Metasploitable

Report generated by Tenable Nessus™ Wed, 30 Apr 2025 14:34:19 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.64.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	1	27

Scan Information

Start time: Wed Apr 30 14:27:42 2025
End time: Wed Apr 30 14:34:19 2025

Host Information

Netbios Name: MAC
IP: 192.168.64.1
MAC Address: 1E:F6:4C:39:6F:64
OS: Darwin

Vulnerabilities

50686 - IP Forwarding Enabled

Synopsis

The remote host has IP forwarding enabled.

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

echo 0 > /proc/sys/net/ipv4/ip_forward

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

sysctl -w net.inet.ip.forwarding=0

For other systems, check with your vendor.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.9

EPSS Score

0.0596

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0511

Plugin Information

Published: 2010/11/23, Modified: 2023/10/17

Plugin Output

tcp/0

15753 - Multiple Vendor DNS Response Flooding Denial Of Service

Synopsis

The remote DNS server is vulnerable to a denial of service attack.

Description

The remote DNS server is vulnerable to a denial of service attack because it replies to DNS responses.

An attacker could exploit this vulnerability by spoofing a DNS packet so that it appears to come from 127.0.0.1 and make the remote DNS server enter into an infinite loop, therefore denying service to legitimate users.

See Also

http://www.nessus.org/u?a04dcb96

Solution

Contact the vendor for an appropriate upgrade.

Risk Factor

Medium

VPR Score

2.7

EPSS Score

0.0196

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	11642
CVE	CVE-2004-0789

Plugin Information

Published: 2004/11/18, Modified: 2018/07/10

Plugin Output

udp/53/dns

```
Nessus sent the following response data :

0x00:  2F 77 81 80 00 01 00 00 00 01 00 00 03 77 77 77    /w...........www
0x10:  06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00 10 00 01    .google.com.....
0x20:  C0 10 00 06 00 01 00 00 00 3C 00 26 03 6E 73 31    .........<.&.ns1
0x30:  C0 10 09 64 6E 73 2D 61 64 6D 69 6E C0 10 2C DC    ...dns-admin..,.
0x40:  B4 64 00 00 03 84 00 00 03 84 00 00 07 08 00 00    .d..............
0x50:  00 3C                                              .<

And the DNS server replied with the following response :

0x00:  2F 77 81 04 00 01 00 00 00 01 00 00 03 77 77 77    /w...........www
0x10:  06 67 6F 6F 67 6C 65 03 63 6F 6D 00 00 10 00 01    .google.com.....
0x20:  C0 10 00 06 00 01 00 00 00 3C 00 26 03 6E 73 31    .........<.&.ns1
0x30:  C0 10 09 64 6E 73 2D 61 64 6D 69 6E C0 10 2C DC    ...dns-admin..,.
0x40:  B4 64 00 00 03 84 00 00 03 84 00 00 07 08 00 00    .d..............
0x50:  00 3C                                              .<
```

10663 - DHCP Server Detection

Synopsis

The remote DHCP server may expose information about the associated network.

Description

This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout.

Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on.

It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.

Solution

Apply filtering to keep this information off the network and remove any options that are not in use.

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2001/05/05, Modified: 2019/03/06

Plugin Output

udp/67

```
Nessus gathered the following information from the remote DHCP server :

  Master DHCP server of this network : 192.168.64.1
  IP address the DHCP server would attribute us : 192.168.64.4
  DHCP server(s) identifier : 192.168.64.1
  Netmask : 255.255.255.0
  Router : 192.168.64.1
  Domain name server(s) : 192.168.64.1
  Domain name : fritz.box
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53/dns

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

udp/53/dns

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 : unknown
Confidence level : 56
```

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: 2025/04/28

Plugin Output

tcp/0

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/850.19.1
```

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/850.19.1
```

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/850.19.1
  X-Apple-ProcessingTime: 1
  X-Apple-RequestReceivedTimestamp: 248193552

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/850.19.1
  X-Apple-ProcessingTime: 1
  X-Apple-RequestReceivedTimestamp: 248201586

Response Body :
```

43829 - Kerberos Information Disclosure

Synopsis

The remote Kerberos server is leaking information.

Description

Nessus was able to retrieve the realm name and/or server time of the remote Kerberos server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/01/08, Modified: 2015/09/24

Plugin Output

tcp/88

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/53/dns

