macOS Vulnerability Scan

Report generated by Tenable Nessus™ Thu, 26 Jun 2025 18:40:34 IST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

127.0.0.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	3	3	1	100

Scan Information

Start time: Thu Jun 26 18:23:02 2025

End time: Thu Jun 26 18:40:33 2025

Host Information

DNS Name: dhvanils-Laptop.local

Netbios Name: dhvanils-Laptop

IP: 127.0.0.1

MAC Address: BA:71:4F:65:90:25 52:4F:27:4C:D5:99 36:D7:8B:6A:5D:84 52:4F:27:4C:D5:79 D2:90:A7:ED:A1:1E 36:D7:8B:6A:5D:80 5E:2B:5E:4E:1C:62 52:4F:27:4C:D5:78 52:4F:27:4C:D5:98

OS: macOS 15.5

Vulnerabilities

240340 - Google Chrome < 138.0.7204.49 Multiple Vulnerabilities

Synopsis

A web browser installed on the remote macOS host is affected by multiple vulnerabilities.

Description

The version of Google Chrome installed on the remote macOS host is prior to 138.0.7204.49. It is, therefore, affected by multiple vulnerabilities as referenced in the 2025_06_stable-channel-update-for-desktop_24 advisory.

- Use after free in Animation. (CVE-2025-6555)

- Insufficient policy enforcement in Loader. (CVE-2025-6556)

- Insufficient data validation in DevTools. (CVE-2025-6557)

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?1f24c7f6
https://crbug.com/407328533
https://crbug.com/40062462
https://crbug.com/406631048

Solution

Upgrade to Google Chrome version 138.0.7204.49 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.3

EPSS Score

0.0009

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2025-6555
CVE	CVE-2025-6556
CVE	CVE-2025-6557

Plugin Information

Published: 2025/06/24, Modified: 2025/06/24

Plugin Output

tcp/0

```
Path              : /Applications/Google Chrome.app
Installed version : 137.0.7151.120
Fixed version     : 138.0.7204.49
```

234620 - Cisco Webex App Client-Side RCE (cisco-sa-webex-app-client-rce-ufyMMYLC)

Synopsis

The remote device is missing a vendor-supplied security patch.

Description

According to its self-reported version, Cisco Webex App Client-Side Remote Code Execution is affected by a vulnerability.

- A vulnerability in the custom URL parser of Cisco Webex App could allow an unauthenticated, remote attacker to persuade a user to download arbitrary files, which could allow the attacker to execute arbitrary commands on the host of the targeted user. This vulnerability is due to insufficient input validation when Cisco Webex App processes a meeting invite link. An attacker could exploit this vulnerability by persuading a user to click a crafted meeting invite link and download arbitrary files. A successful exploit could allow the attacker to execute arbitrary commands with the privileges of the targeted user. (CVE-2025-20236)

Please see the included Cisco BIDs and Cisco Security Advisory for more information.

See Also

http://www.nessus.org/u?86e02dfc

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwn07296

Solution

Upgrade to the relevant fixed version referenced in Cisco bug ID CSCwn07296

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.001

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-20236
XREF	CISCO-BUG-ID:CSCwn07296
XREF	CISCO-SA:cisco-sa-webex-app-client-rce-ufyMMYLC
XREF	IAVA:2025-A-0287
XREF	CWE:829

Plugin Information

Published: 2025/04/18, Modified: 2025/04/18

Plugin Output

tcp/0

```
  Path              : /Users/dhvanil/Library/Application Support/Cisco Spark/
Webexteams_upgrades_arm/44.7.0.30285_a3b68316-d2b7-42ed-bd01-dec566f68663/Webex.app
  Installed version : 44.7.0.30285
  Fixed version     : 44.8
```

234547 - Oracle VM VirtualBox (April 2025 CPU)

Synopsis

The remote host is affected by multiple vulnerabilities

Description

The 7.1.6 versions of VM VirtualBox installed on the remote host are affected by multiple vulnerabilities as referenced in the April 2025 CPU advisory.

- Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data as well as unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox.

(CVE-2025-30712)

- Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. (CVE-2025-30719)

- Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.1.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. (CVE-2025-30725)

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://www.oracle.com/docs/tech/security-alerts/cpuapr2025csaf.json

https://www.oracle.com/security-alerts/cpuapr2025.html

Solution

Apply the appropriate patch according to the April 2025 Oracle Critical Patch Update advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.3

EPSS Score

0.0001

CVSS v2.0 Base Score

6.2 (CVSS2#AV:L/AC:L/Au:M/C:C/I:C/A:P)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-30712
CVE	CVE-2025-30719
CVE	CVE-2025-30725
XREF	IAVA:2025-A-0275

Plugin Information

Published: 2025/04/17, Modified: 2025/04/17

Plugin Output

tcp/0

```
Path              : /Applications/VirtualBox.app
Installed version : 7.1.6
Fixed version     : 7.1.8
```

216141 - Security Update for Microsoft Visual Studio Code (February 2025)

Synopsis

The remote host has an application installed that is missing a security update.

Description

The version of Microsoft Visual Studio Code installed on the remote host is prior to 1.97.1. It is, therefore, affected by multiple vulnerabilities:

- An elevation of privilege vulnerability exists in VS Code 1.97.0 and earlier versions for users of the code serve-web command on Windows. An attacker can place an evil version of the node module that is optionally required by one of the dependencies for the Visual Studio Code remote server in a world writable directory like C:

ode_modules to get it executed under the privileges of the current user. (CVE-2025-24039)

- A vulnerability exists in VS Code 1.97.0 and earlier versions where an attacker with write permissions on certain common directories can place a binary that would be executed automatically by the JavaScript debugger. This requires an attacker to be able to create and modify files on the user's machine. (CVE-2025-24042)

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

See Also

https://code.visualstudio.com/updates/v1_97

https://github.com/microsoft/vscode/issues/240406

https://github.com/microsoft/vscode/issues/240407

Solution

Upgrade to Microsoft Visual Studio Code 1.97.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0008

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-24039
CVE	CVE-2025-24042
XREF	IAVA:2025-A-0108-S

Plugin Information

Published: 2025/02/11, Modified: 2025/06/23

Plugin Output

tcp/0

```
Path              : /Users/dhvanil/Downloads/Visual Studio Code.app
Installed version : 1.96.4
Fixed version     : 1.97.1
```

235122 - Docker Desktop < 4.41.0 Access Control

Synopsis

The remote host has an application installed that is affected by an access control vulnerability.

Description

The version of Docker Desktop for Mac is prior to 4.41.0. It is therefore affected by an access control vulnerability.

Registry Access Management (RAM) is a security feature allowing administrators to restrict access for their developers to only allowed registries. When a MacOS configuration profile is used to enforce organization sign-in, the RAM policies are not being applied, which would allow Docker Desktop users to pull down unapproved, and potentially malicious images from any registry.

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

See Also

https://docs.docker.com/desktop/release-notes/#4411

Solution

Upgrade to Docker Desktop version 4.41.0 or later

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.2

EPSS Score

0.0001

CVSS v2.0 Base Score

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

References

CVE	CVE-2025-4095

XREF CWE:862

Plugin Information

Published: 2025/05/05, Modified: 2025/05/05

Plugin Output

tcp/0

```
Path              : /Applications/Docker.app
Installed version : 4.40.0
Fixed version     : 4.41.0
```

235123 - Docker Desktop < 4.41.0 Information Disclosure Vulnerability

Synopsis

The remote host has an application installed that is affected by an information disclosure vulnerability.

Description

The version of Docker Desktop for Linux is prior to 4.41.0. It is therefore affected by an information disclosure vulnerability.

