.2  
Confidence level : 56  
Method : MLSinFP  
Type : unknown  
Fingerprint : unknown

Remote operating system : Linux Kernel 3.2 on Debian 7.0 (wheezy)  
Confidence level : 95  
Method : SSH  
Type : general-purpose  
Fingerprint : SSH:SSH-2.0-OpenSSH\_6.0p1 Debian-4+deb7u7

Remote operating system : Linux Kernel 3.2.0-6-486  
Confidence level : 99  
Method : uname  
Type : general-purpose  
Fingerprint : uname:Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686 GNU/Linux

Remote operating system : Linux Kernel 3.2 on Debian 7.0 (wheezy)  
Debian unstable (sid)  
Debian testing (wheezy)  
Confidence level : 45  
Method : HTTP  
Type : general-purpose  
Fingerprint : unknown

Remote operating system : Linux Kernel 2.x  
Confidence level : 54  
Method : SinFP  
Type : general-purpose  
Fingerprint : SinFP:  
P1:B10113:F0x12:W14600:00204ffff:M1460:  
P2:B10113:F0x12:W14480:00204fffff0402080afffffff4445414401030304:M1460:  
P3:B00000:F0x00:W0:00:M0  
P4:191303\_7\_p=22

Remote operating system : Linux Kernel 3.2.0-6-486 on Debian 7.11  
Confidence level : 100  
Method : LinuxDistribution

Type : general-purpose  
Fingerprint : unknown

## 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: 2025/06/03

### Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 3.2.0-6-486 on Debian 7.11
Confidence level : 100
Method : LinuxDistribution
```

```
The remote host is running Linux Kernel 3.2.0-6-486 on Debian 7.11
```

## 97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

### Synopsis

Information about the remote host can be disclosed via an authenticated session.

### Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

### Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'password' authentication.
```

```
The output of "uname -a" is :
Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686 GNU/Linux
```

```
Local checks have been enabled for this host.
The remote Debian system is :
7.11
```

```
OS Security Patch Assessment is available for this host.
Runtime : 4.772351 seconds
```

## 117887 - OS Security Patch Assessment Available

**Synopsis**

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

**Description**

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

**Solution**

n/a

**Risk Factor**

None

**References**

XREF IAVB:0001-B-0516

**Plugin Information**

Published: 2018/10/02, Modified: 2021/07/12

**Plugin Output**

tcp/0

OS Security Patch Assessment is available.

Account : flag4  
Protocol : SSH

**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: 2025/08/19

**Plugin Output**

tcp/22/ssh

Service : ssh  
Version : 6.0p1  
Banner : SSH-2.0-OpenSSH\_6.0p1 Debian-4+deb7u7

**168007 - OpenSSL Installed (Linux)****Synopsis**

OpenSSL was detected on the remote Linux host.

**Description**

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

Note: This plugin leverages the '-maxdepth' find command option, which is a feature implemented by the GNU find binary. If the target does not support this option, such as HP-UX and AIX devices, users will need to enable 'thorough tests' in their scan policy to run the find command without using a '-maxdepth' argument.

## See Also

<https://openssl.org/>

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2022/11/21, Modified: 2025/07/28

## Plugin Output

tcp/0

Nessus detected 7 installs of OpenSSL:

```
Path : /usr/bin/openssl
Version : 1.0.1t
Associated Package : openssl 1.0.1t-1
Managed by OS : True

Path : /usr/lib/i386-linux-gnu/libcrypto.so.1.0.0
Version : 1.0.0
Associated Package : libssl1.0.0

Path : /usr/lib/i386-linux-gnu/i686/cmov/libcrypto.so.1.0.0
Version : 1.0.0
Associated Package : libssl1.0.0

Path : /usr/lib/i386-linux-gnu/i586/libcrypto.so.1.0.0
Version : 1.0.0
Associated Package : libssl1.0.0

Path : /usr/lib/i386-linux-gnu/i586/libssl.so.1.0.0
Version : 1.0.1d
Associated Package : libssl1.0.0

Path : /usr/lib/i386-linux-gnu/i686/cmov/libssl.so.1.0.0
Version : 1.0.1d
Associated Package : libssl1.0.0

Path : /usr/lib/i386-linux-gnu/libssl.so.1.0.0
Version : 1.0.1d
Associated Package : libssl1.0.0
```

We are unable to retrieve version info from the following list of OpenSSL files. However, these installs may include their version within the filename or the filename of the Associated Package.

e.g. libssl.so.3 (OpenSSL 3.x), libssl.so.1.1.1 (OpenSSL 1.1.x)

```
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libsureware.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libatalia.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libcswift.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libcapi.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libnuron.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libubsec.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libpadlock.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libgmp.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libaep.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libgost.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libchil.so
/usr/lib/i386-linux-gnu/openssl-1.0.0/engines/lib4758cca.so
```

## 216936 - PHP Scripting Language Installed (Unix)

## Synopsis

The PHP scripting language is installed on the remote Unix host.

**Description**

The PHP scripting language is installed on the remote Unix host.

Note: Enabling the 'Perform thorough tests' setting will search the file system much more broadly.  
Thorough test is required to get results on hosts running MacOS.

**See Also**

<https://www.php.net>

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2024/06/13, Modified: 2025/07/28

**Plugin Output**

tcp/0

```
Path : /usr/bin/php5
Version : 5.4.45
Associated Package : php5-cli: /usr/bin/php5
INI file : /etc/php5/cli/php.ini
INI source : PHP binary grep
Managed by OS : True
```

**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: 2025/05/26

**Plugin Output**

tcp/80/www

Nessus was able to identify the following PHP version information :

```
Version : 5.4.45-0+deb7u14
Source : X-Powered-By: PHP/5.4.45-0+deb7u14
```

**179139 - Package Manager Packages Report (nix)****Synopsis**

Reports details about packages installed via package managers.

**Description**

Reports details about packages installed via package managers

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2023/08/01, Modified: 2025/05/07

**Plugin Output**

tcp/0

Successfully retrieved and stored package data.

**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: 2025/08/12

**Plugin Output**

tcp/0

. You need to take the following 2 actions :

[ JQuery 1.2 < 3.5.0 Multiple XSS (136929) ]  
+ Action to take : Upgrade to JQuery version 3.5.0 or later.  
+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).

[ MySQL Denial of Service (Jul 2020 CPU) (138561) ]  
+ Action to take : Refer to the vendor advisory.  
+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).

**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: 4
- program: 100000 (portmapper), version: 3
- 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: 4
- program: 100000 (portmapper), version: 3
- 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/33929/rpc-status

The following RPC services are available on UDP port 33929 :

- 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

tcp/59938/rpc-status

The following RPC services are available on TCP port 59938 :

- program: 100024 (status), version: 1

## 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

### 133964 - SELinux Status Check

#### Synopsis

SELinux is available on the host and plugin was able to check if it is enabled.

#### Description

SELinux is available on the host and plugin was able to check if it is enabled.

#### Solution

n/a

#### Risk Factor

None

#### Plugin Information

Published: 2020/02/25, Modified: 2025/07/28

#### Plugin Output

tcp/0

SELinux config has been found on the host.

SELinux is enabled.

SELinux policy: default.

SELinux status: permissive.

### 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  
hmac-sha2-256  
hmac-sha2-256-96  
hmac-sha2-512  
hmac-sha2-512-96  
umac-64@openssh.com

The server supports the following options for server\_host\_key\_algorithms :

ecdsa-sha2-nistp256  
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  
hmac-sha2-256  
hmac-sha2-256-96  
hmac-sha2-512  
hmac-sha2-512-96  
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  
ecdh-sha2-nistp256  
ecdh-sha2-nistp384  
ecdh-sha2-nistp521

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

```

## 102094 - SSH Commands Require Privilege Escalation

### Synopsis

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them.

### Description

This plugin reports the SSH commands that failed with a response indicating that privilege escalation is required to run them. Either privilege escalation credentials were not provided, or the command failed to run with the provided privilege escalation credentials.

NOTE: Due to limitations inherent to the majority of SSH servers, this plugin may falsely report failures for commands containing error output expected by sudo, such as 'incorrect password', 'not in the sudoers file', or 'not allowed to execute'.

### Solution

n/a

### Risk Factor

None

### References

XREF	IAVB:0001-B-0507
------	------------------

### Plugin Information

Published: 2017/08/01, Modified: 2020/09/22

### Plugin Output

tcp/0

