My Basic Network Scan

Report generated by Tenable Nessus™ Sat, 31 May 2025 21:50:35 IST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.110.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	2

Host Information

IP: 192.168.110.1

Vulnerabilities

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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- Whether the display of superseded patches is enabled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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/05/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.4
Nessus build : 20028
Plugin feed version : 202505310604
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.110.165
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 120.359 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 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 : 2025/5/31 21:14 IST (UTC +05:30)
Scan duration : 785 sec
Scan for malware : no
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.110.165 to 192.168.110.1 :
192.168.110.165

ttl was greater than 50 - Completing Traceroute.

?

Hop Count: 1

An error was detected along the way.
```

192.168.110.2

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	0	13

Host Information

IP:	192.168.110.2
MAC Address:	00:50:56:E1:01:FD
OS:	CISCO PIX 7.0

Vulnerabilities

12217 - DNS Server Cache Snooping Remote Information Disclosure

Synopsis

The remote DNS server is vulnerable to cache snooping attacks.

Description

The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

See Also

http://cs.unc.edu/~fabian/course_papers/cache_snooping.pdf

Solution

Contact the vendor of the DNS software for a fix.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/04/27, Modified: 2020/04/07

Plugin Output

udp/53/dns

```
Nessus sent a non-recursive query for example.edu
and received 1 answer :

96.7.129.25
```

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

4.0

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

```
IP forwarding appears to be enabled on the remote host.

 Detected local MAC Address        : 000c29558747
 Response from local MAC Address   : 000c29558747

 Detected Gateway MAC Address      : 005056e101fd
 Response from Gateway MAC Address : 005056e101fd
```

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:cisco:pix_firewall:7.0 -> Cisco PIX Firewall Software
```

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

72779 - DNS Server Version Detection

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0937

Plugin Information

Published: 2014/03/03, Modified: 2024/09/24

Plugin Output

tcp/53/dns

```
DNS server answer for "version.bind" (over TCP) :

  dnsmasq-2.51
```

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 : firewall
Confidence level : 70
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:50:56:E1:01:FD : VMware, Inc.
```

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

```
The following is a consolidated list of detected MAC addresses:
  - 00:50:56:E1:01:FD
```

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
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/05/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.4
Nessus build : 20028
Plugin feed version : 202505310604
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.110.165
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 137.220 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 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 : 2025/5/31 21:14 IST (UTC +05:30)
Scan duration : 241 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 : Juniper ScreenOS
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP
Type : firewall
Fingerprint : SinFP:
   P1:B11013:F0x12:W64240:O0204ffff:M1460:
   P2:B11013:F0x12:W64240:O0204ffff:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191004_7_p=53
```

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: 2025/05/09

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0
Confidence level : 70
Method : SinFP


The remote host is running CISCO PIX 7.0
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.110.165 to 192.168.110.2 :
192.168.110.165
192.168.110.2

Hop Count: 1
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

192.168.110.165

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	9	8	1	73

Host Information

IP:	192.168.110.165
MAC Address:	00:0C:29:55:87:47
OS:	Linux Kernel 6.12.13-amd64

Vulnerabilities

190856 - Node.js 18.x < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities (Wednesday February 14 2024 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.19.1, 20.11.1, 21.6.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday February 14 2024 Security Releases advisory.

- On Linux, Node.js ignores certain environment variables if those may have been set by an unprivileged user while the process is running with elevated privileges with the only exception of CAP_NET_BIND_SERVICE. Due to a bug in the implementation of this exception, Node.js incorrectly applies this exception even when certain other capabilities have been set. This allows unprivileged users to inject code that inherits the process's elevated privileges. Impacts: Thank you, to Tobias Nieen for reporting this vulnerability and for fixing it. (CVE-2024-21892)

- A vulnerability in Node.js HTTP servers allows an attacker to send a specially crafted HTTP request with chunked encoding, leading to resource exhaustion and denial of service (DoS). The server reads an unbounded number of bytes from a single connection, exploiting the lack of limitations on chunk extension bytes. The issue can cause CPU and network bandwidth exhaustion, bypassing standard safeguards like timeouts and body size limits. Impacts: Thank you, to Bartek Nowotarski for reporting this vulnerability and thank you Paolo Insogna for fixing it. (CVE-2024-22019)

- The permission model protects itself against path traversal attacks by calling path.resolve() on any paths given by the user. If the path is to be treated as a Buffer, the implementation uses Buffer.from() to obtain a Buffer from the result of path.resolve(). By monkey-patching Buffer internals, namely, Buffer.prototype.utf8Write, the application can modify the result of path.resolve(), which leads to a path traversal vulnerability. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Tobias Nieen for reporting this vulnerability and for fixing it. (CVE-2024-21896)

- setuid() does not affect libuv's internal io_uring operations if initialized before the call to setuid().

This allows the process to perform privileged operations despite presumably having dropped such privileges through a call to setuid(). Impacts: Thank you, to valette for reporting this vulnerability and thank you Tobias Nieen for fixing it. (CVE-2024-22017)

- A vulnerability in the privateDecrypt() API of the crypto library, allowed a covert timing side-channel during PKCS#1 v1.5 padding error handling. The vulnerability revealed significant timing differences in decryption for valid and invalid ciphertexts. This poses a serious threat as attackers could remotely exploit the vulnerability to decrypt captured RSA ciphertexts or forge signatures, especially in scenarios involving API endpoints processing Json Web Encryption messages. Impacts: Thank you, to hkario for reporting this vulnerability and thank you Michael Dawson for fixing it. (CVE-2023-46809)

- Node.js depends on multiple built-in utility functions to normalize paths provided to node:fs functions, which can be overwritten with user-defined implementations leading to filesystem permission model bypass through path traversal attack. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to xion for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. (CVE-2024-21891)

- The Node.js Permission Model does not clarify in the documentation that wildcards should be only used as the last character of a file path. For example: --allow-fs-read=/home/node/.ssh/*.pub will ignore pub and give access to everything after .ssh/. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Tobias Nieen for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. (CVE-2024-21890)

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

See Also

http://www.nessus.org/u?313add11

Solution

Upgrade to Node.js version 18.19.1 / 20.11.1 / 21.6.2 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.1041

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-46809
CVE	CVE-2024-21890
CVE	CVE-2024-21891
CVE	CVE-2024-21892
CVE	CVE-2024-21896
CVE	CVE-2024-22017
CVE	CVE-2024-22019
XREF	IAVB:2024-B-0016-S

Plugin Information

Published: 2024/02/21, Modified: 2025/04/03

Plugin Output

tcp/0

```
Path              : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version     : 20.11.1
```

201082 - OpenSSL 3.1.0 < 3.1.7 Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.7. It is, therefore, affected by a vulnerability as referenced in the 3.1.7 advisory.

- Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash.

In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a no overlap response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. Found by Joseph Birr-Pixton. Thanks to David Benjamin (Google). Fix developed by Matt Caswell. Fixed in OpenSSL 3.3.2 (Affected since 3.3.0). (CVE-2024-5535)

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

See Also

http://www.nessus.org/u?f87142a6

https://www.cve.org/CVERecord?id=CVE-2024-5535

Solution

Upgrade to OpenSSL version 3.1.7 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.1077

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-5535

Plugin Information

Published: 2024/06/27, Modified: 2025/04/14

Plugin Output

tcp/0

```
Path              : /usr/lib/x86_64-linux-gnu/ruby/3.1.0/openssl.so
Reported version : 3.1.5
Fixed version     : 3.1.7
```

192945 - Node.js 18.x < 18.20.1 / 20.x < 20.12.1 / 21.x < 21.7.2 Multiple Vulnerabilities (Wednesday, April 3, 2024 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.20.1, 20.12.1, 21.7.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday, April 3, 2024 Security Releases advisory.