The Recording of environment variables, configured for running containers, in Docker Desktop application logs could lead to unintentional disclosure of sensitive information such as api keys, passwords, etc. A malicious actor with read access to these logs could obtain sensitive credentials information and further use it to gain unauthorized access to other systems. Starting with version 4.41.0, Docker Desktop no longer logs environment variables set by the user.

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

Solution

Upgrade to Docker Desktop version 4.41.0 or later

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

3.6

EPSS Score

0.0002

CVSS v2.0 Base Score

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

References

CVE	CVE-2025-3911

Plugin Information

Published: 2025/05/05, Modified: 2025/05/05

Plugin Output

tcp/0

```
Path              : /Applications/Docker.app
Installed version : 4.40.0
Fixed version     : 4.41.0
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2025/06/16

Plugin Output

tcp/8834/www

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

|-Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=dhvanils-Laptop.local
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus
 Certification Authority
```

234134 - IntelliJ IDEA < 2024.2.4 / 2024.3 (macOS)

Synopsis

The remote host is missing a security update.

Description

The version of IntelliJ IDEA installed on the remote host is prior to 2024.2.4, 2024.3. It is, therefore, affected by a vulnerability as referenced in the advisory.

- In JetBrains IntelliJ IDEA before 2024.3, 2024.2.4 source code could be logged in the idea.log file (CVE-2025-32054)

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

See Also

https://www.jetbrains.com/privacy-security/issues-fixed/

Solution

Upgrade to IntelliJ IDEA version 2024.2.4, 2024.3 or later.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2025-32054
XREF	IAVA:2025-A-0226-S

Plugin Information

Published: 2025/04/10, Modified: 2025/05/22

Plugin Output

tcp/0

```
Path              : /Applications/IntelliJ IDEA CE.app
Installed version : 2024.1.1
Fixed version     : 2024.2.4, 2024.3
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

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

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - dhvanils-laptop.local
```

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: 2025/06/16

Plugin Output

tcp/0

```
Path               : /usr/sbin/httpd
Version            : 2.4.62
Associated Package : macOS system file
Managed by OS      : True
Running            : no

Configs found :

Loaded modules :
```

125406 - Apple Safari Installed (macOS)

Synopsis

A web browser is installed on the remote macOS or Mac OS X host.

Description

Apple Safari, a web browser, is installed on the remote macOS or Mac OS X host.

See Also

https://www.apple.com/safari/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/05/28, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path              : /Applications/Safari.app
Version           : 18.5
Detailed Version : 20621.2.5.11.8
```

61412 - Apple Xcode IDE Detection (Mac OS X)

Synopsis

The remote host has an integrated development environment installed.

Description

The remote Mac OS X host has Apple Xcode installed. Xcode is a development environment for creating applications that will run on Apple products.

See Also

https://developer.apple.com/xcode/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/08/03, Modified: 2023/11/27

Plugin Output

tcp/0

```
Path    : /Applications/Xcode.app/Contents/Developer
Version : 16.4
```

197858 - Aqua Security Trivy Installed (Linux / Unix)

Synopsis

Aqua Security Trivy is installed on the remote Linux / Unix host.

Description

Aqua Security Trivy 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.197858' 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://trivy.dev/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/05/23, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path          : trivy 0.61.0 (homebrew managed) (via package manager)
Version       : 0.61.0
Managed by OS : True
```

234619 - Cisco Webex App Installed (macOS)

Synopsis

Cisco Webex App is installed on the remote macOS host.

Description

Cisco Webex App is installed on the remote macOS host.

See Also

https://www.webex.com/downloads.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/04/18, Modified: 2025/04/18

Plugin Output

tcp/0

```
Nessus detected 4 installs of Webex App:

  Path    : /Users/dhvanil/Library/Application Support/WebEx Folder/Add-ons/Cisco WebEx Start.app
  Version : 15.43.0800

  Path    : /Users/dhvanil/Library/Application Support/Cisco Spark/
Webexteams_upgrades_arm/44.7.0.30285_a3b68316-d2b7-42ed-bd01-dec566f68663/Webex.app
  Version : 44.7.0.30285

  Path    : /Users/dhvanil/Library/Application Support/Cisco Spark/
Webexteams_upgrades_arm/44.8.0.30404_1910f9f6-f0ee-45a9-a23c-14085b7f2e35/Webex.app
  Version : 44.8.0.30404

  Path    : /Users/dhvanil/Library/Application Support/Cisco Spark/
Webexteams_upgrades_arm/45.5.0.32411_b3d2483b-0bfa-448c-85ea-2c5c6f53da55/Webex.app
  Version : 45.5.0.32411
```

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: 2025/04/15

Plugin Output

tcp/0

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

  cpe:/o:apple:mac_os_x:15.5 -> Apple Mac OS X

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.62 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apple:safari:18.5 -> Apple Safari
  cpe:/a:apple:xcode:16.4 -> Apple Xcode Tools
  cpe:/a:docker:docker:4.40.0 -> Docker
  cpe:/a:fortinet:forticlient:7.4.2.1717 -> Fortinet Forticlient for Linux Kernel
  cpe:/a:google:chrome:137.0.7151.120 -> Google Chrome
  cpe:/a:haxx:curl:8.13.0 -> Haxx Curl
  cpe:/a:jetbrains:intellij_idea:2024.1.1 -> JetBrains IntelliJ IDEA
  cpe:/a:microsoft:autoupdate:4.79.25033028 -> Microsoft AutoUpdate for MacOS
  cpe:/a:microsoft:powershell:7.4.6 -> Microsoft PowerShell
  cpe:/a:oracle:vm_virtualbox:7.1.6 -> Oracle VM VirtualBox
  cpe:/a:ruby-lang:ruby:2.6.10 -> Ruby-lang Ruby
```

```
  cpe:/a:tenable:nessus -> Tenable Nessus
  cpe:/a:tenable:nessus:10.8.4 -> Tenable Nessus
  cpe:/a:wireshark:wireshark:4.4.2 -> Wireshark
  cpe:/a:zoom:zoom_cloud_meetings:6.4.12_%2856699%29 -> ZOOM Cloud Meetings (aka
us.zoom.videomeetings) for Android
  x-cpe:/a:apple:xprotect:5302
  x-cpe:/a:aqua_security:trivy:0.61.0
  x-cpe:/a:cisco:webex_app:15.43.0800
  x-cpe:/a:cisco:webex_app:44.7.0.30285
  x-cpe:/a:cisco:webex_app:44.8.0.30404
  x-cpe:/a:cisco:webex_app:45.5.0.32411
  x-cpe:/a:microsoft:visual_studio_code:1.96.4
```

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: 2025/06/16

Plugin Output

tcp/0

```
Path          : curl 8.13.0 (homebrew managed) (via package manager)
Version       : 8.13.0
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: 2025/06/23

Plugin Output

tcp/0

```
Hostname : dhvanils-Laptop.local
  dhvanils-Laptop (LocalHostName)
  dhvanils-Laptop.local (hostname command)
  dhvanil's Laptop (ComputerName)
```

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
```

180577 - Docker Installed (macOS)

Synopsis

Docker is installed on the remote macOS host.

Description

Docker is installed on the remote macOS host.

See Also

https://www.docker.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/07, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path    : /Applications/Docker.app
Version : 4.40.0
```

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 :

 - 127.0.0.1 (on interface lo0)
 - 192.168.29.91 (on interface en0)
```

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 :

 - ::1 (on interface lo0)
 - fe80::1 (on interface lo0)
 - fe80::66f7:8d43:7e1:3370 (on interface utun0)
 - fe80::19db:fd80:764f:ab20 (on interface utun1)
 - fe80::107e:2337:bfa5:7116 (on interface en0)
 - 2405:201:2031:708c:1820:19:7a74:fe60 (on interface en0)
 - 2405:201:2031:708c:49d8:291:7851:537b (on interface en0)
 - fe80::b871:4fff:fe65:9025 (on interface awdl0)
 - fe80::b871:4fff:fe65:9025 (on interface llw0)
 - fe80::f64d:1bdf:8ce1:ec31 (on interface utun2)
 - fe80::ce81:b1c:bd2c:69e (on interface utun3)
 - fe80::b66b:9963:40ae:14e5 (on interface utun4)
 - fe80::8fee:b68a:731d:9b60 (on interface utun5)
```

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 addresses exist on the remote host :

  - ba:71:4f:65:90:25 (interfaces awdl0 & llw0)
  - 52:4f:27:4c:d5:99 (interface anpi1)
  - 36:d7:8b:6a:5d:84 (interface en2)
  - 52:4f:27:4c:d5:79 (interface en4)
  - d2:90:a7:ed:a1:1e (interface ap1)
  - 36:d7:8b:6a:5d:80 (interfaces en1 & bridge0)
  - 5e:2b:5e:4e:1c:62 (interface en0)
  - 52:4f:27:4c:d5:78 (interface en3)
  - 52:4f:27:4c:d5:98 (interface anpi0)
```

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

```
utun0:
  IPv6:
    - Address : fe80::66f7:8d43:7e1:3370
        Prefixlen : 64
        Scope : utun0
        ScopeID : 0xd
lo0:
  IPv4:
    - Address : 127.0.0.1
        Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
        Prefixlen : 128
    - Address : fe80::1
        Prefixlen : 64
        Scope : lo0
        ScopeID : 0x1
utun2:
  IPv6:
    - Address : fe80::f64d:1bdf:8ce1:ec31
        Prefixlen : 64
        Scope : utun2
        ScopeID : 0x11
en0:
  MAC : 5e:2b:5e:4e:1c:62
  Status :  active
  IPv4:
    - Address : 192.168.29.91
        Netmask : 255.255.255.0
        Broadcast : 192.168.29.255
  IPv6:
    - Address : fe80::107e:2337:bfa5:7116
```

```
        Prefixlen : 64
        Scope : en0
        ScopeID : 0xb
    - Address : 2405:201:2031:708c:1820:19:7a74:fe60
        Prefixlen : 64
    - Address : 2405:201:2031:708c:49d8:291:7851:537b
        Prefixlen : 64
en2:
  MAC : 36:d7:8b:6a:5d:84
  Status :  inactive
anpi1:
  MAC : 52:4f:27:4c:d5:99
  Status :  inactive
stf0:
anpi0:
  MAC : 52:4f:27:4c:d5:98
  Status :  inactive
en3:
  MAC : 52:4f:27:4c:d5:78
  Status :  inactive
utun3:
  IPv6:
    - Address : fe80::ce81:b1c:bd2c:69e
        Prefixlen : 64
        Scope : utun3
        ScopeID : 0x12
utun1:
  IPv6:
    - Address : fe80::19db:fd80:764f:ab20
        Prefixlen : 64
        Scope : utun1
        ScopeID : 0xe
en1:
  MAC : 36:d7:8b:6a:5d:80
  Status :  inactive
utun5:
  IPv6:
    - Address : fe80::8fee:b68a:731d:9b60
        Prefixlen : 64
        Scope : utun5
        ScopeID : 0x14
llw0:
  MAC : ba:71:4f:65:90:25
  Status :  inactive
  IPv6:
    - Address : fe80::b871:4fff:fe65:9025
        Prefixlen : 64
        Scope : llw0
        ScopeID : 0x10
ap1:
  MAC : d2:90:a7:ed:a1:1e
  Status :  inactive
utun4:
  IPv6:
    - Address : fe80::b66b:9963:40ae:14e5
        Prefixlen : 64
        Scope : utun4
        ScopeID : 0x13
awdl0:
  MAC : ba:71:4f:65:90:25
  Status :  active
  IPv6:
    - Address : fe80::b871:4fff:fe65:9025
        Prefixlen : 64
        Scope : awdl0
        ScopeID : 0xf
gif0:
en4:
  [...]
```

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:
  en0:
    ipv4_gateways:
      192.168.29.1:
        subnets:
         - 0.0.0.0/0
    ipv6_gateways:
      fe80::f2ed:b8ff:fe35:c62a%en0:
        subnets:
         - ::/0
  utun0:
    ipv6_gateways:
      fe80::%utun0:
        subnets:
         - ::/0
  utun1:
    ipv6_gateways:
      fe80::%utun1:
        subnets:
         - ::/0
  utun2:
    ipv6_gateways:
      fe80::%utun2:
        subnets:
         - ::/0
  utun3:
    ipv6_gateways:
      fe80::%utun3:
        subnets:
         - ::/0
  utun4:
    ipv6_gateways:
```

```
      fe80::%utun4:
        subnets:
         - ::/0
  utun5:
    ipv6_gateways:
      fe80::%utun5:
        subnets:
         - ::/0
Interface Routes:
  en0:
    ipv4_subnets:
     - 169.254.0.0/16
     - 192.168.29.0/24
    ipv6_subnets:
     - 2405:201:2031:708c::/64
     - fe80::/64
  lo0:
    ipv4_subnets:
     - 127.0.0.0/8
    ipv6_subnets:
     - fe80::/64
  utun0:
    ipv6_subnets:
     - fe80::/64
  utun1:
    ipv6_subnets:
     - fe80::/64
  utun2:
    ipv6_subnets:
     - fe80::/64
  utun3:
    ipv6_subnets:
     - fe80::/64
  utun4:
    ipv6_subnets:
     - fe80::/64
  utun5:
    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: 2025/06/23

Plugin Output

tcp/0

```
Nessus has enumerated the path of the current scan user :

/usr/bin
/bin
/usr/sbin
/sbin
```

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:
  - BA:71:4F:65:90:25
  - 52:4F:27:4C:D5:99
  - 36:D7:8B:6A:5D:84
  - 52:4F:27:4C:D5:79
  - D2:90:A7:ED:A1:1E
  - 36:D7:8B:6A:5D:80
  - 5E:2B:5E:4E:1C:62
  - 52:4F:27:4C:D5:78
  - 52:4F:27:4C:D5:98
```

109279 - FileVault Detection (Mac OS X)

Synopsis

Obtains Mac OS X FileVault encryption status.

Description

Nessus was able to determine the Mac OS X FileVault encryption status on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/04/23, Modified: 2025/06/16

Plugin Output

tcp/0

```
Nessus was able to determine that FileVault is enabled on this host.
```

95259 - Fortinet FortiClient Detection (macOS)

Synopsis

An endpoint protection application is installed on the remote host.

Description

Fortinet FortiClient, an endpoint protection application, is installed on the remote macOS or Mac OS X host.

See Also

https://www.forticlient.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/11/22, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path    : /Applications/FortiClient.app/Contents/MacOS/
Version : 7.4.2.1717
```

133180 - Google Chrome Browser Extension Enumeration (macOS)

Synopsis

One or more Chrome browser extensions are installed on the remote host.

Description

Nessus was able to enumerate Chrome browser extensions installed on the remote macOS host.

See Also

https://chrome.google.com/webstore/category/extensions

Solution

Make sure that the use and configuration of these extensions comply with your organization's acceptable use and security policies.

NOTE: This plugins will enumerate Chrome extensions for all users if credentials with elevated privileges are supplied.

Risk Factor

None

Plugin Information

Published: 2020/01/23, Modified: 2025/06/23

Plugin Output

tcp/0

```
User : dhvanil
|- Browser : Chrome
  |- Add-on information :

    Name        : GoFullPage - Full Page Screen Capture
    Description : __MSG_appDesc__
    Version     : 8.5
    Path        : /Users/dhvanil/Library/Application Support/Google/Chrome/Default/Extensions/
fdpohaocaechifimbbbbbknoalclacl/8.5_0/

    Name        : __MSG_extensionName__
    Description : __MSG_disable__
    Version     : 9.2
    Path        : /Users/dhvanil/Library/Application Support/Google/Chrome/Default/Extensions/
gcknhkkoolaabfmlnjonogaaifnjlfnp/9.2_0/

    Name        : __MSG_extName__
    Description : __MSG_extDesc__
    Version     : 1.92.1
```

```
    Path        : /Users/dhvanil/Library/Application Support/Google/Chrome/Default/Extensions/
ghbmnnjooekpmoecnnnilnnbdlolhkhi/1.92.1_0/

    Name        : Wappalyzer - Technology profiler
    Description : Identify web technologies
    Version     : 6.10.83
    Path        : /Users/dhvanil/Library/Application Support/Google/Chrome/Default/Extensions/
gppongmhjkpfnbhagpmjfkannfbllamg/6.10.83_0/

    Name        : __MSG_extension_name__
    Description : forward
    Version     : 2.20.0
    Path        : /Users/dhvanil/Library/Application Support/Google/Chrome/Default/Extensions/
hdhinadidafjejdhmfkjgnolgimiaplp/2.20.0_0/

    Name        : daily.dev | The homepage developers deserve
    Description : Get one personalized feed for all the knowledge you need as a developer.
    Version     : 3.37.3
    Path        : /Users/dhvanil/Library/Application Support/Google/Chrome/Default/Extensions/
jlmpjdjjbgclbocgajdjefcidcncaied/3.37.3_0/

    Name        : InCognito
    Description : Browse LinkedIn Privately. Instantly view profiles anonymously with the flip of a
 switch in your navigation bar.
    Version     : 2.0.0
    Path        : /Users/dhvanil/Library/Application Support/Google/Chrome/Default/Extensions/
kencjkgapindpgehbgolojoocgpcepfk/2.0.0_0/

    Name        : Gifs autoplay for Google™
    Description : Autoplays gifs on Google™ Search Images.
    Version     : 2.3.1
    Path        : /U [...]
```

70890 - Google Chrome Installed (Mac OS X)

Synopsis

The remote Mac OS X host contains an alternative web browser.

Description

Google Chrome is installed on the remote Mac OS X host.

See Also

https://www.google.com/chrome/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0511

Plugin Information

Published: 2013/11/13, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path    : /Applications/Google Chrome.app
Version : 137.0.7151.120
```

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/5000/www

```
The remote web server type is :

AirTunes/860.7.1
```

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/7000/www

```
The remote web server type is :

AirTunes/860.7.1
```

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/8834/www

```
The remote web server type is :

NessusWWW
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2025/03/13

Plugin Output

tcp/0

```
127.0.0.1 resolves as localhost.
```

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/5000/www

```
Response Code : HTTP/1.1 403 Forbidden

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

  Content-Length: 0
  Server: AirTunes/860.7.1
  X-Apple-ProcessingTime: 0
  X-Apple-RequestReceivedTimestamp: 54975789

Response Body :
```

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/7000/www

```
Response Code : HTTP/1.1 403 Forbidden

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

  Content-Length: 0
  Server: AirTunes/860.7.1
  X-Apple-ProcessingTime: 0
  X-Apple-RequestReceivedTimestamp: 54983854

Response Body :
```

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/8834/www

```
Response Code : HTTP/1.1 200 OK

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

  Cache-Control: must-revalidate
  X-Frame-Options: DENY
  Content-Type: text/html
  ETag: 648f9856fb742fd1ad80a4e90e544995
  Connection: close
  X-XSS-Protection: 1; mode=block
  Server: NessusWWW
  Date: Thu, 26 Jun 2025 12:55:37 GMT
  X-Content-Type-Options: nosniff
  Content-Length: 1217
  Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; form-action 'self';
 frame-ancestors 'none'; frame-src https://store.tenable.com; default-src 'self'; connect-src
 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data:; style-src 'self'
 www.tenable.com; object-src 'none'; base-uri 'self';
  Strict-Transport-Security: max-age=31536000; includeSubDomains
  Expect-CT: max-age=0
```

```
Response Body :

<!doctype html>
<html lang="en">
    <head>
        <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
        <meta http-equiv="Content-Security-Policy" content="upgrade-insecure-requests; block-all-
mixed-content; form-action 'self'; frame-src https://store.tenable.com; default-src 'self'; connect-
src 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data:; style-src
 'self' www.tenable.com; object-src 'none'; base-uri 'self';" />
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <meta charset="utf-8" />
        <title>Nessus</title>
        <link rel="stylesheet" href="nessus6.css?v=1744138425399" id="theme-link" />
        <link rel="stylesheet" href="tenable_links.css?v=ac05d80f1e3731b79d12103cdf9367fc" />
        <link rel="stylesheet" href="wizard_templates.css?v=0e2ae10949ed6782467b3810ccce69c5" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <script src="nessus6.js?v=1744138425399"></script>
        <script src="p [...]
```

189236 - JetBrains IntelliJ IDEA Installed (macOS)

Synopsis

JetBrains IntelliJ IDEA is installed on the remote macOS or Mac OS X host.

Description

JetBrains IntelliJ IDEA is installed on the remote macOS or Mac OS X host.

See Also

https://www.jetbrains.com/idea/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/19, Modified: 2025/03/11

Plugin Output

tcp/0

```
Path    : /Applications/IntelliJ IDEA CE.app
Version : 2024.1.1
```

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: IST +0530
Via /etc/localtime: IST-5:30
```

83991 - List Installed Mac OS X Software

Synopsis

This plugin gathers information about all managed / packaged software installed on the remote Mac OS X host.

Description

This plugin gathers information about all managed / packaged software installed on the remote Mac OS X host.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0503

Plugin Information

Published: 2015/06/04, Modified: 2025/06/16

Plugin Output

tcp/0

```
System Profiler managed applications:

50onPaletteServer [version 1.1.0]
  Location: /System/Library/Input Methods/50onPaletteServer.app

ABAssistantService [version 14.0]
  Location: /System/Library/Frameworks/AddressBook.framework/Versions/A/Helpers/
ABAssistantService.app

About This Mac [version 1.0]
  Location: /System/Library/CoreServices/Applications/About This Mac.app

Accessibility Inspector [version 5.0]
  Location: /Applications/Xcode.app/Contents/Applications/Accessibility Inspector.app

Accessibility Tutorial [version 1.0]
  Location: /System/Library/PrivateFrameworks/UniversalAccess.framework/Versions/A/Resources/
Accessibility Tutorial.app

AccessibilityVisualsAgent [version 1.0]
  Location: /System/Library/PrivateFrameworks/AccessibilitySupport.framework/Versions/A/Resources/
AccessibilityVisualsAgent.app
```

```
Activity Monitor [version 10.14]
  Location: /System/Applications/Utilities/Activity Monitor.app

AddPrinter [version 607]
  Location: /System/Library/CoreServices/AddPrinter.app

AddressBookManager [version 14.0]
  Location: /System/Library/Frameworks/AddressBook.framework/Versions/A/Helpers/
AddressBookManager.app

AddressBookSourceSync [version 14.0]
  Location: /System/Library/Frameworks/AddressBook.framework/Versions/A/Helpers/
AddressBookSourceSync.app

AddressBookSync [version 14.0]
  Location: /System/Library/Frameworks/AddressBook.framework/Helpers/AddressBookSync.app

AddressBookUrlForwarder [version 14.0]
  Location: /System/Library/CoreServices/AddressBookUrlForwarder.app

AinuIM [version 1.0]
  Location: /System/Library/Input Methods/AinuIM.app

AirDrop [version 15.5]
  Location: /System/Library/CoreServices/Finder.app/Contents/Applications/AirDrop.app

AirPlayUIAgent [version 2.0]
  Location: /System/Library/CoreServices/AirPlayUIAgent.app

AirPort Base Station Agent [version 2.2.1]
  Location: /System/Library/CoreServices/AirPort Base Station Agent.app

AirPort Utility [version 6.3.9]
  Location: /System/Applications/Utilities/AirPort Utility.app

AirScanLegacyDiscovery [version 607]
   [...]
```

60019 - Mac OS X Admin Group User List

Synopsis

There is at least one user in the 'Admin' group.

Description

Using the supplied credentials, Nessus was able to extract the member list of the 'Admin' and 'Wheel' groups. Members of these groups have administrative access to the remote system.

Solution

Verify that each member of the group should have this type of access.

Risk Factor

None

Plugin Information

Published: 2012/07/18, Modified: 2023/11/27

Plugin Output

tcp/0

```
The following users are members of the 'Admin' group :
  - root
  - dhvanil

The following user is a member of the 'Wheel' group :
  - root
```

58180 - Mac OS X DNS Server Enumeration

Synopsis

Nessus enumerated the DNS servers being used by the remote Mac OS X host.

Description

Nessus was able to enumerate the DNS servers configured on the remote Mac OS X host by looking in /etc/resolv.conf.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/03/01, Modified: 2023/11/27

Plugin Output

tcp/0

```
Nessus found the following nameservers configured in /etc/resolv.conf :

1.1.1.1
```

56567 - Mac OS X XProtect Detection

Synopsis

The remote Mac OS X host has an antivirus application installed on it.

Description

The remote Mac OS X host includes XProtect, an antivirus / anti- malware application from Apple included with recent releases of Snow Leopard (10.6) and later. It is used to scan files that have been downloaded from the Internet by browsers and other tools.

Note that this plugin only gathers information about the application and does not, by itself, perform any security checks or issue a report.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/20, Modified: 2023/11/27

Plugin Output

tcp/0

```
Path    : /Library/Apple/System/Library/CoreServices/XProtect.bundle
Version : 5302
```

187860 - MacOS NetBIOS Identity Information

Synopsis

Detects NetBIOS identity for macOS systems

Description

Detects NetBIOS identity for macOS systems

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/10, Modified: 2025/06/16

Plugin Output

tcp/0

```
NetBIOSName       : dhvanils-Laptop
ServerDescription : dhvanil's Laptop
DOSCodePage       : 437
```

233957 - Microsoft AutoUpdate Installed (macOS)

Synopsis

Microsoft AutoUpdate is installed on the remote macOS host.

Description

Microsoft AutoUpdate is installed on the remote macOS host.

See Also

https://rustdesk.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/04/07, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path    : /Library/Application Support/Microsoft/MAU2.0/Microsoft AutoUpdate.app
Version : 4.79.25033028
```

186477 - Microsoft PowerShell Installed (macOS)

Synopsis

Microsoft PowerShell is installed on the remote macOS or Mac OS X host.

Description

Microsoft PowerShell is installed on the remote macOS or Mac OS X host.

See Also

https://learn.microsoft.com/en-us/powershell/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/11/30, Modified: 2025/03/11

Plugin Output

tcp/0

```
Path    : /Applications/PowerShell.app
Version : 7.4.6
```

129055 - Microsoft Visual Studio Code Installed (Mac OS X)

Synopsis

A code editor is installed on the remote host.

Description

Microsoft Visual Studio Code is installed on the remote Mac OS X host.

See Also

https://code.visualstudio.com/

https://code.visualstudio.com/#alt-downloads

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/09/19, Modified: 2025/03/11

Plugin Output

tcp/0

```
Path    : /Users/dhvanil/Downloads/Visual Studio Code.app
Version : 1.96.4
```

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 : 10.8.4
Nessus build : 20028
Plugin feed version : 202506260211
Scanner edition used : Nessus Home
Scanner OS : DARWIN
Scanner distribution : macosx
Scan type : Normal
Scan name : macOS Vulnerability Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 127.0.0.1
Ping RTT : Unavailable
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 (on the localhost)
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 : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/6/26 18:23 IST (UTC +05:30)
Scan duration : 1051 sec
Scan for malware : no
```

10147 - Nessus Server Detection

Synopsis

A Nessus daemon is listening on the remote port.

Description

A Nessus daemon is listening on the remote port.

See Also

https://www.tenable.com/products/nessus/nessus-professional

Solution

Ensure that the remote Nessus installation has been authorized.

Risk Factor

None

References

XREF	IAVT:0001-T-0673

Plugin Information

Published: 1999/10/12, Modified: 2023/02/08

Plugin Output

tcp/8834/www

```
URL     : https://localhost:8834/
Version : unknown
```

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

udp/137

```
Port 137/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/138

```
Port 138/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/3722

```
Port 3722/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/5000/www

```
Port 5000/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/5353/mdns

```
Port 5353/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/7000/www

```
Port 7000/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/8834/www

```
Port 8834/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/50383

```
Port 50383/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/54703

```
Port 54703/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/57661

```
Port 57661/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/61741

```
Port 61741/udp 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 : Mac OS X 15.5
Confidence level : 100
Method : uname
Type : general-purpose
Fingerprint : uname:Darwin dhvanils-Laptop.local 24.5.0 Darwin Kernel Version 24.5.0: Tue Apr 22
 19:54:33 PDT 2025; root:xnu-11417.121.6~2/RELEASE_ARM64_T8122 arm64


Following fingerprints could not be used to determine OS :
 HTTP:!:Server: AirTunes/860.7.1

SSLcert:!:i/CN:Nessus Certification Authorityi/O:Nessus Users Unitedi/OU:Nessus Certification
 Authoritys/CN:dhvanils-Laptop.locals/O:Nessus Users Uniteds/OU:Nessus Server
ecc248a6aa2aaf70075bd0147c2768b062d9433e
```

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 : Mac OS X 15.5
Confidence level : 100
Method : uname


The remote host is running Mac OS X 15.5
```

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

```
Nessus can run commands on localhost to check if patches are applied.

The output of "uname -a" is :
Darwin dhvanils-Laptop.local 24.5.0 Darwin Kernel Version 24.5.0: Tue Apr 22 19:54:33 PDT 2025;
 root:xnu-11417.121.6~2/RELEASE_ARM64_T8122 arm64

Local checks have been enabled for this host.
The remote macOS or Mac OS X system is :
Mac OS X 15.5

OS Security Patch Assessment is available for this host.
Runtime : 1.283334 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.

Protocol : LOCAL
```

84240 - Oracle VM VirtualBox Installed (Mac OS X)

Synopsis

A virtualization platform is installed on the remote host.

Description

Oracle VM VirtualBox, a virtualization platform, is installed on the remote Mac OS X host.

See Also

https://www.virtualbox.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0696

Plugin Information

Published: 2015/06/17, Modified: 2025/03/11

Plugin Output

tcp/0

```
Path    : /Applications/VirtualBox.app
Version : 7.1.6
```

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: 2025/06/10

Plugin Output

tcp/0

```
. You need to take the following 7 actions :

[ Cisco Webex App Client-Side RCE (cisco-sa-webex-app-client-rce-ufyMMYLC) (234620) ]
+ Action to take : Upgrade to the relevant fixed version referenced in Cisco bug ID CSCwn07296

[ Docker Desktop < 4.41.0 Access Control (235122) ]
+ Action to take : Upgrade to Docker Desktop version 4.41.0 or later

[ Docker Desktop < 4.41.0 Information Disclosure Vulnerability (235123) ]
+ Action to take : Upgrade to Docker Desktop version 4.41.0 or later

[ Google Chrome < 138.0.7204.49 Multiple Vulnerabilities (240340) ]
+ Action to take : Upgrade to Google Chrome version 138.0.7204.49 or later.
+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

```
[ IntelliJ IDEA < 2024.2.4 / 2024.3 (macOS) (234134) ]

+ Action to take : Upgrade to IntelliJ IDEA version 2024.2.4, 2024.3 or later.


[ Oracle VM VirtualBox (April 2025 CPU) (234547) ]

+ Action to take : Apply the appropriate patch according to the April 2025 Oracle Critical Patch
 Update advisory.


[ Security Update for Microsoft Visual Studio Code (February 2025) (216141) ]

+ Action to take : Upgrade to Microsoft Visual Studio Code 1.97.1 or later.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

45405 - Reachable IPv6 address

Synopsis

The remote host may be reachable from the Internet.

Description

Although this host was scanned through a private IPv4 or local scope IPv6 address, some network interfaces are configured with global scope IPv6 addresses. Depending on the configuration of the firewalls and routers, this host may be reachable from Internet.

Solution

Disable IPv6 if you do not actually using it.

Otherwise, disable any unused IPv6 interfaces and implement IP filtering if needed.

Risk Factor

None

Plugin Information

Published: 2010/04/02, Modified: 2024/07/24

Plugin Output

tcp/0

```
The following global addresss were gathered :

  - 2405:201:2031:708c:49d8:291:7851:537b
  - 2405:201:2031:708c:1820:19:7a74:fe60
```

191144 - Ruby Programming Language Installed (macOS)

Synopsis

The Ruby programming language is installed on the remote macOS host.

Description

The Ruby programming language is installed on the remote macOS host.

See Also

https://ruby.org/en/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/02/29, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path    : /usr/bin/ruby
Version : 2.6.10
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/8834/www

```
This port supports TLSv1.3/TLSv1.2.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/8834/www

```
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: dhvanils-Laptop.local

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 5A D4

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jun 26 12:13:31 2025 GMT
Not Valid After: Jun 25 12:13:31 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 9B B9 A4 60 E0 62 6A 59 C1 1F 90 A4 3B FA DE 95 76 58 63
```

```
             20 7D 8A BC A0 30 C4 A3 00 D8 1D F1 8B 95 3F 67 2D F3 46 02
             35 B4 D4 3B 58 58 1D BD 12 0A DF D0 D8 48 3D 77 AC 67 91 AC
             51 6A 22 1A FB 6E 06 B7 04 9D 74 39 36 D1 20 88 E3 02 E5 12
             C6 DE CE 9D E0 EF EE 62 17 3F D5 3C 59 87 16 C4 C5 11 28 8F
             86 07 22 3F 18 C2 16 17 45 DE 4E 8C CC 19 AA 0F 7D CE 27 6B
             A4 F2 5E F3 F3 45 F4 26 DD 3C 54 E2 17 40 0A 0B 6D 8D 85 D4
             75 8E 8C 2F C0 22 95 72 9C 42 E2 D4 EB 43 2A 23 06 78 C2 B1
             4D 2A 68 C3 C1 43 54 BD 57 B4 0F 5C 16 35 54 1B 0F A8 81 CA
             46 5E FF A6 B1 65 E2 96 BD 34 47 2F C5 03 CB 94 77 E6 DE C4
             A1 05 5C EC FC 39 0F AE CD BF 94 60 AA 72 70 24 57 6C EF C7
             EE D4 A0 F9 9B 2F 80 56 E3 44 80 7B 08 B4 9D D7 E4 FE 54 02
             DB 27 47 34 52 0F D4 A0 E8 4C DF AF 3C E1 46 08 EF
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 80 3C 1D CB ED F6 EC B1 2C 0A 51 E3 37 53 8D 69 C7 CD 0F
           E1 23 83 C6 09 9D 9D DD 53 35 B8 23 08 76 FD 95 3B 8E 2F A7
           03 97 59 AB 67 06 B8 04 30 CF E4 1D 3F 4D 1C 0D 60 81 99 55
           50 05 13 07 71 BC B7 2F 4C 0D EA AC 50 E1 DC E4 29 DD 28 60
           36 27 E0 41 40 F3 69 4B A8 F3 54 A3 AB 22 26 F4 F0 2A E0 F4
           6A 2E A9 E0 67 E5 CF C7 79 35 D6 C8 B3 EF 06 07 1A 6D E3 73
           1A 9 [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/8834/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
```

```
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/8834/www

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
    Encrypt={symmetric encryption method}
    MAC={message authentication code}
    {export flag}
```

131568 - Serial Number Identification (macOS)

Synopsis

Detects the serial number of the remote macOS host.

Description

The Serial Number was detected on the remote macOS host.

See Also

https://support.apple.com/en-us/HT201581

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/12/03, Modified: 2025/06/23

Plugin Output

tcp/0

```
Serial Number : L34XD37H7H
```

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/5000/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/7000/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8834/www

```
A TLSv1.2 server answered on this port.
```

tcp/8834/www

```
A web server is running on this port through TLSv1.2.
```

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 Mac OS X system :

  MRT 1.93
  Stumble Guys 0.87.5
  Brave Browser 137.1.79.126
  Burp Suite Community Edition 2025.5.4
  ProtonVPN 5.0.0
  UTM 4.5.4
  PowerShell 7.4.6
  ida-free-pc_90_armmac 9.0
  IDA Free 9 9.0.241217
  Visual Studio Code 1.96.4
  Visual Studio Code 2 1.97.0
  Android Studio 2024.3
  VirtualBox 7.1.6
  Docker 4.40.0
  MKPlayer 1.6.2
  Spotify 1.2.58.498
  Google Chrome 137.0.7151.120
  The Unarchiver 4.3.9
  IntelliJ IDEA CE 2024.1.1
  Wireshark 4.4.2
```

```
FortiClient 7.4.2.1717
FortiClientUninstaller 1.2
Genymotion 3.8.0
Genymotion Shell 3.8.0
maintenancetool 4.5.2
Apache NetBeans 24
manager-osx 1.0
uninstall 3.0
Xcode 16.4
Simulator 16.0
Create ML 6.2
Instruments 16.4
FileMerge 2.11
Reality Composer Pro 2.0
Accessibility Inspector 5.0
Webex 15.43.0800
Webex 44.7.0.30285
Webex 44.8.0.30404
Python 3.9.6
Microsoft AutoUpdate 4.79
Webex 45.5.0.32411
XProtect 151
Recursive File Processing Droplet 1.0
Droplet with Settable Properties 1.0
Recursive Image File Processing Droplet 1.0
Cocoa-AppleScript Applet 1.0
AppleMobileDeviceHelper 5.0
MobileDeviceUpdater 1.0
AppleMobileSync 5.0
AirScanLegacyDiscovery 607
CleanMyMac_5_Updater 0.0.1
GoogleUpdater 138.0.7194.0
Microsoft Teams 25151.505.3727.5755
Keychain Access 11.0
Ticket Viewer 4.1
Wireless Diagnostics 11.0
iOS App Installer 1.0
Finder 15.5
AirDrop 15.5
Computer 15.5
Network 15.5
Recents 15.5
iCloud Drive 15.5
Photos 10.0
Podcasts 1.1.0
Preview 11.0
QuickTime Player 10.5
Reminders 7.0
Shortcuts 7.0
Siri 1.0
Stickies 10.3
Stocks 7.3
System Settings 15.0
TV 1.5.5
TextEdit 1.20
Time Machine 1.3
Tips 15.5
Activity Monitor 10.14
AirPort Utility 6.3.9
Audio MIDI Setup 3.6
Bluetooth File Exchange 9.0
Boot Camp Assistant 6.1.0
ColorSync Utility 12.1.0
Console 1.1
Digital Colour Meter 5.26
Disk Utility 22.7
Grapher 2.7
Migration Assistant 15.5
Print Centre 1.0
```

```
   Screen Sh [...]
```

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

http://www.nessus.org/u?2fb3aca6

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/16, Modified: 2019/11/22

Plugin Output

tcp/8834/www

```
The STS header line is :

Strict-Transport-Security: max-age=31536000; includeSubDomains
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/8834/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/8834/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

110095 - Target Credential Issues by Authentication Protocol - No Issues Found

Synopsis

Nessus was able to log in to the remote host using the provided credentials. No issues were reported with access, privilege, or intermittent failure.