```
Port 53/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/88

```
Port 88/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/5000/www

```
Port 5000/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/5900/vnc

```
Port 5900/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/7000/www

```
Port 7000/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.4
Nessus build : 20028
Plugin feed version : 202504291626
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1804-aarch64
Scan type : Normal
Scan name : Metasploitable
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.64.4
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 111.215 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 0
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/4/30 14:27 CEST (UTC +02:00)
Scan duration : 388 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Darwin
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Windows
Confidence level : 50
Method : Misc
Type : general-purpose
Fingerprint : unknown

Remote operating system : FreeBSD 6.0
FreeBSD 6.1
FreeBSD 6.2
Mac OS X 10.4
Confidence level : 54
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
   P1:B10013:F0x12:W65535:O0204ffff:M1460:
   P2:B10013:F0x12:W65535:O0204ffff010303060101080affffffff4445414404020000:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191004_7_p=5000

Following fingerprints could not be used to determine OS :
```

```
HTTP:!:Server: AirTunes/850.19.1
```

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: 2025/03/31

Plugin Output

tcp/0

```
Remote operating system : Darwin
Confidence level : 56
Method : MLSinFP


The remote host is running Darwin
```

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/5900/vnc

```
A vnc 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.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

udp/0

19288 - VNC Server Security Type Detection

Synopsis

A VNC server is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types'.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/07/22, Modified: 2021/07/13

Plugin Output

tcp/5900/vnc

```
The remote VNC server supports the following security types :\n\n  30 (Mac OSX SecType 30)
    33
    36
  35 (Mac OSX SecType 35)
```

65792 - VNC Server Unencrypted Communication Detection

Synopsis

A VNC server with one or more unencrypted 'security-types' is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/03, Modified: 2014/03/12

Plugin Output

tcp/5900/vnc

10342 - VNC Software Detection

Synopsis

The remote host is running a remote display software (VNC).

Description

The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.

See Also

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

Solution

Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port.

Risk Factor

None

Plugin Information

Published: 2000/03/07, Modified: 2017/06/12

Plugin Output

tcp/5900/vnc

```
The highest RFB protocol version supported by the server is :

  3.889
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 1 NetBIOS names have been gathered :

 MAC              = Computer name

The remote host has the following MAC address on its adapter :

   1e:f6:4c:39:6f:64
```

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

192.168.64.4

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	2	3	1	64

Scan Information

Start time: Wed Apr 30 14:27:42 2025
End time: Wed Apr 30 14:29:33 2025

Host Information

IP: 192.168.64.4
MAC Address: F2:28:C8:53:AF:82
OS: Linux Kernel 6.12.20-arm64

Vulnerabilities

208193 - OpenJDK 8 <= 8u412 / 11.0.0 <= 11.0.23 / 17.0.0 <= 17.0.11 / 21.0.0 <= 21.0.3 / 22.0.0 <= 22.0.1 Multiple Vulnerabilities (2024-07-16)

Synopsis

OpenJDK is affected by multiple vulnerabilities.

Description

The version of OpenJDK installed on the remote host is prior to 8 <= 8u412 / 11.0.0 <= 11.0.23 / 17.0.0 <= 17.0.11 / 21.0.0 <= 21.0.3 / 22.0.0 <= 22.0.1. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024-07-16 advisory.

Please Note: Java CVEs do not always include OpenJDK versions, but are confirmed separately by Tenable using the patch versions from the referenced OpenJDK security advisory.

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running

sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21147)

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21145)

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21140)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition.

Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). (CVE-2024-21144)

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21131)

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21138)

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://openjdk.java.net/groups/vulnerability/advisories/2024-07-16

Solution

Upgrade to an OpenJDK version greater than 8u412 / 11.0.23 / 17.0.11 / 21.0.3 / 22.0.1

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.0019

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-21131
CVE	CVE-2024-21138
CVE	CVE-2024-21140
CVE	CVE-2024-21144
CVE	CVE-2024-21145
CVE	CVE-2024-21147

Plugin Information

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

Plugin Output

tcp/0

234472 - OpenJDK 8 <= 8u442 / 11.0.0 <= 11.0.26 / 17.0.0 <= 17.0.14 / 21.0.0 <= 21.0.6 / 24.0.0 <= 24.0.0 Multiple Vulnerabilities (2025-04-15)

Synopsis

OpenJDK is affected by multiple vulnerabilities.

