tenable Nessus

Report generated by Tenable Nessus™

HA-Hardy

Mon, 03 Nov 2025 09:27:39 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.1.5

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	1	0	1	12

Scan Information

Start time:	Mon Nov 3 09:25:17 2025
End time:	Mon Nov 3 09:27:39 2025

Host Information

IP:	192.168.1.5
MAC Address:	08:00:27:2A:35:8D

Vulnerabilities

207864 - CUPS cups-browsed Remote Unauthenticated Printer Registration (CVE-2024-47176) -

Synopsis

The remote web server is a CUPS server and responds to untrusted requests.

Description

The cups-browsed server running on the remote host trusts any well formatted packet received and responds to a potentially attacker controlled URL. A remote, unauthenticated attacker can exploit this vulnerability to solicit information and, combined with other CVEs, achieve RCE.

See Also

http://www.nessus.org/u?ebf4de66
http://www.nessus.org/u?03d62753

Solution

Upgrade to the latest available version or apply the recommended security patch per the vendor advisory.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2024-47176

Exploitable With

Metasploit (true)

Plugin Information

Published: 2024/09/27, Modified: 2025/07/14

Plugin Output

tcp/631

```
Nessus was able to exploit the vulnerability by sending a CUPS Browsing Protocol packet to the remote host.

The host then responded on the out of band port with:

POST /printers/PUGYob HTTP/1.1
Content-Length: 216
Content-Type: application/ipp
Date: Mon, 03 Nov 2025 09:26:53 GMT
Host: 192.168.1.29:39713
User-Agent: CUPS/2.2.7 (Linux 5.0.0-27-generic; x86_64) IPP/2.0
Expect: 100-continue

.
```

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 CVE-1999-0524

XREF CWE:200

Plugin Information

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

Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```

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

```
URL : http://192.168.1.5/
Version : 2.4.99
Source : Server: Apache/2.4.29 (Ubuntu)
backported : 1
os : ConvertedUbuntu
```

39521 - Backported Security Patch Detection (WWW) -

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80

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

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

```
Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.29 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
```

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 OUIs 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 :

08:00:27:2A:35:8D : PCS Systemtechnik GmbH
```

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:
- 08:00:27:2A:35:8D
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

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

Description

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

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

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

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

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

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80

```
Based on the response to an OPTIONS request :
- HTTP methods GET HEAD OPTIONS POST are allowed on :
/
```

10107 - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/80

```
The remote web server type is :
Apache/2.4.29 (Ubuntu)
```

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

```
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, 03 Nov 2025 09:26:35 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Mon, 09 Sep 2019 06:50:06 GMT
ETag: "2aa6-5921932b778f0"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
Modified from the Debian original for Ubuntu
Last updated: 2016-11-16
See: https://launchpad.net/bugs/1288690
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Ubuntu Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}

div.main_page {
position: relative;
display: table;

width: 800px;

margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding: 0px 0px 0px 0px;

border-width: 2px;
border-color: #212738;
border-style: solid;

background-color: #FFFFFF;

text-align: center;
}

div.page_header {
height: 99px;
width: 100%;

background-color: #F5F6F7;
}

div.page_header span {
margin: 15px 0px 0px 50px;

font-size: 180%;
font-weight: bold;
}

div.page_header img {
margin: 3px 0px 0px 40px;

border: 0px 0px 0px;
}

div.table_of_contents {
clear: left;

min-width: 200px;

margin: 3px 3px 3px 3px;
```

```
background-color: #FFFFFF;

text-align: left;
}

div.table_of_contents_item {
clear: left;

width: 100%;

margin: 4px 0px 0px 0px;

background-color: #FFFFFF;

color: #000000;
text-align: left;
}

div.table_of_contents_item a {
margin: 6px 0px 0px 6px;
}

div.content_section {
margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

div.content_section_text {
padding: 4px 8px 4px 8px;

color: #000000;
font-size: 100%;
}

div.content_section_text pre {
margin: 8px 0px 8px 0px;
padding: 8px 8px 8px 8px;

border-width: 1px;
border-style: dotted;
border-color: #000000;

background-color: #F5F6F7;

font-style: italic;
}

div.content_section_text p {
margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
padding: 4px 8px 4px 16px;
}

div.section_header {
padding: 3px 6px 3px 6px;

background-color: #8E9CB2;

color: #FFFFFF;
font-weight: bold;
font-size: 112%;
text-align: center;
}

div.section_header_red {
background-color: #CD214F;
}

div.section_header_grey {
background-color: #9F9386;
}

.floating_element {
position: relative;
float: left;
}

div.table_of_contents_item a,
div.content_section_text a {
text-decoration: none;
font-weight: bold;
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
color: #000000;
}

div.table_of_contents_item a:hover {
background-color: #000000;

color: #FFFFFF;
}
```

```
div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
background-color: #DCDFE6;

color: #000000;
}

div.content_section_text a:hover {
background-color: #000000;

color: #DCDFE6;
}

div.validator {
}
</style>
</head>
<body>
<div class="main_page">
<div class="page_header floating_element">
<img src="/icons/ubuntu-logo.png" alt="Ubuntu Logo" class="floating_element"/>
<span class="floating_element">
Apache2 Ubuntu Default Page
</span>
</div>
<!-- <div class="table_of_contents floating_element">
<div class="section_header section_header_grey">
TABLE OF CONTENTS
</div>
<div class="table_of_contents_item floating_element">
<a href="#about">About</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#changes">Changes</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#scope">Scope</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#files">Config files</a>
</div>
</div>
-->
<div class="content_section floating_element">