Description

Valid credentials were provided for an authentication protocol on the remote target and Nessus did not log any subsequent errors or failures for the authentication protocol.

When possible, Nessus tracks errors or failures related to otherwise valid credentials in order to highlight issues that may result in incomplete scan results or limited scan coverage. The types of issues that are tracked include errors that indicate that the account used for scanning did not have sufficient permissions for a particular check, intermittent protocol failures which are unexpected after the protocol has been negotiated successfully earlier in the scan, and intermittent authentication failures which are unexpected after a credential set has been accepted as valid earlier in the scan. This plugin reports when none of the above issues have been logged during the course of the scan for at least one authenticated protocol. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for issues to be encountered for one protocol and not another.

For example, authentication to the SSH service on the remote target may have consistently succeeded with no privilege errors encountered, while connections to the SMB service on the remote target may have failed intermittently.

- Resolving logged issues for all available authentication protocols may improve scan coverage, but the value of resolving each issue for a particular protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol and what particular check failed. For example, consistently successful checks via SSH are more critical for Linux targets than for Windows targets, and likewise consistently successful checks via SMB are more critical for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0520

Plugin Information

Published: 2018/05/24, Modified: 2024/03/25

Plugin Output

tcp/0

```
Nessus was able to execute commands locally with sufficient privileges
for all planned checks.
```

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/0

```
Nessus was able to execute commands on localhost.
```

163326 - Tenable Nessus Installed (Linux)

Synopsis

Tenable Nessus is installed on the remote Linux host.

Description

Tenable Nessus is installed on the remote Linux host.

See Also

https://www.tenable.com/products/nessus

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/07/21, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path    : /opt/nessus
Version : 10.8.4
Build   : 20028
```

168392 - Tenable Nessus Installed (macOS)

Synopsis

Tenable Nessus is installed on the remote macOS host.

Description

Tenable Nessus is installed on the remote macOS host.

See Also

https://www.tenable.com/products/nessus

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/12/05, Modified: 2025/06/16

Plugin Output

tcp/0

```
Path           : /Library/Nessus/run/sbin/nessusd
Version        : 10.8.4
Build          : 20028
Version Source : /Library/Nessus/run/var/nessus/nessus.version
```

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 time                                 Tue Jun 24 17:00
reboot time                                 Wed May 28 05:52
shutdown time                               Wed May 28 02:24
reboot time                                 Sun May 11 13:54
shutdown time                               Sun May 11 13:53
reboot time                                 Tue Apr 22 02:03
shutdown time                               Tue Apr 22 02:02
reboot time                                 Sun Apr 20 14:14
shutdown time                               Sun Apr 20 04:10
reboot time                                 Thu Apr 10 14:25
shutdown time                               Thu Apr 10 14:21
reboot time                                 Sun Mar 16 03:54
shutdown time                               Sun Mar 16 03:52
reboot time                                 Thu Feb 27 15:45
shutdown time                               Thu Feb 27 15:45
reboot time                                 Thu Feb 27 15:44
reboot time                                 Tue Feb 11 02:07
shutdown time                               Tue Feb 11 02:05
reboot time                                 Fri Jan 31 01:25
reboot time                                 Mon Jan 20 14:59
shutdown time                               Mon Jan 20 14:59
reboot time                                 Mon Dec  9 20:19
shutdown time                               Mon Dec  9 20:19
reboot time                                 Mon Dec  2 17:15
shutdown time                               Mon Dec  2 17:14
reboot time                                 Sat Nov 30 00:39
shutdown time                               Sat Nov 30 00:36
reboot time                                 Wed Nov 27 18:06
shutdown time                               Wed Nov 27 18:06
reboot time                                 Wed Nov 27 14:49
reboot time                                 Thu Nov 21 15:59
```

```
    shutdown time                               Thu Nov 21 15:59
    reboot time                                 Wed Nov 20 13:10
     [...]
```

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   TT  STAT STARTED      TIME COMMAND
root              8215  38.8  1.1 414925344 186240   ??  S     5:55PM  61:48.64 nessusd -q
root              8505  26.7  0.2 411219552  36496   ??  S     6:28PM   0:00.20 /usr/sbin/
system_profiler -nospawn -xml SPApplicationsDataType -detailLevel full
root               340  17.8  0.1 427003328  21008   ??  Ss    Tue05PM   5:08.69 /System/Library/
Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Support/mds
_windowserver      382  15.5  0.6 412968336 100368   ??  Ss    Tue05PM 123:29.17 /System/Library/
PrivateFrameworks/SkyLight.framework/Resources/WindowServer -daemon
dhvanil           8260  14.2  6.1 414856960 1018448   ??  S     6:02PM  14:50.17 /Applications/
VirtualBox.app/Contents/Resources/VirtualBoxVM.app/Contents/MacOS/VirtualBoxVM --comment kali --
startvm 043d409c-7f72-4a48-802e-87a4b7b499c9 --no-startvm-errormsgbox
root               505   8.4  0.6 439895664  94448   ??  Ss    Tue05PM   6:23.19 /System/Library/
Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Versions/A/Support/mds_stores
dhvanil            862   7.5  2.4 478778176 398976   ??  S     Tue05PM  25:57.73 /Applications/Google
 Chrome.app/Contents/MacOS/Google Chrome
_trustd            395   7.3  0.1 426957120  11008   ??  Ss    Tue05PM   0:38.29 /usr/libexec/trustd
dhvanil           8361   6.3  1.1 1865508000 188384   ??  S     6:15PM   0:08.79 /Applications/
Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/137.0.7151.120/
Helpers/Google Chrome Helper (Renderer).app/Contents/MacOS/Google Chrome Helper (Renderer)
 --type=renderer --metrics-client-id=02d43120-0ec6-4d43-afd7-f3f4fce54beb --lang=en-GB --
num-raster-threads=4 --enable-zero-copy --enable-gpu-memory-buffer-compositor-resources
 --enable-main-frame-before-activation --renderer-client-id=1646 --time-ticks-at-unix-
epoch=-1750764624026555 --launch-time-ticks=54360389696 --shared-files --field-trial-
handle=1718379636,r,12621174580819335943,9850387299252 [...]
```

152743 - Unix Software Discovery Commands Not Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials, but encountered difficulty running commands used to find unmanaged software.

Description

Nessus found problems running commands on the target host which are used to find software that is not managed by the operating system.

Details of the issues encountered are reported by this plugin.

Failure to properly execute commands used to find and characterize unmanaged software on the target host can lead to scans that do not report known vulnerabilities. There may be little in the scan results of unmanaged software plugins to indicate the missing availability of the source commands except audit trail messages.

Commands used to find unmanaged software installations might fail for a variety of reasons, including:

* Inadequate scan user permissions,

* Failed privilege escalation,

* Intermittent network disruption, or

* Missing or corrupt executables on the target host.

Please address the issues reported here and redo the scan.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Failures in commands used to assess Unix software:

  tail -x                     :
    tail: invalid option -- xusage: tail [-F | -f | -r] [-q] [-b # | -c # | -n #] [file ...]


Protocol : LOCAL
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

Plugin Output

tcp/54703

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port   : 54703
  Type   : spontaneous
  Banner :
0x00:  01 00 00 00                                        ....
```

84503 - Wireshark Installed (Mac OS X)

Synopsis

A packet capture utility is installed on the remote host.

Description

Wireshark, a packet capture utility, is installed on the remote Mac OS X host.

See Also

https://www.wireshark.org/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0746

Plugin Information

Published: 2015/07/02, Modified: 2025/03/11

Plugin Output

tcp/0

```
Path    : /Applications/Wireshark.app
Version : 4.4.2
```

118800 - Zoom.us Installed (macOS)

Synopsis

Video conferencing software is installed on the remote macOS / Mac OS X host.

Description

Zoom, video conferencing software, is installed on the remote macOS / Mac OS X host.

NOTE: Detection only works for the scanning user. The plugin needs to be run for each user suspected of having the install.

See Also

https://zoom.us/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/11/07, Modified: 2025/03/11

Plugin Output

tcp/0

```
Product           : zoom
Path              : /Applications/zoom.us.app
Installed version : 6.4.12 (56699)
```

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       : dhvanils-Laptop.local.

  - Advertised services :
    o Service name      : dhvanil's Laptop._airplay._tcp.local.
      Port number       : 7000
    o Service name      : AE229A20C786@dhvanil's Laptop._raop._tcp.local.
      Port number       : 7000
    o Service name      : dhvanil's Laptop._companion-link._tcp.local.
      Port number       : 54703
```

99265 - macOS Remote Listeners Enumeration

Synopsis

It was possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

Nessus was able to use SSH to list the processes running on the remote macOS or Mac OS X host and their TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/06/16

Plugin Output

udp/137

```
The process 'launchd' running under the user 'root' is listening on this port (pid 1).
```

udp/137

```
The process 'netbiosd' running under the user '_netbios' is listening on this port (pid 7686).
```

99265 - macOS Remote Listeners Enumeration

Synopsis

It was possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

Nessus was able to use SSH to list the processes running on the remote macOS or Mac OS X host and their TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/06/16

Plugin Output

udp/138

```
The process 'launchd' running under the user 'root' is listening on this port (pid 1).
```

udp/138

```
The process 'netbiosd' running under the user '_netbios' is listening on this port (pid 7686).
```

99265 - macOS Remote Listeners Enumeration

Synopsis

It was possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

Nessus was able to use SSH to list the processes running on the remote macOS or Mac OS X host and their TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/06/16

Plugin Output

udp/3722

```
The process 'rapportd' running under the user 'dhvanil' is listening on this port (pid 585).
```

99265 - macOS Remote Listeners Enumeration

Synopsis

It was possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

Nessus was able to use SSH to list the processes running on the remote macOS or Mac OS X host and their TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/06/16

Plugin Output

tcp/5000/www

```
The process 'ControlCenter' running under the user 'dhvanil' is listening on this port (pid 628).
```

99265 - macOS Remote Listeners Enumeration

Synopsis

It was possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

Nessus was able to use SSH to list the processes running on the remote macOS or Mac OS X host and their TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/06/16

Plugin Output

udp/5353/mdns

```
The process 'Google\x20Chrome\x20Helper' running under the user 'dhvanil' is listening on this port
 (pid 868).
```

udp/5353/mdns

```
The process 'mDNSResponder' running under the user '_mdnsresponder' is listening on this port (pid
 442).
```

99265 - macOS Remote Listeners Enumeration

Synopsis

It was possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

Nessus was able to use SSH to list the processes running on the remote macOS or Mac OS X host and their TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/06/16

Plugin Output

tcp/7000/www

```
The process 'ControlCenter' running under the user 'dhvanil' is listening on this port (pid 628).
```

99265 - macOS Remote Listeners Enumeration

Synopsis

It was possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

Nessus was able to use SSH to list the processes running on the remote macOS or Mac OS X host and their TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/06/16

Plugin Output

tcp/8834/www

```
The process 'nessusd' running under the user 'root' is listening on this port (pid 8215).
```

99265 - macOS Remote Listeners Enumeration

Synopsis

It was possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

Nessus was able to use SSH to list the processes running on the remote macOS or Mac OS X host and their TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/06/16

Plugin Output

udp/50383

```
The process 'syslogd' running under the user 'root' is listening on this port (pid 347).
```

99265 - macOS Remote Listeners Enumeration

Synopsis

It was possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

Nessus was able to use SSH to list the processes running on the remote macOS or Mac OS X host and their TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/06/16

Plugin Output

tcp/54703

```
The process 'rapportd' running under the user 'dhvanil' is listening on this port (pid 585).
```

99265 - macOS Remote Listeners Enumeration

Synopsis

It was possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

Nessus was able to use SSH to list the processes running on the remote macOS or Mac OS X host and their TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/06/16

Plugin Output

udp/57661

```
The process 'replicatord' running under the user 'dhvanil' is listening on this port (pid 668).
```

99265 - macOS Remote Listeners Enumeration

Synopsis

It was possible to obtain the names of processes listening on the remote UDP and TCP ports.

Description

Nessus was able to use SSH to list the processes running on the remote macOS or Mac OS X host and their TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/06/16

Plugin Output

udp/61741

```
The process 'sharingd' running under the user 'dhvanil' is listening on this port (pid 623).
```

95929 - macOS and Mac OS X User List Enumeration

Synopsis

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

Description

Using the supplied credentials, Nessus was able to extract the member list of the 'Admin' and 'Wheel' groups on the remote host. Members of these groups have administrative access.

Solution

None

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

User   : dhvanil
Groups : _lpadmin
         _appserverusr
         admin
         access_bpf
         _appserveradm

User   : root
Groups : tty
         staff
         kmem
         wheel
         sys
         certusers
         procview
         procmod
         admin
         daemon
         operator

User   : daemon

User   : nobody

----------[ Service Accounts ]----------

User   : _timezone
```

```
User   : _mdnsresponder

User   : _cvmsroot

User   : _backgroundassets
Groups : _backgroundassets

User   : _calendar
Groups : _postgres
         certusers
         _keytabusers

User   : _qtss

User   : _krb_changepw

User   : _modelmanagerd
Groups : _modelmanagerd

User   : _sntpd
Groups : _sntpd

User   : _launchservicesd

User   : _kadmin_admin

User   : _mailman

User   : _reportsystemmemory
Groups : _reportsystemmemory

User   : _postgres

User   : _appinstalld
Groups : _appinstalld

User   : _lda

User   : _corespeechd
Groups : _corespeechd

User   : _aonsensed
Groups : _aonsensed

User   : _diskimagesiod
Groups : _diskimagesiod

User   : _coremediaiod

User   : _gamecontrollerd

User   : _installer

User   : _screensaver

User   : _nearbyd
Groups : _nearbyd

User   : _krb_kerberos

User   : _securityagent

User   : _neuralengine
Groups : _neuralengine

User   : _biome
Groups : _biome

User   : _coreaudiod
```

```
User   : _notification_proxy

User   : _mysql

User   : _cyrus
Groups : certusers

User   : _unknown

User   : _accessoryupdater
Groups : _accessoryupdater

User   : _oahd
Groups : _oahd

User   : _appstore
Groups : _appstore

User   : _krb_krbtgt

User   : _ces

User   : _driverkit
Groups : _driverkit

User   : _www

User   : _coreml
Groups : _coreml

User   : _findmydevice

User   : _windowserver

User   : _appowner

User   : _cvs

User   : _diagnosticservicesd
Groups : _diagnosticservicesd

User   : _ondemand

User   : _datadetectors

User   : _mobileasset

User   : _xserverdocs
Groups : _postgres

User   : _postfix
Groups : certusers
         _keytabusers

User   : _ [...]
```