Description

The version of OpenJDK installed on the remote host is 8 prior to 8u442 / 11.0.0 prior to 11.0.26 / 17.0.0 prior to 17.0.14 / 21.0.0 prior to 21.0.6 / 24.0.0 prior to 24.0.0. It is, therefore, affected by multiple vulnerabilities as referenced in the 2025-04-15 advisory.

Please Note: Java CVEs do not always include OpenJDK versions, but are confirmed separately by Tenable using the patch versions from the referenced OpenJDK security advisory.

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE:8u441, 8u441-perf, 11.0.26, 17.0.14, 21.0.6, 24; Oracle GraalVM for JDK:17.0.14, 21.0.6, 24; Oracle GraalVM Enterprise Edition:20.3.17 and 21.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data.

Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.

(CVE-2025-21587)

- Vulnerability in Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle Java SE: 21.0.6, 24; Oracle GraalVM for JDK: 21.0.6 and 24. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE.

Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data as well as unauthorized read access to a subset of Oracle Java SE accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2025-30691)

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u441, 8u441-perf, 11.0.26, 17.0.14, 21.0.6, 24; Oracle GraalVM for JDK: 17.0.14, 21.0.6, 24; Oracle GraalVM Enterprise Edition: 20.3.17 and 21.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that

comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). (CVE-2025-30698)

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://openjdk.java.net/groups/vulnerability/advisories/2025-04-15

Solution

Upgrade to an OpenJDK version greater than 8u442 / 11.0.26 / 17.0.14 / 21.0.6 / 24.0.0

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2025-21587
CVE	CVE-2025-30691
CVE	CVE-2025-30698

Plugin Information

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

Plugin Output

tcp/0

209225 - OpenJDK 8 <= 8u422 / 11.0.0 <= 11.0.24 / 17.0.0 <= 17.0.12 / 21.0.0 <= 21.0.4 / 23.0.0 <= 23.0.0 Multiple Vulnerabilities (2024-10-15)

Synopsis

OpenJDK is affected by multiple vulnerabilities.

Description

The version of OpenJDK installed on the remote host is 8 prior to 8u422 / 11.0.0 prior to 11.0.24 / 17.0.0 prior to 17.0.12 / 21.0.0 prior to 21.0.4 / 23.0.0 prior to 23.0.0. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024-10-15 advisory.

Please Note: Java CVEs do not always include OpenJDK versions, but are confirmed separately by Tenable using the patch versions from the referenced OpenJDK security advisory.

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21235)

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). (CVE-2024-21208)

- Vulnerability in Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4 and 23. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE.

Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21210)

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE:

8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21217)

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://openjdk.java.net/groups/vulnerability/advisories/2024-10-15

Solution

Upgrade to an OpenJDK version greater than 8u422 / 11.0.24 / 17.0.12 / 21.0.4 / 23.0.0

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.5

EPSS Score

0.0043

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-21208
CVE	CVE-2024-21210
CVE	CVE-2024-21217
CVE	CVE-2024-21235

Plugin Information

Published: 2024/10/17, Modified: 2024/10/17

Plugin Output

tcp/0

214562 - OpenJDK 8 <= 8u432 / 11.0.0 <= 11.0.25 / 17.0.0 <= 17.0.13 / 21.0.0 <= 21.0.5 / 23.0.0 <= 23.0.1 Vulnerability (2025-01-21)

Synopsis

OpenJDK is affected by a vulnerability.

Description

The version of OpenJDK installed on the remote host is 8 prior to 8u432 / 11.0.0 prior to 11.0.25 / 17.0.0 prior to 17.0.13 / 21.0.0 prior to 21.0.5 / 23.0.0 prior to 23.0.1. It is, therefore, affected by a vulnerability as referenced in the 2025-01-21 advisory.

Please Note: Java CVEs do not always include OpenJDK versions, but are confirmed separately by Tenable using the patch versions from the referenced OpenJDK security advisory.