```

Login account : flag4
Commands failed due to lack of privilege escalation :
- Escalation account : (none)
Escalation method : (none)
Plugins :
- Plugin Filename : apache_http_server_nix_installed.nbin
Plugin ID : 141394
Plugin Name : Apache HTTP Server Installed (Linux)
- Command : "strings '/var/log/apache2' 2>&1"
Response : "strings: /var/log/apache2: Permission denied"
Error : ""
- Command : "strings '/var/log/apache2' 2>&1"
Response : "strings: /var/log/apache2: Permission denied"
Error : ""
- Plugin Filename : bios_get_info_ssh.nasl
Plugin ID : 34098
Plugin Name : BIOS Info (SSH)
- Command : "LC_ALL=C /usr/sbin/dmidecode"
Response : "# dmidecode 2.11"
Error : "\n/dev/mem: Permission denied"
- Plugin Filename : enumerate_aws_ami_nix.nasl
Plugin ID : 90191
Plugin Name : Amazon Web Services EC2 Instance Metadata Enumeration (Unix)
- Command : "/usr/sbin/dmidecode -s system-version 2>&1"
Response : "/dev/mem: Permission denied"
Error : ""
- Plugin Filename : enumerate_oci_nix.nasl
Plugin ID : 154138
Plugin Name : Oracle Cloud Infrastructure Instance Metadata Enumeration (Linux / Unix)
- Command : "LC_ALL=C /usr/sbin/dmidecode -s chassis-asset-tag 2>&1"
Response : "/dev/mem: Permission denied"
Error : ""
- Plugin Filename : host_tag_nix.nbin
Plugin ID : 87414
Plugin Name : Host Tagging (Linux)
- Command : "sh -c \"echo 55d04bd9d30e486aa15065014f3a29ca > /etc/enable_tag && echo OK\""
Response : null
Error : "\nsh: 1: \ncannot create /etc/enable_tag: Permission denied"
- Plugin Filename : localusers_pwexpiry.nasl
Plugin ID : 83303
Plugin Name : Unix / Linux - Local Users Information : Passwords Never Expire
- Command : "cat /etc/shadow"
Response : null
Error : "\ncat: \n/etc/shadow\n: Permission denied"

```

**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

**90707 - SSH SCP Protocol Detection****Synopsis**

The remote host supports the SCP protocol over SSH.

**Description**

The remote host supports the Secure Copy (SCP) protocol over SSH.

**See Also**

[https://en.wikipedia.org/wiki/Secure\\_copy](https://en.wikipedia.org/wiki/Secure_copy)

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2016/04/26, Modified: 2024/07/24

**Plugin Output**

tcp/22/ssh

**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_6.0p1 Debian-4+deb7u7
SSH supported authentication : publickey,password
```

**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/80/www

A web server is running on this port.

**22869 - Software Enumeration (SSH)****Synopsis**

It was possible to enumerate installed software on the remote host via SSH.

**Description**

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

## Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

## Risk Factor

None

## References

XREF IAVT:0001-T-0502

## Plugin Information

Published: 2006/10/15, Modified: 2025/03/26

## Plugin Output

tcp/0

Here is the list of packages installed on the remote Debian Linux system :

```

ii acpi 1.6-1 i386 displays information on ACPI devices
ii acpi-support-base 0.140-5+deb7u3 all scripts for handling base ACPI events such as the power button
ii acpid 1:2.0.16-1+deb7u1 i386 Advanced Configuration and Power Interface event daemon
ii adduser 3.113+nmu3 all add and remove users and groups
ii apache2 2.2.22-13+deb7u13 i386 Apache HTTP Server metapackage
ii apache2-mpm-prefork 2.2.22-13+deb7u13 i386 Apache HTTP Server - traditional non-threaded model
ii apache2-utils 2.2.22-13+deb7u13 i386 utility programs for webservers
ii apache2.2-bin 2.2.22-13+deb7u13 i386 Apache HTTP Server common binary files
ii apache2.2-common 2.2.22-13+deb7u13 i386 Apache HTTP Server common files
ii apt 0.9.7.9+deb7u7 i386 commandline package manager
ii apt-listchanges 2.85.11 all package change history notification tool
ii apt-utils 0.9.7.9+deb7u7 i386 package management related utility programs
ii aptitude 0.6.8.2-1 i386 terminal-based package manager
ii aptitude-common 0.6.8.2-1 all architecture independent files for the aptitude package manager
ii at 3.1.13-2+deb7u1 i386 Delayed job execution and batch processing
ii base-files 7.1wheezy11 i386 Debian base system miscellaneous files
ii base-passwd 3.5.26 i386 Debian base system master password and group files
ii bash 4.2+dfsg-0.1+deb7u4 i386 GNU Bourne Again SHell
ii bash-completion 1:2.0-1 all programmable completion for the bash shell
ii bc 1.06.95-2 i386 The GNU bc arbitrary precision calculator language
ii bind9-host 1:9.8.4.dfsg.P1-6+nmu2+deb7u20 i386 Version of 'host' bundled with BIND 9.X
ii binutils 2.22-8+deb7u3 i386 GNU assembler, linker and binary utilities
ii bsd-mailx 8.1.2-0.2011106cv5-1+deb7u1 i386 simple mail user agent
ii bsdmainutils 9.0.3 i386 collection of more utilities from FreeBSD
ii bsdtutils 1:2.20.1-5.3 i386 Basic utilities from 4.4BSD-Lite
ii busybox 1:1.20.0-7 i386 Tiny utilities for small and embedded systems
ii bwidget 1.9.5-1 all Extension widgets for Tcl/Tk
ii bzip2 1.0.6-4 i386 high-quality block-sorting file compressor - utilities
ii ca-certificates 20130119+deb7u3 all Common CA certificates
ii checkpolicy 2.1.8-2 i386 SELinux policy compiler
ii console-setup 1.88 all console font and keymap setup program
ii console-setup-linux 1.88 all Linux specific part of console-setup
ii coreutils 8.13-3.5 i386 GNU core utilities
ii cpio 2.11+dfsg-0.1+deb7u2 i386 GNU cpio -- a program to manage archives of files
ii cpp 4:4.7.2-1 i386 GNU C preprocessor (cpp)
ii cpp-4.7 4.7.2-5 i386 GNU C preprocessor
ii cron 3.0pl1-124 i386 process scheduling daemon
ii curl 7.26.0-1+wheezy25+deb7u1 i386 command line tool for transferring data with URL syntax
ii dash 0.5.7-3 i386 POSIX-compliant shell
ii dbus 1.6.8-1+deb7u6 i386 simple interprocess messaging system (daemon and utilities)
ii dc 1.06.95-2 i386 The GNU dc arbitrary precision reverse-polish calculator
ii debconf 1.5.49 all Debian configuration management system
ii debconf-i18n 1.5.49 all full internationalization support for debconf
ii debian-archive-keyring 2014.3~deb7u1 all GnuPG archive keys of the Debian archive
ii debian-faq 5.0.1 all Debian FAQ
ii debianutils 4.3.2 i386 Miscellaneous utilities specific to Debian
ii dictionaries-common 1.12.11 all Common utilities for spelling dictionary tools
ii diffutils 1:3.2-6 i386 File comparison utilities
ii discover 2.1.2-5.2 i386 hardware identification system
ii discover-data 2.2010.10.18 all Data lists for Discover hardware detection system
ii dkms 2.2.0.3-1.2 all Dynamic Kernel Module Support Framework
ii dmidecode 2.11-9 i386 SMBIOS/DMI table decoder
ii dmsetup 2:1.02.74-8 i386 Linux Kernel Device Mapper userspace library
ii dnsutils 1:9.8.4.dfsg.P1-6+nmu2+deb7u20 i386 Clients provided with BIND
ii doc-debian 6.1 all Debian Project documentation and other documents
ii dpkg 1.16.18 i386 Debian package management system
ii e2fslibs 1.42.5-1.1+deb7u1 i386 ext2/ext3/ext4 file system libraries
ii e2fsprogs 1.42.5-1.1+deb7u1 i386 ext2/ext3/ext4 file system utilities
ii eject 2.1.5+deb1+cv320081104-13+deb7u1 i386 ejects CDs and operates CD-Changers under Linux
ii exim4 4.80-7+deb7u6 all metapackage to ease Exim MTA (v4) installation
ii exim4-base 4.80-7+deb7u6 i386 support files for all Exim MTA (v4) packages
ii exim4-config 4.80-7+deb7u6 all configuration for the Exim MTA (v4)
ii exim4-daemon-light 4.80-7+deb7u6 i386 lightweight Exim MTA (v4) daemon
ii fakeroot 1.18.4-2 i386 tool for simulating superuser privileges
ii file 5.11-2+deb7u9 i386 Determines file type using "magic" numbers
ii findutils 4.4.2-4 i386 utilities for finding files--find, xargs
ii fontconfig 2.9.0-7.1+deb7u1 i386 generic font configuration library - support binaries
ii fontconfig-config 2.9.0-7.1+deb7u1 all generic font configuration library - configuration

```

```

ii fonts-droid 20111207+git-1 all handheld device font with extensive style and language support
ii ftp 0.17-27 i386 classical file transfer client
ii gcc 4:4.7.2-1 i386 GNU C compiler
ii gcc-4.7 4.7.2-5 i386 GNU C compiler
ii gcc-4.7-base 4.7.2-5 i386 GCC, the GNU Compiler Collection (base package)
ii gcc-4.7-multilib 4.7.2-5 i386 GNU C compiler (multilib files)
ii gcc-4.9-backport 4.9.2-10+deb7u1 i386 GCC, the GNU Compiler Collection
ii gcc-multilib 4:4.7.2-1 i386 GNU C compiler (multilib files)
ii geoip-database 20130213-1 all IP lookup command line tools that use the GeoIP library (country database)
ii gettext-base 0.18.1.1-9 i386 GNU Internationalization utilities for the base system
ii ghostscript 9.05~dfsg-6.3+deb7u8 i386 interpreter for the PostScript language and for PDF
ii gnupg 1.4.12-7+deb7u9 i386 GNU privacy guard - a free PGP replacement
ii gpg 1.4.12-7+deb7u9 i386 GNU privacy guard - signature verification tool
ii grep 2.12-2 i386 GNU grep, egrep and fgrep
ii groff-base 1.21-9 i386 GNU troff text-formatting system (base system components)
ii grub-common 1.99-27+deb7u3 i386 GRand Unified Bootloader (common files)
ii grub-pc 1.99-27+deb7u3 i386 GRand Unified Bootloader, version 2 (PC/BIOS version)
ii grub-pc-bin 1.99-27+deb7u3 i386 GRand Unified Bootloader, version 2 (PC/BIOS binaries)
ii grub2-common 1.99-27+deb7u3 i386 GRand Unified Bootloader (common files for version 2)
ii gsfonts 1:8.11+urwcyrl.0.7~pre44-4.2 all Fonts for the Ghostscript interpreter(s)
ii gzip 1.5-1.1 i386 GNU compression utilities
ii hicolor-icon-theme 0.12-1 all default fallback theme for FreeDesktop.org icon themes
ii hostname 3.11 i386 utility to set/show the host name or domain name
ii iamerican 3.3.02-6 all American English dictionary for ispell (standard version)
ii ibritish 3.3.02-6 all British English dictionary for ispell (standard version)
ii ienglish-common 3.3.02-6 all Common files for British and American ispell dictionaries
ii ifupdown 0.7.8 i386 high level tools to configure network interfaces
ii imagemagick 8:6.7.7.10-5+deb7u22 i386 image manipulation programs
ii imagemagick-common 8:6.7.7.10-5+deb7u22 all image manipulation programs -- infrastructure
ii info 4.13a.dfsg.1-10 i386 Standalone GNU Info documentation browser
ii initramfs-tools 0.109.1 all generic modular initramfs generator
ii initscripts 2.88dsf-41+deb7u1 i386 scripts for initializing and shutting down the system
ii insserv 1.14.0-5 i386 boot sequence organizer using LSB init.d script dependency information
ii install-info 4.13a.dfsg.1-10 i386 Manage installed documentation in info format
ii installation-report 2.49 all system installation report
ii iproute 20120521-3+b3 i386 networking and traffic control tools
ii iptables 1.4.14-3.1 i386 administration tools for packet filtering and NAT
ii iputils-ping 3:20101006-1+b1 i386 Tools to test the reachability of network hosts
ii isc-dhcp-client 4.2.2.dfsg.1-5+deb7u9 i386 ISC DHCP client
ii isc-dhcp-common 4.2.2.dfsg.1-5+deb7u9 i386 common files used by all the isc-dhcp* packages
ii iso-codes 3.41-1 all ISO language, territory, currency, script codes and their translations
ii ispell 3.3.02-6 i386 International Ispell (an interactive spelling corrector)
ii kbd 1.15.3-9 i386 Linux console font and keytable utilities
ii keyboard-configuration 1.88 all system-wide keyboard preferences
ii klibc-utils 2.0.1-3.1 i386 small utilities built with klibc for early boot
ii kmod 9-3 i386 tools for managing Linux kernel modules
ii krb5-locales 1.10.1+dfsg-5+deb7u9 all Internationalization support for MIT Kerberos
ii laptop-detect 0.13.7 i386 attempt to detect a laptop
ii less 444-4 i386 pager program similar to more
ii lib64gcc1 1:4.7.2-5 i386 GCC support library (64bit)
ii lib64omp1 4.7.2-5 i386 GCC OpenMP (GOMP) support library (64bit)
ii lib64itm1 4.7.2-5 i386 GNU Transactional Memory Library (64bit)
ii lib64quadmath0 4.7.2-5 i386 GCC Quad-Precision Math Library (64bit)
ii libac11 2.2.51-8 i386 Access control list shared library
ii libaio1 0.3.109-3 i386 Linux kernel AIO access library - shared library
ii libapache2-mod-php5 5.4.45-0+deb7u14 i386 server-side, HTML-embedded scripting language (Apache 2 module)
ii libapalo14 3.3.7-3 i386 Security Enhanced Linux policy analysis library
ii libapr1 1.4.6-3+deb7u2 i386 Apache Portable Runtime Library
ii libaprutil1 1.4.1-3+deb7u1 i386 Apache Portable Runtime Utility Library
ii libaprutil1-dbd-sqlite3 1.4.1-3+deb7u1 i386 Apache Portable Runtime Utility Library - SQLite3 Driver
ii libaprutil1-ldap 1.4.1-3+deb7u1 i386 Apache Portable Runtime Utility Library - LDAP Driver
ii libapt-inst1.5 0.9.7.9+deb7u7 i386 deb package format runtime library
ii libapt-pkg4.12 0.9.7.9+deb7u7 i386 package management runtime library
ii libasprintf0c2 0.18.1.1-9 i386 GNU library to use fprintf and friends in C++
ii libatk1.0-0 2.4.0-2 i386 ATK accessibility toolkit
ii libatk1.0-data 2.4.0-2 all Common files for the ATK accessibility toolkit
ii libattr1 1:2.4.46-8 i386 Extended attribute shared library
ii libaudit0 1:1.7.18-1.1 i386 Dynamic library for security auditing
ii libavahi-client3 0.6.31-2 i386 Avahi client library
ii libavahi-common-data 0.6.31-2 i386 Avahi common data files
ii libavahi-common3 0.6.31-2 i386 Avahi common library
ii libbind9-80 1:9.8.4.dfsg.Pt1-6+nmu2+deb7u20 i386 BIND9 Shared Library used by BIND
ii libblkid1 2.20.1-5.3 i386 block device id library
ii libboost-iostreams1.49.0 1.49.0-3.2 i386 Boost.Iostreams Library
ii libbsd0 0.4.2-1 i386 utility functions from BSD systems - shared library
ii libbz2-1.0 1.0.6-4 i386 high-quality block-sorting file compressor library - runtime
ii libc-bin 2.13-38+deb7u12 i386 Embedded GNU C Library: Binaries
ii libc-dev-bin 2.13-38+deb7u12 i386 Embedded GNU C Library: Development binaries
ii libc6 2.13-38+deb7u12 i386 Embedded GNU C Library: Shared libraries
ii libc6-amd64 2.13-38+deb7u12 i386 Embedded GNU C Library: 64bit Shared libraries for AMD64
ii libc6-dev 2.13-38+deb7u12 i386 Embedded GNU C Library: Development Libraries and Header Files
ii libc6-dev-amd64 2.13-38+deb7u12 i386 Embedded GNU C Library: 64bit Development Libraries for AMD64
ii libc6-i686 2.13-38+deb7u12 i386 Embedded GNU C Library: Shared libraries [i686 optimized]
ii libcairo2 1.12.2-3+deb7u1 i386 The Cairo 2D vector graphics library
ii libcap2 1:2.22-1.2 i386 support for getting/setting POSIX.1e capabilities
ii libclass-isa-perl 0.36-3 all report the search path for a class's ISA tree
ii libcomerr2 1.42.5-1.1+deb7u1 i386 common error description library
ii libcroco3 0.6.6-2+deb7u1 i386 Cascading Style Sheet (CSS) parsing and manipulation toolkit
ii libcurl2 1.5.3-5+deb7u8 i386 Common UNIX Printing System(tm) - Core library
ii libcurlimage2 1.5.3-5+deb7u8 i386 Common UNIX Printing System(tm) - Raster image library
ii libcurl3 7.26.0-1+wheezy25+deb7u1 i386 easy-to-use client-side URL transfer library (OpenSSL flavour)
ii libcwidget3 0.5.16-3.4 i386 high-level terminal interface library for C++ (runtime files)
ii libdatriel 0.2.5-3 i386 Double-array trie library
ii libdb5.1 5.1.29-5+deb7u1 i386 Berkeley v5.1 Database Libraries [runtime]
ii libdbd-mysql-perl 4.021-1+deb7u3 i386 Perl5 database interface to the MySQL database
ii libdbi-perl 1.622-1+deb7u1 i386 Perl Database Interface (DBI)
ii libibus-1-3 1.6.8-1+deb7u6 i386 simple interprocess messaging system (library)
ii libibus-glib-1-2 0.100.2-1 i386 simple interprocess messaging system (Glib-based shared library)
ii libdevmapper1.02.1 2:1.02.74-8 i386 Linux Kernel Device Mapper userspace library