- An attacker can make the Node.js HTTP/2 server completely unavailable by sending a small amount of HTTP/2 frames packets with a few HTTP/2 frames inside. It is possible to leave some data in nghttp2 memory after reset when headers with HTTP/2 CONTINUATION frame are sent to the server and then a TCP connection is abruptly closed by the client triggering the Http2Session destructor while header frames are still being processed (and stored in memory) causing a race condition. Impacts: Thank you, to bart for reporting this vulnerability and Anna Henningsen for fixing it. (CVE-2024-27983)

- The team has identified a vulnerability in the http server of the most recent version of Node, where malformed headers can lead to HTTP request smuggling. Specifically, if a space is placed before a content-length header, it is not interpreted correctly, enabling attackers to smuggle in a second request within the body of the first. Impacts: Thank you, to bpingel for reporting this vulnerability and Paolo Insogna for fixing it. Summary The Node.js project will release new versions of the 18.x, 20.x, 21.x releases lines on or shortly after, Wednesday, April 3, 2024 in order to address: (CVE-2024-27982)

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://nodejs.org/en/blog/vulnerability/april-2024-security-releases/

Solution

Upgrade to Node.js version 18.20.1 / 20.12.1 / 21.7.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.0

EPSS Score

0.6955

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-27982
CVE	CVE-2024-27983
XREF	IAVB:2024-B-0033-S

Plugin Information

Published: 2024/04/05, Modified: 2024/04/19

Plugin Output

tcp/0

```
Path              : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version     : 20.12.1
```

201969 - Node.js 18.x < 18.20.4 / 20.x < 20.15.1 / 22.x < 22.4.1 Multiple Vulnerabilities (Monday, July 8, 2024 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.20.4, 20.15.1, 22.4.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Monday, July 8, 2024 Security Releases advisory.

- The CVE-2024-27980 was identified as an incomplete fix for the BatBadBut vulnerability. This vulnerability arises from improper handling of batch files with all possible extensions on Windows via child_process.spawn / child_process.spawnSync. A malicious command line argument can inject arbitrary commands and achieve code execution even if the shell option is not enabled. This vulnerability affects all users of child_process.spawn and child_process.spawnSync on Windows in all active release lines.

Impact: Thank you, to tianst for reporting this vulnerability and thank you RafaelGSS for fixing it.

(CVE-2024-27980)

- A security flaw in Node.js allows a bypass of network import restrictions. By embedding non-network imports in data URLs, an attacker can execute arbitrary code, compromising system security. Verified on various platforms, the vulnerability is mitigated by forbidding data URLs in network imports. Exploiting this flaw can violate network import security, posing a risk to developers and servers. Impact: Thank you, to dittyroma for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2024-22020)

- A vulnerability has been identified in Node.js, affecting users of the experimental permission model when the --allow-fs-write flag is used. Node.js Permission Model do not operate on file descriptors, however, operations such as fs.fchown or fs.fchmod can use a read-only file descriptor to change the owner and permissions of a file. This vulnerability affects all users using the experimental permission model in Node.js 20 and Node.js 22. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Impact: Thank you, to 4xpl0r3r for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2024-36137)

- A vulnerability has been identified in Node.js, affecting users of the experimental permission model when the --allow-fs-read flag is used. This flaw arises from an inadequate permission model that fails to restrict file stats through the fs.lstat API. As a result, malicious actors can retrieve stats from files that they do not have explicit read access to. This vulnerability affects all users using the experimental permission model in Node.js 20 and Node.js 22. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Impact: Thank you, to haxatron1 for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2024-22018)

- The Permission Model assumes that any path starting with two backslashes \ has a four-character prefix that can be ignored, which is not always true. This subtle bug leads to vulnerable edge cases. This vulnerability affects Windows users of the Node.js Permission Model in version v22.x and v20.x Impact:

Thank you, to tniessen for reporting this vulnerability and thank you RafaelGSS for fixing it.

(CVE-2024-37372)

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://nodejs.org/en/blog/vulnerability/july-2024-security-releases/

Solution

Upgrade to Node.js version 18.20.4 / 20.15.1 / 22.4.1 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0074

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-22018
CVE	CVE-2024-22020
CVE	CVE-2024-27980
CVE	CVE-2024-36137
CVE	CVE-2024-37372
XREF	IAVB:2024-B-0039-S
XREF	IAVB:2024-B-0083-S

Plugin Information

Published: 2024/07/08, Modified: 2025/01/24

Plugin Output

tcp/0

```
Path              : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version     : 20.15.1
```

214404 - Node.js 18.x < 18.20.6 / 20.x < 20.18.2 / 22.x < 22.13.1 / 23.x < 23.6.1 Multiple Vulnerabilities (Tuesday, January 21, 2025 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.20.6, 20.18.2, 22.13.1, 23.6.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Tuesday, January 21, 2025 Security Releases advisory.

- A memory leak could occur when a remote peer abruptly closes the socket without sending a GOAWAY notification. Additionally, if an invalid header was detected by nghttp2, causing the connection to be terminated by the peer, the same leak was triggered. This flaw could lead to increased memory consumption and potential denial of service under certain conditions. This vulnerability affects HTTP/2 Server users on Node.js v18.x, v20.x, v22.x and v23.x. Impact: Thank you, to newtmitch for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2025-23085)

- With the aid of the diagnostics_channel utility, an event can be hooked into whenever a worker thread is created. This is not limited only to workers but also exposes internal workers, where an instance of them can be fetched, and its constructor can be grabbed and reinstated for malicious usage. This vulnerability affects Permission Model users (--permission) on Node.js v20, v22, and v23. Impact: Thank you, to leodog896 for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2025-23083)

- A vulnerability has been identified in Node.js, specifically affecting the handling of drive names in the Windows environment. Certain Node.js functions do not treat drive names as special on Windows. As a result, although Node.js assumes a relative path, it actually refers to the root directory. On Windows, a path that does not start with the file separator is treated as relative to the current directory. This vulnerability affects Windows users of path.join API. Impact: Thank you, to taise for reporting this vulnerability and thank you tniessen for fixing it. (CVE-2025-23084)

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

See Also

http://www.nessus.org/u?68bc9901

Solution

Upgrade to Node.js version 18.20.6 / 20.18.2 / 22.13.1 / 23.6.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.0006

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)

STIG Severity

I

References

CVE	CVE-2025-23083
CVE	CVE-2025-23084
CVE	CVE-2025-23085
XREF	IAVB:2025-B-0012-S

Plugin Information

Published: 2025/01/21, Modified: 2025/05/16

Plugin Output

tcp/0

```
Path              : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version     : 20.18.2
```

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

```
Path              : /usr/lib/jvm/java-17-openjdk-amd64/
Installed version : 17.0.14
Fixed version     : Upgrade to a version greater than 17.0.14
```

192974 - OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.6. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.1.6 advisory.

- Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary:

Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (`p` parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable. Also vulnerable are the OpenSSL pkey and pkeyparam command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2024-4603)

- Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

(CVE-2024-2511)

- Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware

of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Found by William Ahern (Akamai). Fix developed by Matt Caswell. Fix developed by Watson Ladd (Akamai). Fixed in OpenSSL 3.3.1 (Affected since 3.3.0). (CVE-2024-4741)

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

See Also

http://www.nessus.org/u?5ee92eab

http://www.nessus.org/u?6f15218c

http://www.nessus.org/u?f40bd907

https://www.cve.org/CVERecord?id=CVE-2024-2511

https://www.cve.org/CVERecord?id=CVE-2024-4603

https://www.cve.org/CVERecord?id=CVE-2024-4741

Solution

Upgrade to OpenSSL version 3.1.6 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0165

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-2511
CVE	CVE-2024-4603
CVE	CVE-2024-4741
XREF	IAVA:2024-A-0208-S

Plugin Information

Published: 2024/04/08, Modified: 2024/11/14

Plugin Output

tcp/0

```
Path              : /usr/lib/x86_64-linux-gnu/ruby/3.1.0/openssl.so
Reported version : 3.1.5
Fixed version     : 3.1.6
```

205594 - PostgreSQL 12.x < 12.20 / 13.x < 13.16 / 14.x < 14.13 / 15.x < 15.8 / 16.x 16.4 SQL Injection<

Synopsis

The remote database server is affected by an SQL injection vulnerability

Description

The version of PostgreSQL installed on the remote host is 12 prior to 12.20, 13 prior to 13.16, 14 prior to 14.13, 15 prior to 15.8, or 16 prior to 16.4. As such, it is potentially affected by a vulnerability :

- Time-of-check Time-of-use (TOCTOU) race condition in pg_dump in PostgreSQL allows an object creator to execute arbitrary SQL functions as the user running pg_dump, which is often a superuser. The attack involves replacing another relation type with a view or foreign table. The attack requires waiting for pg_dump to start, but winning the race condition is trivial if the attacker retains an open transaction.

Versions before PostgreSQL 16.4, 15.8, 14.13, 13.16, and 12.20 are affected. (CVE-2024-7348)

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

See Also

http://www.nessus.org/u?6be9d6bf

http://www.nessus.org/u?5cdbab17

Solution

Upgrade to PostgreSQL 12.20 / 13.16 / 14.13 / 15.8 / 16.4 or later

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0026

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-7348
XREF	IAVB:2024-B-0117-S

Plugin Information

Published: 2024/08/15, Modified: 2025/05/29

Plugin Output

tcp/0

```
Path              : /usr/lib/postgresql/16/bin/postgres
Installed version : 16.3
Fixed version     : 16.4
```

211655 - PostgreSQL 12.x < 12.21 / 13.x < 13.17 / 14.x < 14.14 / 15.x < 15.9 / 16.x < 16.5 / 17.x < 17.1 Multiple Vulnerabilities

Synopsis

The remote database server is affected by multiple vulnerabilities

Description

The version of PostgreSQL installed on the remote host is 12 prior to 12.21, 13 prior to 13.17, 14 prior to 14.14, 15 prior to 15.9, 16 prior to 16.5, or 17 prior to 17.1. As such, it is potentially affected by multiple vulnerabilities :

- Incorrect control of environment variables in PostgreSQL PL/Perl allows an unprivileged database user to change sensitive process environment variables (e.g. PATH). That often suffices to enable arbitrary code execution, even if the attacker lacks a database server operating system user. (CVE-2024-10979)

- Incorrect privilege assignment in PostgreSQL allows a less-privileged application user to view or change different rows from those intended. An attack requires the application to use SET ROLE, SET SESSION AUTHORIZATION, or an equivalent feature. The problem arises when an application query uses parameters from the attacker or conveys query results to the attacker. If that query reacts to current_setting('role') or the current user ID, it may modify or return data as though the session had not used SET ROLE or SET SESSION AUTHORIZATION. The attacker does not control which incorrect user ID applies. Query text from less-privileged sources is not a concern here, because SET ROLE and SET SESSION AUTHORIZATION are not sandboxes for unvetted queries. (CVE-2024-10978)

- Client use of server error message in PostgreSQL allows a server not trusted under current SSL or GSS settings to furnish arbitrary non-NUL bytes to the libpq application. For example, a man-in-the-middle attacker could send a long error message that a human or screen-scraper user of psql mistakes for valid query results. This is probably not a concern for clients where the user interface unambiguously indicates the boundary between one error message and other text. (CVE-2024-10977)

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

See Also

http://www.nessus.org/u?e9644dd1

Solution

Upgrade to PostgreSQL 13.17 / 14.14 / 15.9 / 16.5 / 17.1 or later

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.014

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-10976
CVE	CVE-2024-10977
CVE	CVE-2024-10978
CVE	CVE-2024-10979
XREF	IAVB:2024-B-0175-S

Plugin Information

Published: 2024/11/20, Modified: 2025/05/29

Plugin Output

tcp/0

```
Path              : /usr/lib/postgresql/16/bin/postgres
Installed version : 16.3
Fixed version     : 16.5
```

216586 - PostgreSQL 13.x < 13.19 / 14.x < 14.16 / 15.x < 15.11 / 16.x < 16.7 / 17.x < 17.3 SQLi

Synopsis

The remote database server is affected by a vulnerability

Description

The version of PostgreSQL installed on the remote host is 13 prior to 13.19, 14 prior to 14.16, 15 prior to 15.11, 16 prior to 16.7, or 17 prior to 17.3. As such, it is potentially affected by a vulnerability :

- Improper neutralization of quoting syntax in PostgreSQL libpq functions PQescapeLiteral(), PQescapeIdentifier(), PQescapeString(), and PQescapeStringConn() allows a database input provider to achieve SQL injection in certain usage patterns. Specifically, SQL injection requires the application to use the function result to construct input to psql, the PostgreSQL interactive terminal. Similarly, improper neutralization of quoting syntax in PostgreSQL command line utility programs allows a source of command line arguments to achieve SQL injection when client_encoding is BIG5 and server_encoding is one of EUC_TW or MULE_INTERNAL. Versions before PostgreSQL 17.3, 16.7, 15.11, 14.16, and 13.19 are affected.

(CVE-2025-1094)

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

See Also

http://www.nessus.org/u?2a3cbcdf

Solution

Upgrade to PostgreSQL 13.19 / 14.16 / 15.11 / 16.7 / 17.3 or later

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.5

EPSS Score

0.8202

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-1094
XREF	IAVB:2025-B-0028-S

Exploitable With

Metasploit (true)

Plugin Information

Published: 2025/02/21, Modified: 2025/05/16

Plugin Output

tcp/0

```
Path              : /usr/lib/postgresql/16/bin/postgres
Installed version : 16.3
Fixed version     : 16.7
```

237199 - Python Library Tornado 6.5.0 DoS

Synopsis

A Python library installed on the remote host is affected by a DoS vulnerability.

Description

The detected version of the Tornado Python package, Tornado, is prior to 6.4.2.

It is therefore affected by a DoS vulnerability that happens When Tornado's multipart/form-data parser encounters certain errors, it logs a warning but continues trying to parse the remainder of the data. This allows remote attackers to generate an extremely high volume of logs, constituting a DoS attack. This DoS is compounded by the fact that the logging subsystem is synchronous.:

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

See Also

http://www.nessus.org/u?5105fc6c

Solution

Upgrade to Tornado version 6.5.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

VPR Score

4.4

EPSS Score

0.001

CVSS v2.0 Base Score

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

STIG Severity

I

References

CVE	CVE-2025-47287

Plugin Information

Published: 2025/05/23, Modified: 2025/05/23

Plugin Output

tcp/0

```
Path              : /usr/lib/python3/dist-packages/tornado-6.4.2.egg-info
Installed version : 6.4.2
Fixed version     : 6.5.0
```

237584 - Curl 8.5.0 < 8.14.0 Improper Certificate Validation (CVE-2025-5025)

Synopsis

The remote host has a program that is affected by a Improper Certificate Validation vulnerability.

Description

The version of Curl installed on the remote host is is missing security update. It is, therefore, affected by a improper certificate validation vulnerability.