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u431-perf, 11.0.25, 17.0.13, 21.0.5, 23.0.1; Oracle GraalVM for JDK: 17.0.13, 21.0.5, 23.0.1; Oracle GraalVM Enterprise Edition: 20.3.16 and 21.3.12. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2025-21502)

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://openjdk.java.net/groups/vulnerability/advisories/2025-01-21

Solution

Upgrade to an OpenJDK version greater than 8u432 / 11.0.25 / 17.0.13 / 21.0.5 / 23.0.1

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.5

EPSS Score

0.0002

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2025-21502

Plugin Information

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

Plugin Output

tcp/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: 2020/04/27

Plugin Output

tcp/8834/www

193405 - OpenJDK 8 <= 8u402 / 11.0.0 <= 11.0.22 / 17.0.0 <= 17.0.10 / 21.0.0 <= 21.0.2 / 22.0.0 <= 22.0.0 Multiple Vulnerabilities (2024-04-16

Synopsis

OpenJDK is affected by multiple vulnerabilities.

Description

The version of OpenJDK installed on the remote host is prior to 8 <= 8u402 / 11.0.0 <= 11.0.22 / 17.0.0 <= 17.0.10 / 21.0.0 <= 21.0.2 / 22.0.0 <= 22.0.0. It is, therefore, affected by multiple vulnerabilities as referenced in the 2024-04-16 advisory.

Please Note: Java CVEs do not always include OpenJDK versions, but are confirmed separately by Tenable using the patch versions from the referenced OpenJDK security advisory.

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u401, 8u401-perf, 11.0.22, 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21094)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Oracle Java SE: 8u401, 8u401-perf, 11.0.22; Oracle GraalVM Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition.

Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.

(CVE-2024-21085)

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u401, 8u401-perf, 11.0.22, 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21011)

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u401-perf, 11.0.22, 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2 and 22; Oracle GraalVM Enterprise Edition: 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2024-21068)

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.22, 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition:

20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). (CVE-2024-21012)

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://openjdk.java.net/groups/vulnerability/advisories/2024-04-16

Solution

Upgrade to an OpenJDK version greater than 8u402 / 11.0.22 / 17.0.10 / 21.0.2 / 22.0.0

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.0029

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-21011
CVE	CVE-2024-21012
CVE	CVE-2024-21068
CVE	CVE-2024-21085
CVE	CVE-2024-21094

Plugin Information

Published: 2024/04/17, Modified: 2024/04/17

Plugin Output

tcp/0

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: 2025/04/28

Plugin Output

tcp/0

142640 - Apache HTTP Server Site Enumeration

Synopsis

The remote host is hosting websites using Apache HTTP Server.

Description

Domain names and IP addresses from Apache HTTP Server configuration file were retrieved from the remote host. Apache HTTP Server is a webserver environment written in C. Note: Only Linux- and Unix-based hosts are currently supported by this plugin.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/11/09, Modified: 2025/02/12

Plugin Output

tcp/0

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:linux:linux_kernel -> Linux Kernel

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.58 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:exiv2:exiv2:0.27.6 -> Exiv2
  cpe:/a:exiv2:libexiv2:0.27.6
  cpe:/a:gnupg:libgcrypt:1.11.0 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:8.5.0 -> Haxx Curl
  cpe:/a:haxx:libcurl:8.5.0 -> Haxx libcurl
  cpe:/a:jmcnamara:spreadsheet%3a%3aparseexcel:0.66 -> John McNamara Spreadsheet::ParseExcel
  cpe:/a:nginx:nginx:1.26.3 -> Nginx
  cpe:/a:nginx:nginx:1.26.3-2 -> Nginx
  cpe:/a:numpy:numpy:1.24.2 -> NumPy
  cpe:/a:openssl:openssl:3.0.15 -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:3.1.4 -> OpenSSL Project OpenSSL
```

```
cpe:/a:openssl:openssl:3.4.0 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:3.5.0 -> OpenSSL Project OpenSSL
cpe:/a:openvpn:openvpn:2.6.7 -> OpenVPN
cpe:/a:oracle:openjdk:17.0.10 -> Oracle OpenJDK -
cpe:/a:oracle:openjdk:22.0.2.9.70 -> Oracle OpenJDK -
cpe:/a:php:php:8.2.12 -> PHP PHP
cpe:/a:postgresql:postgresql:16.2 -> PostgreSQL
cpe:/a:ruby-lang:ruby:3.1.2 -> Ruby-lang Ruby
cpe:/a:sqlite:sqlite -> SQLite
cpe:/a:tenable:nessus -> Tenable Nessus
cpe:/a:tenable:nessus:10.8.4 -> Tenable Nessus
cpe:/a:tukaani:xz:5.8.1 -> Tukaani XZ
cpe:/a:vim:vim:9.1 -> Vim
x-cpe:/a:java:jre:17.0.10
x-cpe:/a:java:jre:22.0.2.9.70
x-cpe:/a:libndp:libndp:1.9
```

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: 2025/04/28

Plugin Output

tcp/0

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: 2025/04/28

Plugin Output

tcp/0

```
Hostname : kali2023
  kali2023 (hostname command)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

159273 - Dockerfile Detection for Linux/UNIX

Synopsis

Detected Dockerfiles on the host.

Description

The host contains Dockerfiles, text files containing instructions to build Docker images.

See Also

https://docs.docker.com/engine/reference/builder/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/03/29, Modified: 2025/04/28

Plugin Output

tcp/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 :

 - 192.168.64.4 (on interface eth0)
 - 127.0.0.1 (on interface lo)
```

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following IPv6 interfaces are set on the remote host :

 - fdd6:cbc0:b164:afaa:2561:306f:7485:ab25 (on interface eth0)
 - fe80::11b:da99:c1d8:702 (on interface eth0)
 - fdd6:cbc0:b164:afaa:3f7:35f1:d9fe:4013 (on interface eth0)
 - ::1 (on interface lo)
```

33276 - Enumerate MAC Addresses via SSH

Synopsis

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

Description

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

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

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

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: 2025/04/28

Plugin Output

tcp/0

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: 2025/04/28

Plugin Output

tcp/0

204827 - Exiv2 Installed (Linux / Unix)

Synopsis

Exiv2 is installed on the remote Linux / Unix host.

Description

Exiv2 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.204827' scanner setting in Nessus 8.15.1 or later.

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

See Also

https://exiv2.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/04/28

Plugin Output

tcp/0

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
```

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: Wed, 30 Apr 2025 12:27:52 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 [...]
```

171410 - IP Assignment Method Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/04/28

Plugin Output

tcp/0

147817 - Java Detection and Identification (Linux / Unix)

Synopsis

Java is installed on the remote Linux / Unix host.

Description

One or more instances of Java are installed on the remote Linux / Unix host. This may include private JREs bundled with the Java Development Kit (JDK).

Notes:

- This plugin attempts to detect Oracle and non-Oracle JRE instances such as Zulu Java, Amazon Corretto, AdoptOpenJDK, IBM Java, etc

- To discover instances of JRE that are not in PATH, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

See Also

https://en.wikipedia.org/wiki/Java_(software_platform)

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0690

Plugin Information

Published: 2021/03/16, Modified: 2025/04/28

Plugin Output

tcp/0

189990 - Jmcnamara Spreadsheet-ParseExcel Installed (Unix)

Synopsis

Jmcnamara Spreadsheet-ParseExcel is installed on the remote Unix host.

Description

Jmcnamara Spreadsheet-ParseExcel is installed on the remote Unix host.

See Also

https://github.com/jmcnamara/spreadsheet-parseexcel

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/02/05, Modified: 2025/04/28

Plugin Output

tcp/0

151883 - Libgcrypt Installed (Linux/UNIX)

Synopsis

Libgcrypt is installed on this host.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2025/04/28

Plugin Output

tcp/0

200214 - Libndp Installed (Linux / Unix)

Synopsis

Libndp is installed on the remote Linux / Unix host.

Description

Libndp 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.200214' 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://github.com/jpirko/libndp

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/07, Modified: 2025/04/28

Plugin Output

tcp/0

157358 - Linux Mounted Devices

Synopsis

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

Description

Report the mounted devices information on the target machine at scan time using the following commands.

/bin/df -h /bin/lsblk /bin/mount -l

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

95928 - Linux User List Enumeration

Synopsis

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

Description

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

Solution

None

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.4
Nessus build : 20028
Plugin feed version : 202504291626
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1804-aarch64
Scan type : Normal
Scan name : Metasploitable
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.64.4
Ping RTT : Unavailable
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 0
Safe checks : yes
Optimize the test : no
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 : 2025/4/30 14:27 CEST (UTC +02:00)
Scan duration : 111 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