<div class="section_header section_header_red">
<div id="about"></div>
It works!
</div>
<div class="content_section_text">
<p>
This is the default welcome page used to test the correct
operation of the Apache2 server after installation on Ubuntu systems.
It is based on the equivalent page on Debian, from which the Ubuntu Apache
packaging is derived.
If you can read this page, it means that the Apache HTTP server installed at
this site is working properly. You should <b>replace this file</b> (located at
<tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
</p>


<p>
If you are a normal user of this web site and don't know what this page is
about, this probably means that the site is currently unavailable due to
maintenance.
If the problem persists, please contact the site's administrator.
</p>

</div>
<div class="section_header">
<div id="changes"></div>
Configuration Overview
</div>
<div class="content_section_text">
<p>
Ubuntu's Apache2 default configuration is different from the
upstream default configuration, and split into several files optimized for
interaction with Ubuntu tools. The configuration system is
<b>fully documented in
/usr/share/doc/apache2/README.Debian.gz</b>. Refer to this for the full
documentation. Documentation for the web server itself can be
found by accessing the <a href="/manual">manual</a> if the <tt>apache2-doc</tt>
package was installed on this server.

</p>
<p>
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
</p>
<pre>
/etc/apache2/
|-- apache2.conf
|  `-- ports.conf
|-- mods-enabled
|  |-- *.load
|  `-- *.conf
|-- conf-enabled
```

```
| `-- *.conf
|-- sites-enabled
| `-- *.conf
</pre>
<ul>
<li>
<tt>apache2.conf</tt> is the main configuration
file. It puts the pieces together by including all remaining configuration
files when starting up the web server.
</li>

<li>
<tt>ports.conf</tt> is always included from the
main configuration file. It is used to determine the listening ports for
incoming connections, and this file can be customized anytime.
</li>

<li>
Configuration files in the <tt>mods-enabled/</tt>,
<tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
particular configuration snippets which manage modules, global configuration
fragments, or virtual host configurations, respectively.
</li>

<li>
They are activated by symlinking available
configuration files from their respective
*-available/ counterparts. These should be managed
by using our helpers
<tt>
a2enmod,
a2dismod,
</tt>
<tt>
a2ensite,
a2dissite,
</tt>
and
<tt>
a2enconf,
a2disconf
</tt>. See their respective man pages for detailed information.
</li>

<li>
The binary is called apache2. Due to the use of
environment variables, in the default configuration, apache2 needs to be
started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
<b>Calling <tt>/usr/bin/apache2</tt> directly will not work</b> with the
default configuration.
</li>
</ul>
</div>

<div class="section_header">
<div id="docroot"></div>
Document Roots
</div>

<div class="content_section_text">
<p>
By default, Ubuntu does not allow access through the web browser to
<em>any</em> file apart of those located in <tt>/var/www</tt>,
<a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="nofollow">public_html</a>
directories (when enabled) and <tt>/usr/share</tt> (for web
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
document root directory in <tt>/etc/apache2/apache2.conf</tt>.
</p>
<p>
The default Ubuntu document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www. This is different
to previous releases which provides better security out of the box.
</p>
</div>

<div class="section_header">
<div id="bugs"></div>
Reporting Problems
</div>
<div class="content_section_text">
<p>
Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
Apache2 package with Ubuntu. However, check <a
href="https://bugs.launchpad.net/ubuntu/+source/apache2"
rel="nofollow">existing bug reports</a> before reporting a new bug.
</p>
<p>
Please report bugs specific to modules (such as PHP and others)
to respective packages, not to the web server itself.
</p>
</div>




</div>
</div>
<div class="validator">
```

```
</div>
</body>
</html>
```

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 : HA-Hardy
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.29
Port scanner(s) : nessus_syn_scanner
Port range : 65535
Ping RTT : 137.859 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 : 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 : 2025/11/3 9:25 UTC
```

```
Scan duration : 136 sec
Scan for malware : no
```

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 192.168.1.29 to 192.168.1.5 :
192.168.1.29
192.168.1.5

Hop Count: 1
```

135860 - WMI Not Available -

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2025/07/21

Plugin Output

tcp/445

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

66717 - mDNS Detection (Local Network) -

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

```
Nessus was able to extract the following information :

- mDNS hostname : ubuntu.local.
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations