



**jango**

---

Report generated by Tenable Nessus™

Mon, 30 Sep 2024 17:27:19 EDT

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.50.158.....	4
-----------------------	---

Nessus Essentials

---

## **Vulnerabilities by Host**

---

192.168.50.158



#### Scan Information

Start time: Mon Sep 30 17:19:33 2024

End time: Mon Sep 30 17:27:19 2024

#### Host Information

IP: 192.168.50.158

MAC Address: 08:00:27:2A:5D:12

OS: Linux Kernel 4.4 on Ubuntu 16.04 (xenial), Linux Kernel 2.6 on Ubuntu 16.10 (yakkety)

#### Vulnerabilities

##### 10704 - Apache Multiviews Arbitrary Directory Listing

#### Synopsis

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

#### Description

The Apache web server running on the remote host is affected by an information disclosure vulnerability. An unauthenticated, remote attacker can exploit this, by sending a crafted request, to display a listing of a remote directory, even if a valid index file exists in the directory.

For Apache web server later than 1.3.22, review listing directory configuration to avoid disclosing sensitive information

#### See Also

<http://www.nessus.org/u?f39e976b>

<http://www.nessus.org/u?a96611bc>

<http://www.nessus.org/u?c1c382bc>

#### Solution

Upgrade to Apache version 1.3.22 or later. Alternatively, as a workaround, disable Multiviews.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

2.2

## EPSS Score

0.9652

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

BID	3009
CVE	CVE-2001-0731
XREF	OWASP:OWASP-CM-004
XREF	EDB-ID:21002

## Plugin Information

Published: 2016/02/16, Modified: 2020/10/21

## Plugin Output

tcp/80/www

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

http://192.168.50.158/?M=A

This produced the following truncated output (limited to 10 lines) :

----- snip -----

192.168.50.158

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of </title>
</head>
<body>
<h1>Index of </h1>
<table>
<tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr>
[...]
```

----- snip -----

## 18261 - Apache Banner Linux Distribution Disclosure

### Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

### Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

### Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

```
The Linux distribution detected was :  
- Ubuntu 16.04 (xenial)  
- Ubuntu 16.10 (yakkety)
```

## 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://192.168.50.158/
Version  : 2.4.99
Source   : Server: Apache/2.4.18 (Ubuntu)
backported : 1
os       : ConvertedUbuntu
```



## 39519 - Backported Security Patch Detection (FTP)

### Synopsis

Security patches are backported.

### Description

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

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

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

### See Also

[https://access.redhat.com/security/updates/backporting/?sc\\_cid=3093](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/21/ftp

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

## 39521 - Backported Security Patch Detection (WWW)

### Synopsis

Security patches are backported.

### Description

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

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

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

### See Also

[https://access.redhat.com/security/updates/backporting/?sc\\_cid=3093](https://access.redhat.com/security/updates/backporting/?sc_cid=3093)

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/80/www

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

## 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: 2024/09/03

### Plugin Output

tcp/0

The remote operating system matched the following CPE's :

```
cpe:/o:canonical:ubuntu_linux:16.04 -> Canonical Ubuntu Linux  
cpe:/o:canonical:ubuntu_linux:16.10 -> Canonical Ubuntu Linux
```

Following application CPE's matched on the remote system :

```
cpe:/a:apache:http_server:2.4.18 -> Apache Software Foundation Apache HTTP Server  
cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
```

## 54615 - Device Type

### Synopsis

It is possible to guess the remote device type.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 85
```

## 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:5D:12 : 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: 2020/05/13

### Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 08:00:27:2A:5D:12
```

## 10092 - FTP Server Detection

### Synopsis

An FTP server is listening on a remote port.

### Description

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

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0030

XREF IAVT:0001-T-0943

### Plugin Information

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

### Plugin Output

tcp/21/ftp

```
The remote FTP banner is :
```

```
220 (vsFTPd 3.0.3)
```

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/80/www



Based on the response to an OPTIONS request :

- HTTP methods 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/www

```
The remote web server type is :  
Apache/2.4.18 (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/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, 30 Sep 2024 23:23:20 GMT

Server: Apache/2.4.18 (Ubuntu)

Vary: Accept-Encoding

Content-Length: 746

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

<html>

<head>

<title>Index of </title>

</head>

<body>

<h1>Index of </h1>

```

<table>
  <tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
  <tr><th colspan="5"><hr></th></tr>
  <tr><td valign="top"></td><td><a href="site/">site/</a></td><td align="right">2021-06-10 18:05 </td><td align="right"> - </td><td>&nbsp;</td></tr>
  <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.18 (Ubuntu) Server at 192.168.50.158 Port 80</address>
</body></html>

```

### Synopsis

---

It is possible to determine which TCP ports are open.

### Description

---

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

---

Protect your target with an IP filter.

### Risk Factor

---

None

### Plugin Information

---

Published: 2009/02/04, Modified: 2024/05/20

### Plugin Output

---

tcp/21/ftp

```
Port 21/tcp was found to be open
```

### Synopsis

---

It is possible to determine which TCP ports are open.

### Description

---

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

---

Protect your target with an IP filter.

### Risk Factor

---

None

### Plugin Information

---

Published: 2009/02/04, Modified: 2024/05/20

### Plugin Output

---

tcp/80/www

```
Port 80/tcp was found to be open
```

## 19506 - Nessus Scan Information

### Synopsis

This plugin displays information about the Nessus scan.

### Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2024/08/05

### Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.8.2
Nessus build : 20007
Plugin feed version : 202409300116
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : jango
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.50.100
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 179.119 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 : no
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 : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/9/30 17:19 EDT
Scan duration : 454 sec
Scan for malware : no
```



## 11936 - OS Identification

### Synopsis

It is possible to guess the remote operating system.

### Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2003/12/09, Modified: 2024/06/19

### Plugin Output

tcp/0

```
Remote operating system : Ubuntu 16.x
Confidence level : 85
Method : HTTP
```

Not all fingerprints could give a match. If you think some or all of the following could be used to identify the host's operating system, please email them to [os-signatures@nessus.org](mailto:os-signatures@nessus.org). Be sure to include a brief description of the host itself, such as the actual operating system or product / model names.

SinFP!!:

```
P1:B10113:F0x12:W29200:00204ffff:M1460:
P2:B10113:F0x12:W28960:00204ffff0402080afffffff4445414401030307:M1460:
P3:B00000:F0x00:W0:00:M0
P4:191002_7_p=80
```

The remote host is running Ubuntu 16.x

## 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/21/ftp

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

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/80/www

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

## 25220 - TCP/IP Timestamps Supported

### Synopsis

---

The remote service implements TCP timestamps.

### Description

---

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

### See Also

---

<http://www.ietf.org/rfc/rfc1323.txt>

### Solution

---

n/a

### Risk Factor

---

None

### Plugin Information

---

Published: 2007/05/16, Modified: 2023/10/17

### Plugin Output

---

tcp/0

## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

### Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.50.100 to 192.168.50.158 :  
192.168.50.100  
192.168.50.158
```

```
Hop Count: 1
```

## 52703 - vsftpd Detection

### Synopsis

An FTP server is listening on the remote port.

### Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

### See Also

<http://vsftpd.beasts.org/>

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/03/17, Modified: 2019/11/22

### Plugin Output

tcp/21/ftp

```
Source  : 220 (vsFTPd 3.0.3)
Version : 3.0.3
```