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: 2025/02/19

Plugin Output

tcp/8834/www

```
Port 8834/tcp was found to be open
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Linux Kernel 6.12.20-arm64
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux kali2023 6.12.20-arm64 #1 SMP Kali 6.12.20-1kali1 (2025-03-26) aarch64
 GNU/Linux


Following fingerprints could not be used to determine OS :
 HTTP:!:Server: NessusWWW

SSLcert:!:i/CN:Nessus Certification Authorityi/O:Nessus Users Unitedi/OU:Nessus Certification
 Authoritys/CN:kali2023s/O:Nessus Users Uniteds/OU:Nessus Server
42c036e4216841aedca784715c49aedbc75edccc
```

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: 2025/03/31

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 6.12.20-arm64
Confidence level : 99
Method : uname


The remote host is running Linux Kernel 6.12.20-arm64
```

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 :
Linux kali2023 6.12.20-arm64 #1 SMP Kali 6.12.20-1kali1 (2025-03-26) aarch64 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
kali-rolling

This is a Kali Linux system

OS Security Patch Assessment is available for this host.
Runtime : 1.124924 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

148373 - OpenJDK Java Detection (Linux / Unix)

Synopsis

A distribution of Java is installed on the remote Linux / Unix host.

Description

One or more instances of OpenJDK Java are installed on the remote host. This may include private JREs bundled with the Java Development Kit (JDK).

Notes:

- Addition information provided in plugin Java Detection and Identification (Unix)

- Additional instances of Java may be discovered by enabling thorough tests

See Also

https://openjdk.java.net/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/04/07, Modified: 2025/02/12

Plugin Output

tcp/0

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

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

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

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

See Also

https://openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/04/28

Plugin Output

tcp/0

232856 - OpenVPN Installed (Linux)

Synopsis

OpenVPN is installed on the remote Linux host.

Description

OpenVPN is installed on the remote Linux host.

Note: Enabling the 'Perform thorough tests' setting will search the file system more broadly.

See Also

https://openvpn.net/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/03/19, Modified: 2025/04/28

Plugin Output

tcp/0

216936 - PHP Scripting Language Installed (Unix)

Synopsis

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

Description

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

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

See Also

https://www.php.net

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/13, Modified: 2025/04/28

Plugin Output

tcp/0

179139 - Package Manager Packages Report (nix)

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/01, Modified: 2025/03/03

Plugin Output

tcp/0

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: 2025/04/08

Plugin Output

tcp/0

130024 - PostgreSQL Client/Server Installed (Linux)

Synopsis

One or more PostgreSQL server or client versions are available on the remote Linux host.

Description

One or more PostgreSQL server or client versions have been detected on the remote Linux host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/10/18, Modified: 2025/04/28

Plugin Output

tcp/0

202184 - Ruby Programming Language Installed (Linux)

Synopsis

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

Description

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

See Also

https://ruby.org/en/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/11, Modified: 2025/04/28

Plugin Output

tcp/0

174788 - SQLite Local Detection (Linux)

Synopsis

The remote Linux host has SQLite Database software installed.

Description

Version information for SQLite was retrieved from the remote host. SQLite is an embedded database written in C.

- To discover instances of SQLite that are not in PATH, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

See Also

https://www.sqlite.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/04/26, Modified: 2025/04/28

Plugin Output

tcp/0

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: 2023/07/10

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

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}
```

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

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

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

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

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

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: 2025/04/28

Plugin Output

tcp/0

192709 - Tukaani XZ Utils Installed (Linux / Unix)

Synopsis

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

Description

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

XZ Utils consists of several components, including:

- liblzma

- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.192709' scanner setting in Nessus 8.15.1 or later.

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2025/04/28

Plugin Output

tcp/0

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

152742 - Unix Software Discovery Commands Available

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

189731 - Vim Installed (Linux)

Synopsis

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

https://www.vim.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2025/04/28

Plugin Output

tcp/0

182848 - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

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

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/04/28

Plugin Output

tcp/0

204828 - libexiv2 Installed (Linux / Unix)

Synopsis

libexiv2 is installed on the remote Linux / Unix host.

Description

libexiv2 is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.204828' scanner setting in Nessus 8.15.1 or later.

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

See Also

https://exiv2.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/04/28

Plugin Output

tcp/0

136340 - nginx Installed (Linux/UNIX)

Synopsis

NGINX is installed on the remote Linux / Unix host.

Description

NGINX, a web server with load balancing capabilities, is installed on the remote Linux / Unix host.

See Also

https://www.nginx.com

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/05/05, Modified: 2025/04/28

Plugin Output

tcp/0