- libcurl supports *pinning* of the server certificate public key for HTTPS transfers. Due to an omission, this check is not performed when connecting with QUIC for HTTP/3, when the TLS backend is wolfSSL. Documentation says the option works with wolfSSL, failing to specify that it does not for QUIC and HTTP/3. Since pinning makes the transfer succeed if the pin is fine, users could unwittingly connect to an impostor server without noticing. (CVE-2025-5025)

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://curl.se/docs/CVE-2025-5025.html

Solution

Upgrade Curl to version 8.14.0 or later

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)

VPR Score

4.4

EPSS Score

0.0001

CVSS v2.0 Base Score

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

STIG Severity

I

References

CVE	CVE-2025-5025
XREF	IAVA:2025-A-0379

Plugin Information

Published: 2025/05/30, Modified: 2025/05/30

Plugin Output

tcp/0

```
Path              : /usr/bin/curl
Installed version : 8.13.0
Fixed version     : 8.14.0
```

237583 - Curl 8.8.0 < 8.14.0 Improper Certificate Validation (CVE-2025-4947)

Synopsis

The remote host has a program that is affected by a improper certificate validation vulnerability.

Description

The version of Curl installed on the remote host is is missing security update. It is, therefore, affected by a improper certificate validation vulnerability.

- libcurl accidentally skips the certificate verification for QUIC connections when connecting to a host specified as an IP address in the URL. Therefore, it does not detect impostors or man-in-the-middle attacks. (CVE-2025-4947)

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://curl.se/docs/CVE-2025-4947.html

Solution

Upgrade Curl to version 8.14.0 or later

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)

VPR Score

2.5

EPSS Score

0.0001

CVSS v2.0 Base Score

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

STIG Severity

I

References

CVE	CVE-2025-4947
XREF	IAVA:2025-A-0379

Plugin Information

Published: 2025/05/30, Modified: 2025/05/30

Plugin Output

tcp/0

```
Path              : /usr/bin/curl
Installed version : 8.13.0
Fixed version     : 8.14.0
```

197900 - Intel Media SDK Multiple Vulnerabilities (INTEL-SA-00935)

Synopsis

The version of Intel Media SDK installed on the remote host is affected by multiple vulnerabilities.

Description

The version of Intel Media SDK installed on the remote host is affected by multiple vulnerabilities:

- Improper input validation in Intel Media SDK software all versions may allow an authenticated user to potentially enable denial of service via local access. (CVE-2023-48368)

- Improper buffer restrictions in Intel Media SDK all versions may allow an authenticated user to potentially enable escalation of privilege via local access. (CVE-2023-45221)

- Out-of-bounds read in Intel Media SDK and some Intel oneVPL software before version 23.3.5 may allow an authenticated user to potentially enable escalation of privilege via local access. (CVE-2023-22656)

- Out-of-bounds write in Intel Media SDK all versions and some Intel oneVPL software before version 23.3.5 may allow an authenticated user to potentially enable escalation of privilege via local access. (CVE-2023-47282)

- Improper buffer restrictions in Intel Media SDK software all versions may allow an authenticated user to potentially enable denial of service via local access. (CVE-2023-47169)

Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?c8710b2e

Solution

Intel has issued a Product Discontinuation notice for Intel Media SDK software and recommends that users of the Intel Media SDK software uninstall it or discontinue use at their earliest convenience.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2023-48368
CVE	CVE-2023-45221
CVE	CVE-2023-22656
CVE	CVE-2023-47282
CVE	CVE-2023-47169
XREF	IAVB:2024-B-0064

Plugin Information

Published: 2024/05/24, Modified: 2024/05/27

Plugin Output

tcp/0

```
Path              : /usr/lib/x86_64-linux-gnu/libmfxhw64.so.1.35
Installed version : 22.5.4
Fixed version     : None
```

236766 - Node.js 20.x < 20.19.2 / 22.x < 22.15.1 / 22.x < 22.15.1 / 23.x < 23.11.1 / 24.x < 24.0.2 Multiple Vulnerabilities (Wednesday, May 14, 2025 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 20.19.2, 22.15.1, 22.15.1, 23.11.1, 24.0.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday, May 14, 2025 Security Releases advisory.

- In Node.js, the ReadFileUtf8 internal binding leaks memory due to a corrupted pointer in uv_fs_s.file: a UTF-16 path buffer is allocated but subsequently overwritten when the file descriptor is set. This results in an unrecoverable memory leak on every call. Repeated use can cause unbounded memory growth, leading to a denial of service. Impact: Thank you, to Justin Nietzel for reporting and fixing this vulnerability.

(CVE-2025-23165)

- The C++ method SignTraits::DeriveBits() may incorrectly call ThrowException() based on user-supplied inputs when executing in a background thread, crashing the Node.js process. Such cryptographic operations are commonly applied to untrusted inputs. Thus, this mechanism potentially allows an adversary to remotely crash a Node.js runtime. Impact: Thank you, @panva and @tniessen, for reporting and fixing this vulnerability. (CVE-2025-23166)

- A flaw in Node.js 20's HTTP parser allows improper termination of HTTP/1 headers using \r \rX instead of the required \r \r . This inconsistency enables request smuggling, allowing attackers to bypass proxy- based access controls and submit unauthorized requests. The issue was resolved by upgrading llhttp to version 9, which enforces correct header termination. Impact: Thank you, to kenballus for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2025-23167)

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://nodejs.org/en/blog/vulnerability/may-2025-security-releases/

Solution

Upgrade to Node.js version 20.19.2 / 22.15.1 / 22.15.1 / 23.11.1 / 24.0.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.1

EPSS Score

0.0004

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)

STIG Severity

I

References

CVE	CVE-2025-23165
CVE	CVE-2025-23166
CVE	CVE-2025-23167
XREF	IAVB:2025-B-0079

Plugin Information

Published: 2025/05/15, Modified: 2025/05/16

Plugin Output

tcp/0

```
Path              : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version     : 20.19.2
```

209154 - OpenSSL 3.1.0 < 3.1.8 Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 3.1.8. It is, therefore, affected by a vulnerability as referenced in the 3.1.8 advisory.

- Issue summary: Use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes. Impact summary: Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only named curves are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary (GF(2^m)) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low. In particular, the X9.62 encoding is used for ECC keys in X.509 certificates, so problematic inputs cannot occur in the context of processing X.509 certificates. Any problematic use-cases would have to be using an exotic curve encoding. The affected APIs include:

EC_GROUP_new_curve_GF2m(), EC_GROUP_new_from_params(), and various supporting BN_GF2m_*() functions.

Applications working with exotic explicit binary (GF(2^m)) curve parameters, that make it possible to represent invalid field polynomials with a zero constant term, via the above or similar APIs, may terminate abruptly as a result of reading or writing outside of array bounds. Remote code execution cannot easily be ruled out. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.

(CVE-2024-9143)

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

See Also

http://www.nessus.org/u?5f636435

https://openssl-library.org/news/secadv/20241016.txt

https://openssl-library.org/policies/general/security-policy/#low

https://www.cve.org/CVERecord?id=CVE-2024-9143

Solution

Upgrade to OpenSSL version 3.1.8 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.2

EPSS Score

0.0036

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-9143
XREF	IAVA:2025-A-0127-S

Plugin Information

Published: 2024/10/16, Modified: 2025/05/23

Plugin Output

tcp/0

```
Path              : /usr/lib/x86_64-linux-gnu/ruby/3.1.0/openssl.so
Reported version : 3.1.5
Fixed version     : 3.1.8
```

237112 - OpenSSL 3.5.0 < 3.5.1 Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 3.5.1. It is, therefore, affected by a vulnerability as referenced in the 3.5.1 advisory.