```

```
ii libdiscover2 2.1.2-5.2 i386 hardware identification library
ii libdjvuibre-text 3.5.25.3-1 all Linguistic support files for libdjvuibre
ii libdjvuibre21 3.5.25.3-1 i386 Runtime support for the DjVu image format
ii libdns88 1:9.8.4.dfsg.P1-6+nmu2+deb7u20 i386 DNS Shared Library used by BIND
ii libdrm-intel 2.4.40-1~deb7u2 i386 Userspace interface to intel-specific kernel DRM services -- runtime
ii libdrm-nouveau1a 2.4.40-1~deb7u2 i386 Userspace interface to nouveau-specific kernel DRM services -- runtime
ii libdrm-radeon1 2.4.40-1~deb7u2 i386 Userspace interface to radeon-specific kernel DRM services -- runtime
ii libdrm2 2.4.40-1~deb7u2 i386 Userspace interface to kernel DRM services -- runtime
ii libedit2 2.11-20080614-5 i386 BSD editline and history libraries
ii libept1.4.12 1.0.9 i386 High-level library for managing Debian package information
ii libevent-2.0-5 2.0.19-stable-3+deb7u2 i386 Asynchronous event notification library
ii libexiv2-12 0.23-1+deb7u2 i386 EXIF/IPTC metadata manipulation library
ii libexpat1 2.1.0-1+deb7u5 i386 XML parsing C library - runtime library
ii libff15 3.0.10-3+deb7u2 i386 Foreign Function Interface library runtime
ii libfontconfig1 2.9.0-7.1+deb7u1 i386 generic font configuration library - runtime
ii libfontenc1 1:1.1.1-1 i386 X11 font encoding library
ii libfreetype6 2.4.9-1.1+deb7u7 i386 FreeType 2 font engine, shared library files
ii libfuse2 2.9.0-2+deb7u2 i386 Filesystem in Userspace (library)
ii libgc1c2 1:7.1-9.1+deb7u1 i386 conservative garbage collector for C and C++
ii libgcc1 1:4.7.2-5 i386 GCC support library
ii libgcrypt11 1.5.0-5+deb7u6 i386 LGPL Crypto library - runtime library
ii libgd2-xpm 2.0.36~rc1-dfsg-6.1+deb7u11 i386 GD Graphics Library version 2
ii libgdbm3 1.8.3-11 i386 GNU dbm database routines (runtime version)
ii libgdk-pixbuf2.0-0 2.26.1-1+deb7u8 i386 GDK Pixbuf library
ii libgdk-pixbuf2.0-common 2.26.1-1+deb7u8 all GDK Pixbuf library - data files
ii libgeoip1 1.4.8+dfsg-3 i386 non-DNS IP-to-country resolver library
ii libgl1-mesa-dri 8.0.5-4+deb7u2 i386 free implementation of the OpenGL API -- DRI modules
ii libgl1-mesa-glx 8.0.5-4+deb7u2 i386 free implementation of the OpenGL API -- GLX runtime
ii libglade2-0 1:2.6.4-1 i386 library to load .glade files at runtime
ii libglapi-mesa 8.0.5-4+deb7u2 i386 free implementation of the GL API -- shared library
ii libglib2.0-0 2.33.12+really2.32.4-5 i386 GLib library of C routines
ii libglib2.0-data 2.33.12+really2.32.4-5 all Common files for GLib library
ii libgmp10 2.5.0.5+dfsg-2 i386 Multiprecision arithmetic library
ii libgnutls26 2.12.20-8+deb7u5 i386 GNU TLS library - runtime library
ii libgomp1 4.7.2-5 i386 GCC OpenMP (GOMP) support library
ii libgpg-error0 1.10-3.1 i386 library for common error values and messages in GnuPG components
ii libgpgme11 1.2.0-1.4+deb7u1 i386 GPGME - GnuPG Made Easy
ii libgpm2 1.20.4-6 i386 General Purpose Mouse - shared library
ii libgs9 9.05~dfsg-6.3+deb7u8 i386 interpreter for the PostScript language and for PDF - Library
ii libgs9-common 9.05~dfsg-6.3+deb7u8 all interpreter for the PostScript language and for PDF - common files
ii libgssapi-krb5-2 1.10.1+dfsg-5+deb7u9 i386 MIT Kerberos runtime libraries - krb5 GSS-API Mechanism
ii libgssglue1 0.4-2 i386 mechanism-switch gssapi library
ii libgtk2.0-0 2.24.10-2 i386 GTK+ graphical user interface library
ii libgtk2.0-bin 2.24.10-2 i386 programs for the GTK+ graphical user interface library
ii libgtk2.0-common 2.24.10-2 all common files for the GTK+ graphical user interface library
ii libhtml-template-perl 2.91-1 all module for using HTML templates with Perl
ii libice6 2:1.0.8-2 i386 X11 Inter-Client Exchange library
ii libidn11 1.25-2+deb7u3 i386 GNU Libidn library, implementation of IETF IDN specifications
ii libijs-0.35 0.35-8 i386 IJS raster image transport protocol: shared library
ii libilmbase6 1.0.1-4 i386 several utility libraries from ILM used by OpenEXR
ii libisc84 1:9.8.4.dfsg.P1-6+nmu2+deb7u20 i386 ISC Shared Library used by BIND
ii libisccc80 1:9.8.4.dfsg.P1-6+nmu2+deb7u20 i386 Command Channel Library used by BIND
ii libisccfg82 1:9.8.4.dfsg.P1-6+nmu2+deb7u20 i386 Config File Handling Library used by BIND
ii libitm1 4.7.2-5 i386 GNU Transactional Memory Library
ii libjasper1 1.900.1-13+deb7u6 i386 JasPer JPEG-2000 runtime library
ii libjbig0 2.0-2+deb7u1 i386 JBIGkit libraries
ii libjbig2dec0 0.13-4~deb7u2 i386 JBIG2 decoder library - shared libraries
ii libjpeg8 8d-1+deb7u1 i386 Independent JPEG Group's JPEG runtime library
ii libk5crypto3 1.10.1+dfsg-5+deb7u9 i386 MIT Kerberos runtime libraries - Crypto Library
ii libkeyutils1 1.5.5-3+deb7u1 i386 Linux Key Management Utilities (library)
ii liblible 2.0.1-3.1 i386 minimal libe subset for use with initramfs
ii liblkmmod2 9-3 i386 libkmod shared library
ii libkrb5-3 1.10.1+dfsg-5+deb7u9 i386 MIT Kerberos runtime libraries
ii libkrb5support0 1.10.1+dfsg-5+deb7u9 i386 MIT Kerberos runtime libraries - Support library
ii liblcms1 1.19.dfsg2-1.2+deb7u1 i386 Little CMS color management library
ii liblcms2-2 2.2+git20110628-2.2+deb7u2 i386 Little CMS 2 color management library
ii libldap-2.4-2 2.4.31-2+deb7u3 i386 OpenLDAP libraries
ii liblensfun-data 0.2.5-2 all Lens Correction library - Data
ii liblensfun0 0.2.5-2 i386 Lens Correction library - Runtime files
ii liblocale-gettext-perl 1.05-7+b1 i386 module using libc functions for internationalization in Perl
ii liblockfile-bin 1.09-5 i386 support binaries for and cli utilities based on liblockfile
ii liblockfile1 1.09-5 i386 NFS-safe locking library
ii liblqr1-0 0.4.1-2 i386 converts plain array images into multi-size representation
ii libltdl7 2.4.2-1.1 i386 A system independent dlopen wrapper for GNU libtool
ii liblwres80 1:9.8.4.dfsg.P1-6+nmu2+deb7u20 i386 Lightweight Resolver Library used by BIND
ii liblzma5 5.1.1alpha+20120614-2 i386 XZ-format compression library
ii libmagic1 5.11-2+deb7u9 i386 File type determination library using "magic" numbers
ii libmagickcore5 8:6.7.7.10-5+deb7u22 i386 low-level image manipulation library
ii libmagickcore5-extra 8:6.7.7.10-5+deb7u22 i386 low-level image manipulation library - extra codecs
ii libmagickwand5 8:6.7.7.10-5+deb7u22 i386 image manipulation library
ii libmount1 2.20.1-5.3 i386 block device id library
ii libmpc2 0.9-4 i386 multiple precision complex floating-point library
ii libmpfr4 3.1.0-5 i386 multiple precision floating-point computation
ii libmysqlclient18 5.5.60-0+deb7u1 i386 MySQL database client library
ii libncurses5 5.9-10 i386 shared libraries for terminal handling
ii libncursesw5 5.9-10 i386 shared libraries for terminal handling (wide character support)
ii libnetpbm10 2:10.0-15+b1 i386 Graphics conversion tools shared libraries
ii libnewt0.52 0.52.14-11.1 i386 Not Erik's Windowing Toolkit - text mode windowing with slang
ii libnfnetlink0 1.0.0-1.1 i386 Netfilter netlink library
ii libnfsidmap2 0.25-4 i386 NFS idmapping library
ii libonig2 5.9.1-1+deb7u1 i386 Oniguruma regular expressions library
ii libopenexr6 1.6.1-6+deb7u1 i386 runtime files for the OpenEXR image library
ii libp11-kit0 0.12-3 i386 Library for loading and coordinating access to PKCS#11 modules - runtime
ii libpam-modules 1.1.3-7.1 i386 Pluggable Authentication Modules for PAM
ii libpam-modules-bin 1.1.3-7.1 i386 Pluggable Authentication Modules for PAM - helper binaries
ii libpam-runtime 1.1.3-7.1 all Runtime support for the PAM library
ii libpam0g 1.1.3-7.1 i386 Pluggable Authentication Modules library
ii libpango1.0-0 1.30.0-1 i386 Layout and rendering of internationalized text
ii libpaper-utils 1.1.24+nmu2 i386 library for handling paper characteristics (utilities)
```

```

ii libpaper1 1.1.24+nmu2 i386 library for handling paper characteristics
ii libpcis1 1:3.1.9-6 i386 Linux PCI Utilities (shared library)
ii libpciaccess0 0.13.1-2 i386 Generic PCI access library for X
ii libpcre3 1:8.30-5 i386 Perl 5 Compatible Regular Expression Library - runtime files
ii libpipeline1 1.2.1-1 i386 pipeline manipulation library
ii libpixman-1-0 0.26.0-4+deb7u2 i386 pixel-manipulation library for X and cairo
ii libpng12-0 1.2.49-1+deb7u2 i386 PNG library - runtime
ii libpopt0 1.16-7 i386 lib for parsing cmdline parameters
ii libprocps0 1:3.3.3-3+deb7u1 i386 library for accessing process information from /proc
ii libpth20 2.0.7-16 i386 The GNU Portable Threads
ii libqdbm14 1.8.78-2 i386 QDBM Database Libraries without GDBM wrapper[runtime]
ii libqpoli 3.3.7-3 i386 Security Enhanced Linux policy abstraction library
ii libquadmath0 4.7.2-5 i386 GCC Quad-Precision Math Library
ii libreadline6 6.2+dfsg-0.1 i386 GNU readline and history libraries, run-time libraries
ii librsvg2-2 2.36.1-2+deb7u3 i386 SAX-based renderer library for SVG files (runtime)
ii librsvg2-common 2.36.1-2+deb7u3 i386 SAX-based renderer library for SVG files (extra runtime)
ii librtmp0 2.4+20111222.git4e06e21-1+deb7u1 i386 toolkit for RTMP streams (shared library)
ii libssasl2-2 2.1.25.dfsg1-6+deb7u1 i386 Cyrus SASL - authentication abstraction library
ii libssasl2-modules 2.1.25.dfsg1-6+deb7u1 i386 Cyrus SASL - pluggable authentication modules
ii libselinux1 2.1.9-5 i386 SELinux runtime shared libraries
ii libsemanage-common 2.1.6-6 all Common files for SELinux policy management libraries
ii libsemanage1 2.1.6-6 i386 SELinux policy management library
ii libsepolicy 2.1.4-3 i386 SELinux library for manipulating binary security policies
ii libsetools-tcl 3.3.7-3 i386 SETools Tcl bindings
ii libsigc++-2.0-0c2a 2.2.10-0.2 i386 type-safe Signal Framework for C++ - runtime
ii libssl1.2 2.2.4-15 i386 S-Lang programming library - runtime version
ii libsm6 2:1.2.1-2 i386 X11 Session Management library
ii libsqlite3-0 3.7.13-1+deb7u4 i386 SQLite 3 shared library
ii libss2 1.42.5-1.1+deb7u1 i386 command-line interface parsing library
ii libssh2-1 1.4.2-1.1+deb7u2 i386 SSH2 client-side library
ii libssl1.0.0 1.0.1t-1+deb7u4 i386 SSL shared libraries
ii libstdc++6 4.7.2-5 i386 GNU Standard C++ Library v3
ii libswitch-perl 2.16-2 all switch statement for Perl
ii libsystemd-login0 44-11+deb7u5 i386 systemd login utility library
ii libtasn1-3 2.13-2+deb7u5 i386 Manage ASN.1 structures (runtime)
ii libtext-charwidth-perl 0.04-7+b1 i386 get display widths of characters on the terminal
ii libtext-iconv-perl 1.7-5 i386 converts between character sets in Perl
ii libtext-wrapi18n-perl 0.06-7 all internationalized substitute of Text::Wrap
ii libthai-data 0.1.18-2 all Data files for Thai language support library
ii libthai0 0.1.18-2 i386 Thai language support library
ii libtiff4 3.9.6-11+deb7u11 i386 Tag Image File Format (TIFF) library (old version)
ii libtinfo5 5.9-10 i386 shared low-level terminfo library for terminal handling
ii libtirpc1 0.2.2-5+deb7u1 i386 transport-independent RPC library
ii libtokyocabinet9 1.4.47-2 i386 Tokyo Cabinet Database Libraries [runtime]
ii libudev0 175-7.2 i386 libudev shared library
ii libusb-0.1-4 2:0.1.12-20+nmu1 i386 userspace USB programming library
ii libusb-1.0-0 2:1.0.11-1 i386 userspace USB programming library
ii libustr-1.0-1 1.0.4-3 i386 Micro string library: shared library
ii libutempter0 1.1.5-4 i386 A privileged helper for utmp/wtmp updates (runtime)
ii libuuid-perl 0.02-5 i386 Perl extension for using UUID interfaces as defined in e2fsprogs
ii libuuid1 2.20.1-5.3 i386 Universally Unique ID library
ii libwmf0.2-7 0.2.8.4-10.3+deb7u2 i386 Windows metafile conversion library
ii libwrap0 7.6.q-24 i386 Wietse Venema's TCP wrappers library
ii libx11-6 2:1.5.0-1+deb7u4 i386 X11 client-side library
ii libx11-data 2:1.5.0-1+deb7u4 all X11 client-side library
ii libx11-xcb1 2:1.5.0-1+deb7u4 i386 Xlib/XCB interface library
ii libxapian22 1.2.12-2+deb7u1 i386 Search engine library
ii libxaug1 1:1.0.7-1 i386 X11 authorisation library
ii libxaw7 2:1.0.10-2 i386 X11 Athena Widget library
ii libxcb-glx0 1.8.1-2+deb7u1 i386 X C Binding, glx extension
ii libxcb-render0 1.8.1-2+deb7u1 i386 X C Binding, render extension
ii libxcb-shape0 1.8.1-2+deb7u1 i386 X C Binding, shape extension
ii libxcb-shm0 1.8.1-2+deb7u1 i386 X C Binding, shm extension
ii libxcb1 1.8.1-2+deb7u1 i386 X C Binding
ii libcomposite1 1:0.4.3-2 i386 X11 Composite extension library
ii libcursor1 1:1.1.13-1+deb7u2 i386 X cursor management library
ii libxdamage1 1:1.1.3-2 i386 X11 damaged region extension library
ii libxdmcp6 1:1.1.1-1 i386 X11 Display Manager Control Protocol library
ii libxext6 2:1.3.1-2+deb7u1 i386 X11 miscellaneous extension library
ii libxfixed3 1:5.0-4+deb7u2 i386 X11 miscellaneous 'fixes' extension library
ii libxfont1 1:1.4.5-5+deb7u1 i386 X11 font rasterisation library
ii libxft2 2.3.1-1 i386 FreeType-based font drawing library for X
ii libxi6 2:1.6.1-1+deb7u3 i386 X11 Input extension library
ii libxinerama1 2:1.1.2-1+deb7u1 i386 X11 Xinerama extension library
ii libxkbfile1 1:1.0.8-1 i386 X11 keyboard file manipulation library
ii libxml2 2.8.0+dfsg1-7+wheezy12 i386 GNOME XML library
ii libxmlmu2 2:1.1.1-1 i386 X11 miscellaneous utility library
ii libxmlmu1 2:1.1.1-1 i386 X11 miscellaneous micro-utility library
ii libxpm4 1:3.5.10-1+deb7u1 i386 X11 pixmap library
ii libxrandr2 2:1.3.2-2+deb7u2 i386 X11 RandR extension library
ii libxrender1 1:0.9.7-1+deb7u3 i386 X Rendering Extension client library
ii libxss1 1:1.2.2-1 i386 X11 Screen Saver extension library
ii libxt6 1:1.1.3-1+deb7u1 i386 X11 toolkit intrinsics library
ii libxtst6 2:1.2.1-1+deb7u2 i386 X11 Testing -- Record extension library
ii libxv1 2:1.0.7-1+deb7u2 i386 X11 Video extension library
ii libxxf86dg1 2:1.1.3-2+deb7u1 i386 X11 Direct Graphics Access extension library
ii libxxf86vm1 1:1.1.2-1+deb7u1 i386 X11 XFree86 video mode extension library
ii linux-base 3.5 all Linux image base package
ii linux-headers-3.2.0-6-686-pae 3.2.102-1 i386 Header files for Linux 3.2.0-6-686-pae
ii linux-headers-3.2.0-6-common 3.2.102-1 i386 Common header files for Linux 3.2.0-6
ii linux-headers-686-pae 3.2+46+deb7u2 i386 Header files for Linux 686-pae configuration (meta-package)
ii linux-image-3.2.0-4-486 3.2.96-2 i386 Linux 3.2 for older PCs
ii linux-image-3.2.0-6-486 3.2.102-1 i386 Linux 3.2 for older PCs
ii linux-image-486 3.2+46+deb7u2 i386 Linux for older PCs (meta-package)
ii linux-kbuild-3.2 3.2.101-1 i386 Kbuild infrastructure for Linux 3.2
ii linux-libc-dev 3.2.102-1 i386 Linux support headers for userspace development
ii locales 2.13-38+deb7u12 all Embedded GNU C Library: National Language (locale) data [support]
ii login 1:4.1.5.1-1+deb7u1 i386 system login tools
ii logrotate 3.8.1-4 i386 Log rotation utility

