tenable Nessus

Report generated by Tenable Nessus™

Sky - Tower

Thu, 06 Nov 2025 08:02:37 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.1.18

0	0	1	1	19
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Nov 6 08:00:02 2025
End time:	Thu Nov 6 08:02:37 2025

Host Information

IP:	192.168.1.18
MAC Address:	08:00:27:54:4A:37
OS:	Linux Kernel 3.2 on Debian 7.0 (wheezy), Debian unstable (sid), Debian testing (wheezy)

Vulnerabilities

88098 - Apache Server ETag Header Information Disclosure -

Synopsis

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

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	6939
CVE	CVE-2003-1418
XREF	CWE:200

Plugin Information

Published: 2016/01/22, Modified: 2025/02/11

Plugin Output

tcp/80

```
Nessus was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

Source : ETag: "57-470-4fc42b97adc0a"
Inode number : 87
File size : 1136 bytes
File modification time : Jun. 20, 2014 at 11:23:36 GMT
```

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 difference between the local and remote clocks is 13 seconds.
```

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)
```

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://192.168.1.18/
Version : 2.2.99
```

```
Source : Server: Apache/2.2.22 (Debian)
backported : 1
os : ConvertedDebian
```

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:2.2.22 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:http_server:2.2.99 -> Apache Software Foundation Apache HTTP Server
cpe:/a:squid-cache:squid:3.1.20 -> squid-cache.org Squid
```

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 : 45
```

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 :

08:00:27:54:4A:37 : 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:
- 08:00:27:54:4A:37
```

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 :

/
```

10192 - HTTP Proxy CONNECT Request Relaying -

Synopsis

An HTTP proxy running on the remote host can be used to establish interactive sessions.

Description

The proxy allows users to perform CONNECT requests such as :

CONNECT http://cvs.example.org:23

This request gives the person who made it the ability to have an interactive session with a third-party site.

This issue may allow attackers to bypass your firewall by connecting to sensitive ports such as 23 (telnet) via the proxy, or it may allow internal users to bypass the firewall rules and connect to ports or sites they should not be allowed to.

In addition, your proxy may be used to perform attacks against other networks.

Solution

Reconfigure your proxy to refuse CONNECT requests.

Risk Factor

None

Plugin Information

Published: 1999/06/22, Modified: 2016/04/27

Plugin Output

tcp/3128/http_proxy

10195 - HTTP Proxy Open Relay Detection -

Synopsis

The remote web proxy server accepts requests.

Description

The remote web proxy accepts unauthenticated HTTP requests from the Nessus scanner. By routing requests through the affected proxy, a user may be able to gain some degree of anonymity while browsing websites, which will see requests as originating from the remote host itself rather than the user's host.

Solution

Make sure access to the proxy is limited to valid users / hosts.

Risk Factor

None

Plugin Information

Published: 1999/06/22, Modified: 2014/04/25

Plugin Output

tcp/3128/http_proxy

11305 - HTTP Proxy Open gopher:// Request Relaying -

Synopsis

The HTTP proxy accepts gopher:// requests.

Description

Gopher is an old network protocol which predates HTTP and is nearly unused today. As a result, gopher-compatible software is generally less audited and more likely to contain security bugs than others.

By making gopher requests, an attacker may evade your firewall settings, by making connections to port 70, or may even exploit arcane flaws in this protocol to gain more privileges on this host.

Solution

Reconfigure your proxy so that it refuses gopher requests.

Risk Factor

None

Plugin Information

Published: 2003/03/02, Modified: 2020/01/02

Plugin Output

tcp/3128/http_proxy

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/2.2.22 (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

```
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: Thu, 06 Nov 2025 08:01:18 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Fri, 20 Jun 2014 11:23:36 GMT
ETag: "57-470-4fc42b97adc0a"
Accept-Ranges: bytes
Content-Length: 1136
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :

<html>
<body>

<div style="height:100%; width:100%;background-image:url('background.jpg');
background-size:100%;
background-position:50% 50%;
background-repeat:no-repeat;">
<div style="
background-color:white;
border-color: #000000;
border-width: 5px;
border-style: solid;
width: 300px;
height:180px;
position:absolute;
top:50%;
left:50%;
margin-top:-100px; /* this is half the height of your div*/
margin-left:-100px;
">
<form style="margin: 0 auto;width:250px;" action='login.php' method='POST'>
<br><strong>Skytech Login:</strong><br><br>
<label for="email" style="display: inline-block; width: 90px;" >E-mail:</label>
<input name="email" type="text" size=15 ><br><br>
<label for="password" style="display: inline-block; width: 90px;">Password:</label>
<input name="password" type="password" size=15><br><br>
<input type="submit" value="Login">
</form>
</div>

</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 : Sky - Tower
Scan policy used : Advanced Scan
Scanner IP : 192.168.1.28
Port scanner(s) : nessus_syn_scanner
Port range : 65535
Ping RTT : 147.390 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 : 2025/11/6 8:00 UTC
Scan duration : 146 sec
Scan for malware : no
```

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 : 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
```

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 on Debian 7.0 (wheezy)
Debian unstable (sid)
Debian testing (wheezy)
Confidence level : 45
Method : HTTP


The remote host is running one of these operating systems :
Linux Kernel 3.2 on Debian 7.0 (wheezy)
Debian unstable (sid)
Debian testing (wheezy)
```

49692 - Squid Proxy Version Detection -

Synopsis

It was possible to obtain the version number of the remote Squid proxy server.

Description

The remote host is running the Squid proxy server, an open source proxy server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/09/28, Modified: 2024/06/17

Plugin Output

tcp/8080

```
URL : http://192.168.1.18:3128/
Version : 3.1.20
Source : Server: squid/3.1.20
```

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 192.168.1.28 to 192.168.1.18 :
192.168.1.28
192.168.1.18

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.
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

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

Remediations

Suggested Remediations