- Issue summary: Use of -addreject option with the openssl x509 application adds a trusted use instead of a rejected use for a certificate. Impact summary: If a user intends to make a trusted certificate rejected for a particular use it will be instead marked as trusted for that use. A copy & paste error during minor refactoring of the code introduced this issue in the OpenSSL 3.5 version. If, for example, a trusted CA certificate should be trusted only for the purpose of authenticating TLS servers but not for CMS signature verification and the CMS signature verification is intended to be marked as rejected with the -addreject option, the resulting CA certificate will be trusted for CMS signature verification purpose instead. Only users which use the trusted certificate format who use the openssl x509 command line application to add rejected uses are affected by this issue. The issues affecting only the command line application are considered to be Low severity. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 3.4, 3.3, 3.2, 3.1, 3.0, 1.1.1 and 1.0.2 are also not affected by this issue.

(CVE-2025-4575)

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

See Also

http://www.nessus.org/u?71c5cf95

https://openssl-library.org/news/secadv/20250522.txt

http://www.nessus.org/u?eac4598c

https://www.cve.org/CVERecord?id=CVE-2025-4575

Solution

Upgrade to OpenSSL version 3.5.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.3

EPSS Score

0.0002

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2025-4575
XREF	IAVA:2025-A-0378

Plugin Information

Published: 2025/05/22, Modified: 2025/05/30

Plugin Output

tcp/0

```
Path              : /usr/bin/openssl
Reported version : 3.5.0
Fixed version     : 3.5.1
```

tcp/0

```
Path              : /usr/lib/x86_64-linux-gnu/libcrypto.so.3
Reported version : 3.5.0
Fixed version     : 3.5.1
```

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

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

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

182210 - OpenSSL SEoL (3.1.x)

Synopsis

An unsupported version of OpenSSL is installed on the remote host.

Description

According to its version, OpenSSL is 3.1.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

See Also

https://www.openssl.org/policies/releasestrat.html

https://www.openssl.org/news/vulnerabilities-3.1.html

Solution

Upgrade to a version of OpenSSL that is currently supported.

Risk Factor

Low

Plugin Information

Published: 2023/09/29, Modified: 2024/10/07

Plugin Output

tcp/0

```
Path                                  : /usr/lib/x86_64-linux-gnu/ruby/3.1.0/openssl.so
Installed version                     : 3.1.5
Security End of Life                  : March 14, 2025
Time since Security End of Life (Est.) : >= 1 month
```

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: 2025/05/28

Plugin Output

tcp/0

```
Path    : /usr/sbin/apache2
Version : 2.4.63
Running : no

Configs found :
  - /etc/apache2/apache2.conf

Loaded modules :
  - libphp8.2
  - mod_access_compat
  - mod_alias
  - mod_auth_basic
  - mod_authn_core
  - mod_authn_file
  - mod_authz_core
  - mod_authz_host
  - mod_authz_user
  - mod_autoindex
```

```
      - mod_deflate
      - mod_dir
      - mod_env
      - mod_filter
      - mod_mime
      - mod_mpm_prefork
      - mod_negotiation
      - mod_reqtimeout
      - mod_setenvif
      - mod_status
```

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

```
Sites and configs present in /usr/sbin/apache2 Apache installation:
  - following sites are present in /etc/apache2/apache2.conf Apache config file:
    +  - *:80
```

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:2.4.63 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:exiv2:exiv2:0.27.6 -> Exiv2
  cpe:/a:exiv2:libexiv2:0.27.6
  cpe:/a:exiv2:libexiv2:3.1
  cpe:/a:gnupg:libgcrypt:1.11.0 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:8.13.0 -> Haxx Curl
  cpe:/a:haxx:libcurl:8.13.0 -> 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:nodejs:node.js:20.11.0 -> Nodejs Node.js
  cpe:/a:numpy:numpy:1.26.4 -> NumPy
```

```
cpe:/a:openssl:openssl:3.0.15 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:3.1.5 -> 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:2.6.14 -> OpenVPN
cpe:/a:oracle:openjdk:17.0.14 -> Oracle OpenJDK -
cpe:/a:oracle:openjdk:21.0.7 -> Oracle OpenJDK -
cpe:/a:oracle:openjdk:23.0.2 -> Oracle OpenJDK -
cpe:/a:php:php:8.2.21 -> PHP PHP
cpe:/a:postgresql:postgresql:16.3 -> PostgreSQL
cpe:/a:postgresql:postgresql:17.5 -> PostgreSQL
cpe:/a:ruby-lang:ruby:3.3.8 -> 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:tornadoweb:tornado:6.4.2 -> Tornado Web Server Tornado
cpe:/a:tukaani:xz:5.8.1 -> Tukaani XZ
cpe:/a:vim:vim:9.1 -> Vim
cpe:/a:vmware:open_vm_tools:12.5.0 -> VMware Open VM Tools
x-cpe:/a:intel:media_sdk:22.5.4
x-cpe:/a:java:jre:17.0.14
x-cpe:/a:java:jre:21.0.7
x-cpe:/a:java:jre:23.0.2
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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of Curl:

  Path          : curl 8.13.0-5 (via package manager)
  Version       : 8.13.0
  Managed by OS : True

  Path    : /usr/bin/curl
  Version : 8.13.0
```

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: 2025/05/27

Plugin Output

tcp/0

```
Hostname : kali
  kali (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: 2025/05/28

Plugin Output

tcp/0

```
Dockerfiles found: 3
 - /usr/share/metasploit-framework/tools/payloads/ysoserial/Dockerfile
 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/net-ssh-7.3.0/Dockerfile
 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/puma-6.6.0/tools/Dockerfile
```

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 :

 - 192.168.110.165 (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 :

 - fe80::83b9:22c4:f7bc:466b (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

```
The following MAC address exists on the remote host :

  - 00:0c:29:55:87:47 (interface eth0)
```

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

```
lo:
  IPv4:
    - Address : 127.0.0.1
      Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
      Prefixlen : 128
      Scope : host
      ScopeID : 0x10
eth0:
  MAC : 00:0c:29:55:87:47
  IPv4:
    - Address : 192.168.110.165
      Netmask : 255.255.255.0
      Broadcast : 192.168.110.255
  IPv6:
    - Address : fe80::83b9:22c4:f7bc:466b
      Prefixlen : 64
      Scope : link
      ScopeID : 0x20
```

179200 - Enumerate the Network Routing configuration via SSH

Synopsis

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

Plugin Output

tcp/0

```
Gateway Routes:
  eth0:
    ipv4_gateways:
      192.168.110.2:
        subnets:
         - 0.0.0.0/0
Interface Routes:
  eth0:
    ipv4_subnets:
     - 192.168.110.0/24
    ipv6_subnets:
     - fe80::/64
```

168980 - Enumerate the PATH Variables

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/05/28

Plugin Output

tcp/0

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

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

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:0C:29:55:87:47 : VMware, Inc.
```

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

```
The following is a consolidated list of detected MAC addresses:
  - 00:0C:29:55:87:47
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of Exiv2:

  Path    : /usr/bin/exiv2
  Version : 0.27.6

  Path          : exiv2 0.27.6-1 (via package manager)
  Version       : 0.27.6
  Managed by OS : True
```

168982 - Filepaths contain Dangerous characters (Linux)

Synopsis

This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential.

Description

This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential. Although almost any character is valid for an entry in this kind of filesystem, such as semicolons, use of some of them may lead to problems or security compromise when used in further commands.

This product has chosen in certain plugins to avoid digging within those files and directories for security reasons.

These should be renamed to avoid security compromise.

Solution

Rename these files or folders to not include dangerous characters.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2024/07/24

Plugin Output

tcp/22

```
The following files and directories contain potentially dangerous characters such as brackets,
 ampersand, or semicolon.
This scanner avoided access to these files when possible for safety:

xz-utils 5.8.1-1 (via package manager)
```

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: Sat, 31 May 2025 15:46:22 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: 2025/05/27

Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ eth0
  + IPv4
    - Address       : 192.168.110.165
      Assign Method : dynamic
  + IPv6
    - Address       : fe80::83b9:22c4:f7bc:466b
      Assign Method : static
```

197894 - Intel Media SDK Installed (Linux)

Synopsis

Intel Media SDK is installed on the remote Linux host.