```

```

ii lsb-base 4.1+Debian8+deb7u1 all Linux Standard Base 4.1 init script functionality
ii lsb-release 4.1+Debian8+deb7u1 all Linux Standard Base version reporting utility
ii lsof 4.86+dfsg-1 i386 Utility to list open files
ii m4 1.4.16-3 i386 a macro processing language
ii make 3.81-8.2 i386 An utility for Directing compilation.
ii man-db 2.6.2-1 i386 on-line manual pager
ii manpages 3.44-1 all Manual pages about using a GNU/Linux system
ii manpages-dev 3.44-1 all Manual pages about using GNU/Linux for development
ii mawk 1.3.3-17 i386 a pattern scanning and text processing language
ii menu 2.1.46 i386 generates programs menu for all menu-aware applications
ii mime-support 3.52-1+deb7u1 all MIME files 'mime.types' & 'mailcap', and support programs
ii mlocate 0.23.1-1 i386 quickly find files on the filesystem based on their name
ii module-init-tools 9-3 all transitional dummy package (module-init-tools to kmod)
ii mount 2.20.1-5.3 i386 Tools for mounting and manipulating filesystems
ii multiarch-support 2.13-38+deb7u12 i386 Transitional package to ensure multiarch compatibility
ii mutt 1.5.21-6.2+deb7u3 i386 text-based mailreader supporting MIME, GPG, PGP and threading
ii mysql-client 5.5.60-0+deb7u1 all MySQL database client (metapackage depending on the latest version)
ii mysql-client-5.5 5.5.60-0+deb7u1 i386 MySQL database client binaries
ii mysql-common 5.5.60-0+deb7u1 all MySQL database common files, e.g. /etc/mysql/my.cnf
ii mysql-server 5.5.60-0+deb7u1 all MySQL database server (metapackage depending on the latest version)
ii mysql-server-5.5 5.5.60-0+deb7u1 i386 MySQL database server binaries and system database setup
ii mysql-server-core-5.5 5.5.60-0+deb7u1 i386 MySQL database server binaries
ii nano 2.2.6-1+b1 i386 small, friendly text editor inspired by Pico
ii ncurses-base 5.9-10 all basic terminal type definitions
ii ncurses-bin 5.9-10 i386 terminal-related programs and man pages
ii ncurses-term 5.9-10 all additional terminal type definitions
ii net-tools 1.60-24.2 i386 The NET-3 networking toolkit
ii netbase 5.0 all Basic TCP/IP networking system
ii netcat-traditional 1.10-40 i386 TCP/IP swiss army knife
ii netpbm 2:10.0-15+b1 i386 Graphics conversion tools between image formats
ii nfs-common 1:1.2.6-4 i386 NFS support files common to client and server
ii openssh-blacklist 0.4.1+nmu1 all list of default blacklisted OpenSSH RSA and DSA keys
ii openssh-blacklist-extra 0.4.1+nmu1 all list of non-default blacklisted OpenSSH RSA and DSA keys
ii openssh-client 1:6.0p1-4+deb7u7 i386 secure shell (SSH) client, for secure access to remote machines
ii openssh-server 1:6.0p1-4+deb7u7 i386 secure shell (SSH) server, for secure access from remote machines
ii openssl 1.0.1t-1+deb7u4 i386 Secure Socket Layer (SSL) binary and related cryptographic tools
ii os-prober 1.58 i386 utility to detect other OSes on a set of drives
ii passwd 1:4.1.5.1-1+deb7u1 i386 change and administer password and group data
ii patch 2.6.1-3+deb7u1 i386 Apply a diff file to an original
ii pciutils 1:3.1.9-6 i386 Linux PCI Utilities
ii perl 5.14.2-21+deb7u6 i386 Larry Wall's Practical Extraction and Report Language
ii perl-base 5.14.2-21+deb7u6 i386 minimal Perl system
ii perl-modules 5.14.2-21+deb7u6 all Core Perl modules
ii php5 5.4.45-0+deb7u14 all server-side, HTML-embedded scripting language (metapackage)
ii php5-cli 5.4.45-0+deb7u14 i386 command-line interpreter for the php5 scripting language
ii php5-common 5.4.45-0+deb7u14 i386 Common files for packages built from the php5 source
ii php5-curl 5.4.45-0+deb7u14 i386 CURL module for php5
ii php5-gd 5.4.45-0+deb7u14 i386 GD module for php5
ii php5-ldap 5.4.45-0+deb7u14 i386 LDAP module for php5
ii php5-mysql 5.4.45-0+deb7u14 i386 MySQL module for php5
ii php5-xmlrpc 5.4.45-0+deb7u14 i386 XML-RPC module for php5
ii policycoreutils 2.1.10-9+deb7u1 i386 SELinux core policy utilities
ii poppler-data 0.4.5-10 all encoding data for the poppler PDF rendering library
ii procmail 3.22-20+deb7u2 i386 Versatile e-mail processor
ii procps 1:3.3.3-3+deb7u1 i386 /proc file system utilities
ii psmisc 22.19-1+deb7u1 i386 utilities that use the proc file system
ii python 2.7.3-4+deb7u1 all interactive high-level object-oriented language (default version)
ii python-apt 0.8.8.2 i386 Python interface to libapt-pkg
ii python-apt-common 0.8.8.2 all Python interface to libapt-pkg (locales)
ii python-chardet 2.0.1-2 all universal character encoding detector
ii python-crypto 2.6-4+deb7u8 i386 cryptographic algorithms and protocols for Python
ii python-debian 0.1.21 all Python modules to work with Debian-related data formats
ii python-debianbts 1.11 all Python interface to Debian's Bug Tracking System
ii python-fpconst 0.7.2-5 all Utilities for handling IEEE 754 floating point special values
ii python-gevent 0.13.6-1+nmu3 i386 gevent is a coroutine-based Python networking library
ii python-greenlet 0.3.1-2.5 i386 Lightweight in-process concurrent programming
ii python-ipy 1:0.75-1 all Python module for handling IPv4 and IPv6 addresses and networks
ii python-minimal 2.7.3-4+deb7u1 all minimal subset of the Python language (default version)
ii python-oauthlib 0.1.2-1 all generic, spec-compliant implementation of OAuth for Python
ii python-reportbug 6.4.4+deb7u2 all Python modules for interacting with bug tracking systems
ii python-requests 0.12.1-1+deb7u1 all elegant and simple HTTP library for Python, built for human beings
ii python-selinux 2.1.9-5 i386 Python bindings to SELinux shared libraries
ii python-semanage 2.1.6-6 i386 Python bindings for SELinux policy management
ii python-sepolgen 1.1.5-3 all Python module used in SELinux policy generation
ii python-setools 3.3.7-3 i386 SETools Python bindings
ii python-six 1.1.0-2 all Python 2 and 3 compatibility library (Python 2 interface)
ii python-soappy 0.12.0-4 all SOAP Support for Python
ii python-support 1.0.15 all automated rebuilding support for Python modules
ii python2.7 2.7.3-6+deb7u4 i386 Interactive high-level object-oriented language (version 2.7)
ii python2.7-minimal 2.7.3-6+deb7u4 i386 Minimal subset of the Python language (version 2.7)
ii readline-common 6.2+dfsg-0.1 all GNU readline and history libraries, common files
ii reportbug 6.4.4+deb7u2 all reports bugs in the Debian distribution
ii rpcbind 0.2.0-8+deb7u2 i386 converts RPC program numbers into universal addresses
ii rsyslog 5.8.11-3+deb7u2 i386 reliable system and kernel logging daemon
ii sed 4.2.1-10 i386 The GNU sed stream editor
ii selinux-policy-default 2:2.2010126-12 all Strict and Targeted variants of the SELinux policy
ii sensible-utils 0.0.7+deb7u1 all Utilities for sensible alternative selection
ii setools 3.3.7-3 i386 tools for Security Enhanced Linux policy analysis
ii sgml-base 1.26+nmu4 all SGML infrastructure and SGML catalog file support
ii shared-mime-info 1.0-1+b1 i386 FreeDesktop.org shared MIME database and spec
ii ssl-cert 1.0.32+deb7u1 all simple debconf wrapper for OpenSSL
ii sysv-rc 2.88dsf-41+deb7u1 all System-V-like runlevel change mechanism
ii sysvinit 2.88dsf-41+deb7u1 i386 System-V-like init utilities
ii sysvinit-utils 2.88dsf-41+deb7u1 i386 System-V-like utilities
ii tar 1.26+dfsg-0.1+deb7u1 i386 GNU version of the tar archiving utility
ii task-english 3.14.1 all General English environment
ii task-ssh-server 3.14.1 all SSH server
ii tasksel 3.14.1 all Tool for selecting tasks for installation on Debian systems
ii tasksel-data 3.14.1 all Official tasks used for installation of Debian systems

```

```

ii tcl 8.5.0-2.1 all The Tool Command Language (default version) - run-time files
ii tcl8.5 8.5.11-2 i386 Tcl (the Tool Command Language) v8.5 - run-time files
ii tcpcd 7.6.q-24 i386 Wietse Venema's TCP wrapper utilities
ii telnet 0.17-36 i386 The telnet client
ii texinfo 4.13a.dfsg.1-10 i386 Documentation system for on-line information and printed output
ii time 1.7-24 i386 GNU time program for measuring CPU resource usage
ii tk 8.5.0-2.1 all The Tk toolkit for Tcl and X11 (default version) - run-time files
ii tk8.5 8.5.11-2 i386 Tk toolkit for Tcl and X11, v8.5 - run-time files
ii traceroute 1:2.0.18-3 i386 Traces the route taken by packets over an IPv4/IPv6 network
ii ttf-dejavu-core 2.33-3 all Vera font family derivate with additional characters
ii tzdata 2018e-0+deb7u1 all time zone and daylight-saving time data
ii ucf 3.0025+nmu3 all Update Configuration File: preserve user changes to config files.
ii udev 175-7.2 i386 /dev/ and hotplug management daemon
ii ufwrau-batch 0.18-2 i386 batch importer for raw camera images
ii unzip 6.0-8+deb7u6 i386 De-archiver for .zip files
ii usbutils 1:005-3 i386 Linux USB utilities
ii util-linux 2.20.1-5.3 i386 Miscellaneous system utilities
ii util-linux-locales 2.20.1-5.3 all Locales files for util-linux
ii vim-common 2:7.3.547-7+deb7u4 i386 Vi IMproved - Common files
ii vim-tiny 2:7.3.547-7+deb7u4 i386 Vi IMproved - enhanced vi editor - compact version
ii virtualbox-guest-dkms 4.1.42-dfsg-1+deb7u1 all x86 virtualization solution - guest addition module source for dkms
ii virtualbox-guest-utils 4.1.42-dfsg-1+deb7u1 i386 x86 virtualization solution - non-X11 guest utilities
ii virtualbox-guest-x11 4.1.42-dfsg-1+deb7u1 i386 x86 virtualization solution - X11 guest utilities
ii virtualbox-ose-guest-x11 4.1.42-dfsg-1+deb7u1 all transitional package for virtualbox-guest-x11
ii w3m 0.5.3-8 i386 WWW browsable pager with excellent tables/frames support
ii wamerican 7.1-1 all American English dictionary words for /usr/share/dict
ii wget 1.13.4-3+deb7u6 i386 retrieves files from the web
ii whiptail 0.52.14-11.1 i386 Displays user-friendly dialog boxes from shell scripts
ii whois 5.1.1~deb7u1 i386 intelligent WHOIS client
ii x11-common 1:7.7+3~deb7u1 all X Window System (X.Org) infrastructure
ii x11-utils 7.7~1 i386 X11 utilities
ii x11-xkb-utils 7.7~1 i386 X11 XKB utilities
ii xauth 1:1.0.7-1 i386 X authentication utility
ii xbitmaps 1.1.1-1 all Base X bitmaps
ii xfonts-base 1:1.0.3 all standard fonts for X
ii xfonts-encodings 1:1.0.4-1 all Encodings for X.Org fonts
ii xfonts-utils 1:7.7~1 i386 X Window System font utility programs
ii xkb-data 2.5.1-3 all X Keyboard Extension (XKB) configuration data
ii xml-core 0.13+nmu2 all XML infrastructure and XML catalog file support
ii xserver-common 2:1.12.4-6+deb7u8 all common files used by various X servers
ii xserver-xorg-core 2:1.12.4-6+deb7u8 i386 Xorg X server - core server
ii xterm 278-4 i386 X terminal emulator
ii xz-utils 5.1.1alpha+20120614-2 i386 XZ-format compression utilities
ii zip 3.0-6 i386 Archiver for .zip files
ii zlib1g 1:1.2.7.dfsg-13 i386 compression library - runtime

```

## 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

## 110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege

### Synopsis

Nessus was able to log in to the remote host using the provided credentials. The provided credentials were not sufficient to complete all requested checks.

### Description

Nessus was able to execute credentialled checks because it was possible to log in to the remote host using provided credentials, however the credentials were not sufficiently privileged to complete all requested checks.

**Solution**

n/a

**Risk Factor**

None

**References**

XREF IAVB:0001-B-0502

**Plugin Information**

Published: 2018/06/06, Modified: 2024/03/25

**Plugin Output**

tcp/22/ssh

Nessus was able to log into the remote host, however this credential did not have sufficient privileges for all planned checks :

```
User: 'flag4'  
Port: 22  
Proto: SSH  
Method: password
```

See the output of the following plugin for details :

```
Plugin ID : 102094  
Plugin Name : SSH Commands Require Privilege Escalation
```

**141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided****Synopsis**

Valid credentials were provided for an available authentication protocol.

**Description**

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

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

**Plugin Information**

Published: 2020/10/15, Modified: 2024/03/25

**Plugin Output**

tcp/22/ssh

Nessus was able to log in to the remote host via the following :

User: 'flag4'  
Port: 22  
Proto: SSH  
Method: password

## 56468 - Time of Last System Startup

### Synopsis

The system has been started.

### Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

### Plugin Output

tcp/0

```
reboot system boot 3.2.0-6-486 Mon Oct 27 20:05 - 20:21 (00:15)
reboot system boot 3.2.0-6-486 Mon Oct 27 07:45 - 20:21 (12:35)
reboot system boot 3.2.0-6-486 Thu Feb 28 12:10 - 12:11 (00:01)
reboot system boot 3.2.0-6-486 Tue Feb 19 22:56 - 23:51 (00:55)
```

```
wtmp begins Tue Feb 19 22:56:17 2019
```

## 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 192.168.1.9 to 192.168.1.7 :
192.168.1.9
192.168.1.7
```

```
Hop Count: 1
```

## 192709 - Tukaani XZ Utils Installed (Linux / Unix)

### Synopsis

Tukaani XZ Utils is installed on the remote Linux / Unix host.

### Description

Tukaani XZ Utils is installed on the remote Linux / Unix host.

XZ Utils consists of several components, including:

- liblzma
- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.192709' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

## See Also

<https://xz.tukaani.org/xz-utils/>

## Solution

n/a

## Risk Factor

None

## Plugin Information

Published: 2024/03/29, Modified: 2025/07/28

## Plugin Output

tcp/0

Nessus detected 2 installs of XZ Utils:

```
Path : /usr/bin/xz
Version : 5.1.1
Associated Package : xz-utils 5.1.1alpha
Confidence : High
Managed by OS : True
Version Source : Package

Path : /lib/i386-linux-gnu/liblzma.so.5.0.0
Version : 5.1.1
Associated Package : liblzma5 5.1.1alpha
Confidence : High
Managed by OS : True
Version Source : Package
```

## 110483 - Unix / Linux Running Processes Information

### Synopsis

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

### Description

Generated report details the running processes on the target machine at scan time.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

### Solution

n/a

### Risk Factor

None

## Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

## Plugin Output

tcp/0

```

USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.1 0.0 2296 776 ? Ss 20:05 0:01 init [2]
root 2 0.0 0.0 0 0 ? S 20:05 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S 20:05 0:00 [ksoftirqd/0]
root 6 0.0 0.0 0 0 ? S 20:05 0:00 [watchdog/0]
root 7 0.0 0.0 0 0 ? S< 20:05 0:00 [cpuset]
root 8 0.0 0.0 0 0 ? S< 20:05 0:00 [khelper]
root 9 0.0 0.0 0 0 ? S 20:05 0:00 [kdevtmpfs]
root 10 0.0 0.0 0 0 ? S< 20:05 0:00 [netns]
root 11 0.0 0.0 0 0 ? S 20:05 0:00 [sync_supers]
root 12 0.0 0.0 0 0 ? S 20:05 0:00 [bdi-default]
root 13 0.0 0.0 0 0 ? S< 20:05 0:00 [kintegrityd]
root 14 0.0 0.0 0 0 ? S< 20:05 0:00 [kblockd]
root 15 0.0 0.0 0 0 ? S 20:05 0:00 [khungtaskd]
root 16 0.0 0.0 0 0 ? S 20:05 0:00 [kswapd0]
root 17 0.0 0.0 0 0 ? SN 20:05 0:00 [ksmd]
root 18 0.0 0.0 0 0 ? S 20:05 0:00 [fsnotify_mark]
root 19 0.0 0.0 0 0 ? S< 20:05 0:00 [crypto]
root 68 0.0 0.0 0 0 ? S< 20:05 0:00 [ata_sff]
root 75 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_0]
root 82 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_1]
root 110 0.0 0.0 0 0 ? S 20:05 0:00 [khubd]
root 135 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_2]
root 136 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_3]
root 137 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_4]
root 138 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_5]
root 139 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_6]
root 140 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_7]
root 141 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_8]
root 142 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_9]
root 143 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_10]
root 144 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_11]
root 145 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_12]
root 146 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_13]
root 147 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_14]
root 148 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_15]
root 149 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_16]
root 150 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_17]
root 151 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_18]
root 152 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_19]
root 153 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_20]
root 154 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_21]
root 155 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_22]
root 156 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_23]
root 157 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_24]
root 158 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_25]
root 159 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_26]
root 160 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_27]
root 161 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_28]
root 162 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_29]
root 163 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_30]
root 164 0.0 0.0 0 0 ? S 20:05 0:00 [scsi_eh_31]
root 192 0.0 0.0 0 0 ? S 20:05 0:00 [kworker/u:30]
root 193 0.0 0.0 0 0 ? S 20:05 0:00 [kworker/u:31]
root 283 0.0 0.0 0 0 ? S 20:05 0:00 [kworker/0:3]
root 310 0.0 0.0 0 0 ? S 20:05 0:00 [jbd2/sda1-8]
root 311 0.0 0.0 0 0 ? S< 20:05 0:00 [ext4-dio-unwrit]
root 460 0.0 0.1 2692 1252 ? Ss 20:05 0:00 udevd --daemon
root 551 0.0 0.0 0 0 ? S< 20:05 0:00 [ttm_swap]
root 612 0.0 0.0 2688 896 ? S 20:05 0:00 udevd --daemon
root 613 0.0 0.0 2688 900 ? S 20:05 0:00 udevd --daemon
root 643 0.0 0.0 0 0 ? S< 20:05 0:00 [kpsmoused]
root 1801 0.0 0.0 2400 948 ? Ss 20:05 0:00 /sbin/rpcbind -w
statd 1840 0.0 0.1 2704 1388 ? Ss 20:05 0:00 /sbin/rpc.statd
root 1848 0.0 0.0 0 0 ? S< 20:05 0:00 [rpcliod]
root 1850 0.0 0.0 0 0 ? S< 20:05 0:00 [nfsiod]
root 1857 0.0 0.0 2592 572 ? Ss 20:05 0:00 /usr/sbin/rpc.idmapd
root 1990 0.0 0.2 5196 2108 ? Ss 20:05 0:00 dhclient -v -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases eth0
root 2186 0.0 0.1 27900 1744 ? S1 20:05 0:00 /usr/sbin/rsyslogd -c5
root 2238 0.0 0.0 1892 608 ? Ss 20:05 0:00 /usr/sbin/acpid
root 2274 0.0 0.8 43680 8924 ? Ss 20:05 0:00 /usr/sbin/apache2 -k start
daemon 2300 0.0 0.0 2168 316 ? Ss 20:05 0:00 /usr/sbin/atd
www-data 2311 1.4 1.1 45900 11440 ? S 20:05 0:13 /usr/sbin/apache2 -k start
www-data 2312 1.5 1.2 45936 12528 ? S 20:05 0:14 /usr/sbin/apache2 -k start
www-data 2313 1.8 1.1 45892 11432 ? S 20:05 0:16 /usr/sbin/apache2 -k start
www-data 2314 1.5 1.4 49952 15504 ? S 20:05 0:13 /usr/sbin/apache2 -k start
www-data 2315 1.5 1.0 44884 10428 ? S 20:05 0:14 /usr/sbin/apache2 -k start
root 2348 0.0 0.0 3852 988 ? Ss 20:05 0:00 /usr/sbin/cron
103 2378 0.0 0.0 3032 652 ? Ss 20:05 0:00 /usr/bin/dbus-daemon --system
root 2444 0.0 0.1 6496 1092 ? Ss 20:05 0:00 /usr/sbin/shd
root 2454 0.0 0.0 1948 592 ? S 20:05 0:00 /bin/sh /usr/bin/mysqld_safe
root 2626 0.0 0.0 0 0 ? S 20:05 0:00 [flush:8:0]
mysql 2792 0.3 4.8 328548 49668 ? S1 20:05 0:03 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/mysql/plugin --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock --port=3306
root 2793 0.0 0.0 1868 600 ? S 20:05 0:00 logger -t mysqld -p daemon.error
101 3216 0.0 0.0 7420 988 ? Ss 20:06 0:00 /usr/sbin/exim4 -bd -q30m
root 3245 0.0 0.0 3796 840 tty2 Ss+ 20:06 0:00 /sbin/getty 38400 tty2
root 3246 0.0 0.0 3796 840 tty3 Ss+ 20:06 0:00 /sbin/getty 38400 tty3
root 3247 0.0 0.0 3796 844 tty4 Ss+ 20:06 0:00 /sbin/getty 38400 tty4
root 3248 0.0 0.0 3796 844 tty5 Ss+ 20:06 0:00 /sbin/getty 38400 tty5
root 3249 0.0 0.0 3796 844 tty6 Ss+ 20:06 0:00 /sbin/getty 38400 tty6
root 3263 0.0 0.0 0 0 ? S 20:11 0:00 [kworker/0:1]
root 3264 0.0 0.1 2856 1384 tty1 Ss 20:12 0:00 /bin/login --
flag4 3265 0.0 0.2 5520 2688 tty1 S+ 20:12 0:00 -bash
www-data 3352 5.8 1.0 45636 11132 ? S 20:17 0:13 /usr/sbin/apache2 -k start
www-data 3463 6.3 1.0 44868 10360 ? S 20:17 0:13 /usr/sbin/apache2 -k start
www-data 3467 6.2 1.0 44868 10408 ? S 20:18 0:11 /usr/sbin/apache2 -k start
www-data 3480 5.2 1.0 44868 10364 ? S 20:18 0:07 /usr/sbin/apache2 -k start

```

```

www-data 3482 4.1 1.6 51288 16584 ? S 20:19 0:05 /usr/sbin/apache2 -k start
root 3514 0.0 0.0 0 0 ? S 20:20 0:00 [kworker/0:0]
root 3853 0.0 0.2 9300 2956 ? Ss 20:21 0:00 sshd: flag4 [priv]
root 3854 0.0 0.2 9300 2964 ? Ss 20:21 0:00 sshd: flag4 [priv]
flag4 3860 0.0 0.1 9436 1804 ? S 20:21 0:00 sshd: flag4@notty
flag4 3861 0.0 0.1 9436 1844 ? S 20:21 0:00 sshd: flag4@notty
flag4 3863 0.0 0.1 4364 1280 ? Ss 20:21 0:00 bash -c /bin/ps auxww 2>/dev/null
flag4 3864 0.0 0.1 4360 1132 ? R 20:21 0:00 /bin/ps auxww

```

## 152742 - Unix Software Discovery Commands Available

### Synopsis

Nessus was able to log in to the remote host using the provided credentials and is able to execute all commands used to find unmanaged software.

### Description

Nessus was able to determine that it is possible for plugins to find and identify versions of software on the target host. Software that is not managed by the operating system is typically found and characterized using these commands. This was measured by running commands used by unmanaged software plugins and validating their output against expected results.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

### Plugin Output

tcp/0

Unix software discovery checks are available.

```

Account : flag4
Protocol : SSH

```

## 20094 - VMware Virtual Machine Detection

### Synopsis

The remote host is a VMware virtual machine.

### Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

### Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

### Risk Factor

None

### Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

### Plugin Output

tcp/0

The remote host is a VMware virtual machine.

## 189731 - Vim Installed (Linux)

### Synopsis

Vim is installed on the remote Linux host.

**Description**

Vim is installed on the remote Linux host.

**See Also**

<https://www.vim.org/>

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2024/01/29, Modified: 2025/07/28

**Plugin Output**

tcp/0

```
Path : /usr/bin/vim.tiny
Version : 7.3
```

**10302 - Web Server robots.txt Information Disclosure****Synopsis**

The remote web server contains a 'robots.txt' file.

**Description**

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

**See Also**

<http://www.robotstxt.org/orig.html>

**Solution**

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

**Risk Factor**

None

**Plugin Information**

Published: 1999/10/12, Modified: 2018/11/15

**Plugin Output**

tcp/80/www

Contents of robots.txt :

```
# 
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used: http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html
```

```
User-agent: *
Crawl-delay: 10
```

```

# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/

```

## 182848 - libcurl Installed (Linux / Unix)

### Synopsis

libcurl is installed on the remote Linux / Unix host.

### Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

### See Also

<https://curl.se/>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/10/10, Modified: 2025/07/28

### Plugin Output

tcp/0

```

Path : /usr/lib/i386-linux-gnu/libcurl.so.4.2.0
Version : 7.26.0
Associated Package : libcurl3 7.26.0-1
Managed by OS : True

```

## 204828 - libexiv2 Installed (Linux / Unix)

### Synopsis

libexiv2 is installed on the remote Linux / Unix host.

### Description

libexiv2 is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.204828' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

### See Also

<https://exiv2.org/>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/07/29, Modified: 2025/07/28

### Plugin Output

tcp/0

```
Path : /usr/lib/libexiv2.so.12.0.0
Version : 0.23
Associated Package : libexiv2-12 0.23-1
Managed by OS : True
```

© 2025 Tenable™, Inc. All rights reserved.