Description

Intel Media SDK is installed on the remote Linux host.

See Also

https://github.com/Intel-Media-SDK/MediaSDK

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/05/24, Modified: 2025/05/28

Plugin Output

tcp/0

```
Path    : /usr/lib/x86_64-linux-gnu/libmfxhw64.so.1.35
Version : 22.5.4
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 3 installs of Java:

  Path             : /usr/lib/jvm/java-17-openjdk-amd64/
  Version          : 17.0.14
  Application      : OpenJDK Java
  Binary Location  : /usr/lib/jvm/java-17-openjdk-amd64/bin/java
  Details          : This Java install appears to be OpenJDK due to the install directory
                     name (high confidence).
  Detection Method : "find" utility
```

```
Path             : /usr/lib/jvm/java-21-openjdk-amd64/
Version          : 21.0.7
Application      : OpenJDK Java
Binary Location  : /usr/lib/jvm/java-21-openjdk-amd64/bin/java
Details          : This Java install appears to be OpenJDK due to the install directory
                   name (high confidence).
Detection Method : "find" utility

Path             : /usr/lib/jvm/java-23-openjdk-amd64/
Version          : 23.0.2
Application      : OpenJDK Java
Binary Location  : /usr/lib/jvm/java-23-openjdk-amd64/bin/java
Details          : This Java install appears to be OpenJDK due to the install directory
                   name (high confidence).
Detection Method : "find" utility
```

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: 2025/05/28

Plugin Output

tcp/0

```
Path    : /usr/share/perl5/Spreadsheet/ParseExcel.pm
Version : 0.66
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 4 installs of Libgcrypt:

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.11.0

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.5.0
  Version : 1.11.0

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.11.0

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20.5.0
  Version : 1.11.0
```

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: 2025/05/28

Plugin Output

tcp/0

```
Path          : libndp0 1.9-1 (via package manager)
Version       : 1.9
Managed by OS : True
```

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

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            917M     0  917M   0% /dev
tmpfs           197M  1.3M  196M   1% /run
/dev/sda1        79G   31G   44G  42% /
tmpfs           983M  4.0K  983M   1% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-journald.service
tmpfs           983M   96K  983M   1% /tmp
tmpfs           1.0M     0  1.0M   0% /run/credentials/getty@tty1.service
tmpfs           197M  132K  197M   1% /run/user/0


$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0 80.1G  0 disk
##sda1   8:1    0 80.1G  0 part /


$ mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=938056k,nr_inodes=234514,mode=755,inode64)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=600,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=201168k,mode=755,inode64)
```

```
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro) [root]
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
cgroup2 on /sys/fs/cgroup type cgroup2
 (rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
 (rw,relatime,fd=40,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=632)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k,inode64)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /run/credentials/systemd-journald.service type tmpfs
 (ro,nosuid,nodev,noexec,relatime,nosymfollow,size=1 [...]
```

193143 - Linux Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Via date: IST +0530
Via timedatectl: Time zone: Asia/Kolkata (IST, +0530)
Via /etc/timezone: Asia/Kolkata
Via /etc/localtime: IST-5:30
```

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

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

User         : kali
Home folder  : /home/kali
Start script : /usr/bin/zsh
Groups       : kali
               dip
               scanner
               netdev
               users
               dialout
               wireshark
               video
               cdrom
               adm
               audio
               sudo
               kaboxer
               bluetooth
               plugdev
               floppy

----------[ System Accounts ]----------

User         : root
Home folder  : /root
Start script : /usr/bin/zsh
Groups       : root
```

```
User         : daemon
Home folder  : /usr/sbin
Start script : /usr/sbin/nologin
Groups       : daemon

User         : bin
Home folder  : /bin
Start script : /usr/sbin/nologin
Groups       : bin

User         : sys
Home folder  : /dev
Start script : /usr/sbin/nologin
Groups       : sys

User         : sync
Home folder  : /bin
Start script : /bin/sync
Groups       : nogroup

User         : games
Home folder  : /usr/games
Start script : /usr/sbin/nologin
Groups       : games

User         : man
Home folder  : /var/cache/man
Start script : /usr/sbin/nologin
Groups       : man

User         : lp
Home folder  : /var/spool/lpd
Start script : /usr/sbin/nologin
Groups       : lp

User         : mail
Home folder  : /var/mail
Start script : /usr/sbin/nologin
Groups       : mail

User         : news
Home folder  : /var/spool/news
Start script : /usr/sbin/nologin
Groups       : news

User         : uucp
Home folder  : /var/spool/uucp
Start script : /usr/sbin/nologin
Groups       : uucp

User         : proxy
Home folder  : /bin
Start script : /usr/sbin/nologin
Groups       : proxy

User         : www-data
Home folder  : /var/www
Start script : /usr/sbin/nologin
Groups       : www-data

User         : backup
Home folder  : /var/backups
Start script : /usr/sbin/nologin
Groups       : backup

User         : list
Home folder  : /var/list
Start script : /usr/sbin/nologin
Groups       : list
```

```
User         : irc
Home folder  : /run/ircd
Start script  [...]
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/05/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.4
Nessus build : 20028
Plugin feed version : 202505310604
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.110.165
Ping RTT : Unavailable
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes (on the localhost)
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/5/31 21:14 IST (UTC +05:30)
Scan duration : 2143 sec
Scan for malware : no
```

10147 - Nessus Server Detection

Synopsis

A Nessus daemon is listening on the remote port.

Description

A Nessus daemon is listening on the remote port.

See Also

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

Solution

Ensure that the remote Nessus installation has been authorized.

Risk Factor

None

References

XREF IAVT:0001-T-0673

Plugin Information

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

Plugin Output

tcp/8834/www

```
URL     : https://192.168.110.165:8834/
Version : unknown
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/8834/www

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

178771 - Node.js Installed (Linux / UNIX)

Synopsis

Node.js is installed on the remote Linux / UNIX host.

Description

Node.js is installed on the remote Linux / UNIX host.

See Also

https://nodejs.org

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/07/25, Modified: 2025/05/28

Plugin Output

tcp/0

```
Path    : /usr/lib/python3/dist-packages/playwright/driver/node
Version : 20.11.0
```

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 6.12.13-amd64
Confidence level : 99
Method : uname
Type : general-purpose
Fingerprint : uname:Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11)
 x86_64 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:kalis/O:Nessus Users Uniteds/OU:Nessus Server
a485a5cd5e6744ad40eeab99d308301ba6c19a24
```

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: 2025/05/09

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 6.12.13-amd64
Confidence level : 99
Method : uname


The remote host is running Linux Kernel 6.12.13-amd64
```

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 kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64 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 : 6.671268 seconds
```

117887 - OS Security Patch Assessment Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0516

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
OS Security Patch Assessment is available.

Protocol : LOCAL
```

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

```
Path            : /usr/lib/jvm/java-17-openjdk-amd64/
Version         : 17.0.14
Binary Location : /usr/lib/jvm/java-17-openjdk-amd64/bin/java
```

tcp/0

```
Path            : /usr/lib/jvm/java-21-openjdk-amd64/
Version         : 21.0.7
Binary Location : /usr/lib/jvm/java-21-openjdk-amd64/bin/java
```

tcp/0

```
Path            : /usr/lib/jvm/java-23-openjdk-amd64/
Version         : 23.0.2
Binary Location : /usr/lib/jvm/java-23-openjdk-amd64/bin/java
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 6 installs of OpenSSL:

  Path               : /opt/nessus/bin/openssl
  Version            : 3.0.15
  Associated Package : nessus

  Path    : /usr/lib/x86_64-linux-gnu/ruby/3.3.0/openssl.so
  Version : 3.4.0

  Path    : /usr/lib/x86_64-linux-gnu/ruby/3.1.0/openssl.so
  Version : 3.1.5
```

```
  Path    : /usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Version : 3.5.0

  Path          : openssl 3.5.0-1 (via package manager)
  Version       : 3.5.0
  Managed by OS : True

  Path    : /usr/bin/openssl
  Version : 3.5.0

We are unable to retrieve version info from the following list of OpenSSL files. However, these
 installs may include their version within the filename or the filename of the Associated Package.

e.g. libssl.so.3 (OpenSSL 3.x), libssl.so.1.1 (OpenSSL 1.1.x)

/usr/lib/x86_64-linux-gnu/libssl.so.3
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of OpenVPN:

  Path           : openvpn 2.6.14-1 (via package manager)
  Version        : 2.6.14
  Managed by OS : True

  Path    : /usr/sbin/openvpn
  Version : 2.6.14
```

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: 2025/05/28

Plugin Output

tcp/0

```
Path       : /usr/bin/php8.2
Version    : 8.2.21
INI file   : /etc/php/8.2/cli/php.ini
INI source : PHP binary grep
```

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: 2025/05/07

Plugin Output

tcp/0

```
Successfully retrieved and stored package data.
```

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: 2025/05/13

Plugin Output

tcp/0

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

[ Curl 8.5.0 < 8.14.0 Improper Certificate Validation (CVE-2025-5025) (237584) ]

+ Action to take : Upgrade Curl to version 8.14.0 or later

[ Curl 8.8.0 < 8.14.0 Improper Certificate Validation (CVE-2025-4947) (237583) ]

+ Action to take : Upgrade Curl to version 8.14.0 or later

[ Node.js 20.x < 20.19.2 / 22.x < 22.15.1 / 22.x < 22.15.1 / 23.x < 23.11.1 / 24.x < 24.0.2 Multiple
 Vulnerabilities (Wednesday, May 14, 2025 Security Releases). (236766) ]

+ Action to take : Upgrade to Node.js version 20.19.2 / 22.15.1 / 22.15.1 / 23.11.1 / 24.0.2 or
 later.

+Impact : Taking this action will resolve 21 different vulnerabilities (CVEs).

[ 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) (234472) ]
```

```
+ Action to take : Upgrade to an OpenJDK version greater than 8u442 / 11.0.26 / 17.0.14 / 21.0.6 /
 24.0.0

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ OpenSSL 3.5.0 < 3.5.1 Vulnerability (237112) ]

+ Action to take : Upgrade to OpenSSL version 3.5.1 or later.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).


[ PostgreSQL 13.x < 13.19 / 14.x < 14.16 / 15.x < 15.11 / 16.x < 16.7 / 17.x < 17.3 SQLi (216586) ]

+ Action to take : Upgrade to PostgreSQL 13.19 / 14.16 / 15.11 / 16.7 / 17.3 or later

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).


[ Python Library Tornado 6.5.0 DoS (237199) ]

+ Action to take : Upgrade to Tornado version 6.5.0 or later.
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of PostgreSQL client:

  Path    : /usr/lib/postgresql/17/bin/psql
  Version : 17.5

  Path    : /usr/lib/postgresql/16/bin/psql
  Version : 16.3
```

tcp/0

```
Nessus detected 2 installs of PostgreSQL:

  Path    : /usr/lib/postgresql/17/bin/postgres
  Version : 17.5

  Path    : /usr/lib/postgresql/16/bin/postgres
  Version : 16.3
```

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: 2025/05/28

Plugin Output

tcp/0

```
Path          : package: ruby3.3  3.3.8-2
Version       : 3.3.8
Managed by OS : True
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of SQLite:

  Path    : /usr/bin/sqlite3
  Version : unknown

  Path    : /bin/sqlite3
  Version : unknown
```

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

```
Subject Name:

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

Issuer Name:

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

Serial Number: 00 EF 6F

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 30 17:52:53 2025 GMT
Not Valid After: May 29 17:52:53 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A9 50 C8 74 E9 D2 DE 44 70 66 B7 98 E6 13 C2 FB 6C 93 3B
```

```
             30 72 97 47 24 1A 13 B5 41 D5 BD DA 96 88 03 1E BE 19 10 60
             09 6F 69 AA 93 31 73 D8 2C 77 2C 4D 28 C3 A2 21 42 4F 0F EB
             4A 08 54 86 BC 6D 03 E2 63 21 69 7C 61 BD CC 6A 80 A3 A1 50
             08 81 10 8C B3 C5 9F 9D F4 5E 3A C9 B5 FD F8 5D ED C0 0B 23
             4B 19 1B 38 E2 DD 96 D8 A4 1B F2 A9 B7 46 2A 08 03 DE D7 15
             9A 99 3A CD C5 67 B2 98 63 B2 09 16 CC DF A7 8B 02 F9 4A 2E
             63 AA CA 49 6B D2 2C A4 F5 9A 1D 2C 1B 77 04 5C C5 0B 69 35
             C0 61 A9 61 DA 51 D7 62 34 A1 B1 49 14 45 1D F7 9A 9E 87 66
             A4 27 DC B1 1B FD 17 EA 2D 6D 82 04 B1 67 A6 15 AB 02 1C 43
             2E 00 8A 2C 01 AD 71 F2 77 95 5A C3 91 EB 7C A7 55 46 B7 EE
             6E 5C 4A 87 A1 0C 97 68 78 3A 9C F2 50 A4 F2 90 73 B0 CF 3C
             AD E3 75 CF DC FD CB 61 B1 0D BE C5 5E 69 24 21 19
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 16 49 6C A0 EF 9D 31 24 73 CA C8 1E CE 27 E5 C4 6C 4B C6
           36 F8 49 82 A6 8C F4 F4 C3 4F 35 EF FF 15 65 E0 50 7D 8E 97
           70 9E DB 4E F0 8C 37 BB B0 BF D8 8C 81 32 49 74 6F AD 38 DC
           7F BD 5A 08 D0 B5 B0 58 CD 8F 66 1B EF 9C 88 F0 69 49 02 19
           DB 7D 70 12 ED 69 49 0A E7 E1 1D 2B 50 DC 8E 28 12 74 00 C6
           C5 30 34 10 81 61 38 C7 61 F6 74 57 E3 3D BF 59 A9 0C 8E 13
           2C 8F 2D 73 8B 69  [...]
```

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

```
Here is the list of packages installed on the remote Debian Linux system :

  ii   7zip  24.09+dfsg-7  amd64  7-Zip file archiver with a high compression ratio
  ii   accountsservice  23.13.9-7  amd64  query and manipulate user account information
  ii   acl  2.3.2-2+b1  amd64  access control list - utilities
  ii   adduser  3.152  all  add and remove users and groups
  ii   adwaita-icon-theme  48.0-1  all  default icon theme of GNOME
  ii   aircrack-ng  1:1.7+git20230807.4bf83f1a-2  amd64  wireless WEP/WPA cracking utilities
  ii   alsa-topology-conf  1.2.5.1-3  all  ALSA topology configuration files
  ii   alsa-ucm-conf  1.2.14-1  all  ALSA Use Case Manager configuration files
  ii   amass  4.2.0-0kali1  amd64  In-depth DNS Enumeration and Network Mapping
  ii   amass-common  4.2.0-0kali1  all  In-depth DNS Enumeration and Network Mapping
  ii   amd64-microcode  3.20250311.1  amd64  Platform firmware and microcode for AMD CPUs and SoCs
  ii   apache2  2.4.63-1  amd64  Apache HTTP Server
  ii   apache2-bin  2.4.63-1  amd64  Apache HTTP Server (modules and other binary files)
  ii   apache2-data  2.4.63-1  all  Apache HTTP Server (common files)
  ii   apache2-utils  2.4.63-1  amd64  Apache HTTP Server (utility programs for web servers)
  ii   apparmor  4.1.0-1  amd64  user-space parser utility for AppArmor
  ii   apt  2.9.29+kali1  amd64  commandline package manager
  ii   apt-file  3.3  all  search for files within Debian packages (command-line interface)
  ii   apt-utils  2.9.29+kali1  amd64  package management related utility programs
  ii   arj  3.10.22-28  amd64  archiver for .arj files
```

```
ii  arp-scan  1.10.0-2+b1  amd64  arp scanning and fingerprinting tool
ii  arping  2.25-1  amd64  sends IP and/or ARP pings (to the MAC address)
ii  aspell  0.60.8.1-4  amd64  GNU Aspell spell-checker
ii  aspell-en  2020.12.07-0-1  all  English dictionary for GNU Aspell
ii  aspnetcore-runtime-6.0  6.0.8-1  amd64
ii  aspnetcore-targeting-pack-6.0  6.0.9-1  amd64
ii  at-spi2-common  2.56.2-1  all  Assistive [...]
```

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8834/www

```
The STS header line is :

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8834/www

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

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8834/www

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

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

Synopsis

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

Description

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

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

Please note the following :

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

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

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

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0520

Plugin Information

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

Plugin Output

tcp/0

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

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/0

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

163326 - Tenable Nessus Installed (Linux)

Synopsis

Tenable Nessus is installed on the remote Linux host.

Description

Tenable Nessus is installed on the remote Linux host.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/07/21, Modified: 2025/05/28

Plugin Output

tcp/0

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

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

```
The host has not yet been rebooted.
```

237200 - Tornado Detection

Synopsis

A Tornado Python library is installed on the remote host.

Description

A Tornado Python library is installed on the remote host.

Note that Nessus has relied upon on the application's self-reported version number.

See Also

https://python.Tornado.com/v0.1/docs/get_started/quickstart/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/05/23, Modified: 2025/05/27

Plugin Output

tcp/0

```
Path    : /usr/lib/python3/dist-packages/tornado-6.4.2.egg-info
Version : 6.4.2
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 3 installs of XZ Utils:

  Path          : xz-utils 5.8.1-1 (via package manager)
  Version       : 5.8.1
  Managed by OS : True
```

```
Path               : /usr/lib/x86_64-linux-gnu/liblzma.so.5.8.1
Version            : 5.8.1
Associated Package : liblzma5 5.8.1-1
Confidence         : High
Managed by OS      : True
Version Source     : Package

Path           : /usr/bin/xz
Version        : 5.8.1
Confidence     : Medium
Version Source : File contents
```

110483 - Unix / Linux Running Processes Information

Synopsis

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

Plugin Output

tcp/0

```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.4  23816  9952 ?        Ss   17:29   0:05 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    17:29   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    17:29   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   17:29   0:00 [kworker/R-rcu_gp]
root           5  0.0  0.0      0     0 ?        I<   17:29   0:00 [kworker/R-sync_wq]
root           6  0.0  0.0      0     0 ?        I<   17:29   0:00 [kworker/R-slub_flushwq]
root           7  0.0  0.0      0     0 ?        I<   17:29   0:00 [kworker/R-netns]
root          12  0.0  0.0      0     0 ?        I<   17:29   0:00 [kworker/R-mm_percpu_wq]
root          13  0.0  0.0      0     0 ?        I    17:29   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    17:29   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    17:29   0:00 [rcu_tasks_trace_kthread]
root          16  0.3  0.0      0     0 ?        S    17:29   0:42 [ksoftirqd/0]
root          17  0.7  0.0      0     0 ?        I    17:29   1:48 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    17:29   0:00 [rcu_exp_par_gp_kthread_worker/1]
root          19  0.0  0.0      0     0 ?        S    17:29   0:00 [rcu_exp_gp_kthread_worker]
root          20  0.0  0.0      0     0 ?        S    17:29   0:07 [migration/0]
root          21  0.0  0.0      0     0 ?        S    17:29   0:00 [idle_inject/0]
root          22  0.0  0.0      0     0 ?        S    17:29   0:00 [cpuhp/0]
root          23  0.0  0.0      0     0 ?        S    17:29   0:00 [cpuhp/1]
root          24  0.0  0.0      0     0 ?        S    17:29   0:00 [idle_inject/1]
root          25  0.0  0.0      0     0 ?        S    17:29   0:07 [migration/1]
root          26  0.0  0.0      0     0 ?        S    17:29   0:11 [ksoftirqd/1]
root          31  0.0  0.0      0     0 ?        S    17:29   0:00 [kdevtmpfs]
root  [...]
```

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

```
Unix software discovery checks are available.

Protocol : LOCAL
```

186361 - VMWare Tools or Open VM Tools Installed (Linux)

Synopsis

VMWare Tools or Open VM Tools were detected on the remote Linux host.

Description

VMWare Tools or Open VM Tools were detected on the remote Linux host.

See Also

https://kb.vmware.com/s/article/340

http://www.nessus.org/u?c0628155

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/11/28, Modified: 2025/05/28

Plugin Output

tcp/0

```
Path    : /usr/bin/vmtoolsd
Version : 12.5.0
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of Vim:

  Path    : /usr/bin/vim.tiny
  Version : 9.1

  Path    : /usr/bin/vim.basic
  Version : 9.1
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:

  Path    : /usr/lib/x86_64-linux-gnu/libcurl.so.4.8.0
  Version : 8.13.0

  Path    : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.8.0
  Version : 8.13.0
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of libexiv2:

  Path          : libexiv2-27 0.27.6-1 (via package manager)
  Version       : 0.27.6
  Managed by OS : True

  Path    : /usr/lib/x86_64-linux-gnu/libexiv2.so.0.27.6
  Version : 3.1
```

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: 2025/05/28

Plugin Output

tcp/0

```
Nessus detected 2 installs of nginx:

  Path    : nginx (via package manager)
  Version : 1.26.3-2

  Path             : /usr/sbin/nginx
  Version          : 1.26.3
  Detection Method : Binary in $PATH
  Full Version     : 1.26.3
  Nginx Plus       : False
```

192.168.110.254

0	0	0	1	5
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP: 192.168.110.254

MAC Address: 00:50:56:F4:9B:AD

Vulnerabilities

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 : 192.168.110.254
  IP address the DHCP server would attribute us : 192.168.110.130
  DHCP server(s) identifier : 192.168.110.254
  Netmask : 255.255.255.0
  Router : 192.168.110.2
  Domain name server(s) : 192.168.110.2
  Domain name : localdomain
  Broadcast address : 192.168.110.255
  Netbios Name server(s) : 192.168.110.2
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:50:56:F4:9B:AD : VMware, Inc.
```

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

```
The following is a consolidated list of detected MAC addresses:
  - 00:50:56:F4:9B:AD
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/05/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.4
Nessus build : 20028
Plugin feed version : 202505310604
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.110.165
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 130.891 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 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 : 2025/5/31 21:14 IST (UTC +05:30)
Scan duration : 786 sec
Scan for malware : no
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.110.165 to 192.168.110.254 :
192.168.110.165

ttl was greater than 50 - Completing Traceroute.

?

Hop Count: 1

An error was detected along the way.
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```