My Basic Network Scan

Report generated by Tenable Nessus™ Fri, 08 Aug 2025 18:02:04 IST

Vulnerabilities by Plugin

Vulnerabilities by Plugin

56584 (1) - Mozilla Foundation Unsupported Application Detection (macOS)

Synopsis

The remote host contains one or more unsupported applications from the Mozilla Foundation.

Description

According to its version, there is at least one unsupported Mozilla application (Firefox and/or Thunderbird) installed on the remote host.

This version of the software is no longer actively maintained.

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

See Also

https://www.mozilla.org/en-US/firefox/organizations/faq/

https://www.mozilla.org/en-US/security/known-vulnerabilities/

https://www.mozilla.org/en-US/firefox/new/

https://www.mozilla.org/en-US/thunderbird/

Solution

Upgrade to a version that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	IAVA:0001-A-0565

Plugin Information

Published: 2011/10/21, Modified: 2024/12/30

Plugin Output

127.0.0.1 (tcp/445)

```
Product           : Mozilla Firefox
Path              : /Applications/Firefox.app
Installed version : 136.0.1
Latest version    : 141.0.0
EOL URL           : https://www.mozilla.org/en-US/firefox/releases/
```

179692 (1) - Node.js 16.x < 16.20.2 / 18.x < 18.17.1 / 20.x < 20.5.1 Multiple Vulnerabilities (Wednesday August 09 2023 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 16.20.2, 18.17.1, 20.5.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday August 09 2023 Security Releases advisory:

- Permissions policies can be bypassed via Module._load (CVE-2023-32002)

- Permission model bypass by specifying a path traversal sequence in a Buffer (CVE-2023-32004)

- process.binding() can bypass the permission model through path traversal (CVE-2023-32558)

- Permissions policies can impersonate other modules in using module.constructor.createRequire() (CVE-2023-32006)

- Permissions policies can be bypassed via process.binding (CVE-2023-32559)

- fs.statfs can retrive stats from files restricted by the Permission Model (CVE-2023-32005)

- fs.mkdtemp() and fs.mkdtempSync() are missing getValidatedPath() checks (CVE-2023-32003)

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?c4ab34c1

Solution

Upgrade to Node.js version 16.20.22 / 18.17.1 / 20.5.1 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

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

VPR Score

6.7

EPSS Score

0.0103

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

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

STIG Severity

I

References

CVE	CVE-2023-32002
CVE	CVE-2023-32003
CVE	CVE-2023-32004
CVE	CVE-2023-32005
CVE	CVE-2023-32006
CVE	CVE-2023-32558
CVE	CVE-2023-32559
XREF	IAVB:2023-B-0059-S

Plugin Information

Published: 2023/08/11, Modified: 2024/01/09

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /usr/local/bin/node
Installed version : 18.12.1
Fixed version     : 18.17.1
```

183390 (1) - Node.js 18.x < 18.18.2 / 20.x < 20.8.1 Multiple Vulnerabilities (Friday October 13 2023 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 18.18.2, 20.8.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Friday October 13 2023 Security Releases advisory.

- Undici did not always clear Cookie headers on cross-origin redirects. By design, cookie headers are forbidden request headers, disallowing them to be set in RequestInit.headers in browser environments.

Since undici handles headers more liberally than the spec, there was a disconnect from the assumptions the spec made, and undici's implementation of fetch. As such this may lead to accidental leakage of cookie to a 3rd-party site or a malicious attacker who can control the redirection target (ie. an open redirector) to leak the cookie to the 3rd party site. More details area available in GHSA-wqq4-5wpv-mx2g (CVE-2023-45143)

- Rapidly creating and cancelling streams (HEADERS frame immediately followed by RST_STREAM) without bound causes denial of service. See https://www.cve.org/CVERecord?id=CVE-2023-44487 for details. Impacts:

(CVE-2023-44487)

- A previously disclosed vulnerability (CVE-2023-30584) was patched insufficiently. The new path traversal vulnerability arises because the implementation does not protect itself against the application overwriting built-in utility functions with user-defined implementations. Impacts: Please note that at the time this CVE is issued, the permission model is an experimental feature of Node.js. Thanks to Tobias Nieen who reported and created the security patch. (CVE-2023-39331)

- Various node:fs functions allow specifying paths as either strings or Uint8Array objects. In Node.js environments, the Buffer class extends the Uint8Array class. Node.js prevents path traversal through strings (see CVE-2023-30584) and Buffer objects (see CVE-2023-32004), but not through non-Buffer Uint8Array objects. This is distinct from CVE-2023-32004 (report 2038134), which only referred to Buffer objects. However, the vulnerability follows the same pattern using Uint8Array instead of Buffer. Impacts:

Please note that at the time this CVE is issued, the permission model is an experimental feature of Node.js. Thanks to Tobias Nieen who reported and created the security patch. (CVE-2023-39332)

- When the Node.js policy feature checks the integrity of a resource against a trusted manifest, the application can intercept the operation and return a forged checksum to node's policy implementation, thus effectively disabling the integrity check. Impacts: Please note that at the time this CVE is issued, the policy mechanism is an experimental feature of Node.js. Thanks to Tobias Nieen who reported and created the security patch. (CVE-2023-38552)

- Maliciously crafted export names in an imported WebAssembly module can inject JavaScript code. The injected code may be able to access data and functions that the WebAssembly module itself does not have access to, similar to as if the WebAssembly module was a JavaScript module. Impacts: Thanks to dittyroma for reporting the issue and to Tobias Nieen for fixing it. (CVE-2023-39333)

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?158127f8

Solution

Upgrade to Node.js version 18.18.2 / 20.8.1 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

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

VPR Score

6.9

EPSS Score

0.9441

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

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

STIG Severity

I

References

CVE	CVE-2023-38552
CVE	CVE-2023-39331
CVE	CVE-2023-39332
CVE	CVE-2023-39333
CVE	CVE-2023-44487
CVE	CVE-2023-45143

XREF	CISA-KNOWN-EXPLOITED:2023/10/31
XREF	CEA-ID:CEA-2024-0004
XREF	IAVB:2023-B-0083-S

Plugin Information

Published: 2023/10/19, Modified: 2024/02/23

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /usr/local/bin/node
Installed version : 18.12.1
Fixed version     : 18.18.2
```

190856 (1) - 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

5.9

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

127.0.0.1 (tcp/0)

```
Path              : /usr/local/bin/node
Installed version : 18.12.1
Fixed version     : 18.19.1
```

209250 (1) - Oracle MySQL Server 8.0.x < 8.0.40 (January 2025 CPU)

Synopsis

The remote host is affected by multiple vulnerabilities

Description

The versions of MySQL Server installed on the remote host are affected by multiple vulnerabilities as referenced in the January 2025 CPU advisory.

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging (Kerberos)). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2024-37371)

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging (OpenSSL)).

Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2024-5535)

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging (curl)). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server.

Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2024-7264)

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

See Also

https://www.oracle.com/security-alerts/cpuoct2024.html

https://www.oracle.com/docs/tech/security-alerts/cpuoct2024csaf.json

https://www.oracle.com/security-alerts/cpujan2025.html

https://www.oracle.com/docs/tech/security-alerts/cpujan2025csaf.json

Solution

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

Risk Factor

High

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

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-21193
CVE	CVE-2024-21194
CVE	CVE-2024-21196
CVE	CVE-2024-21197
CVE	CVE-2024-21198
CVE	CVE-2024-21199
CVE	CVE-2024-21201
CVE	CVE-2024-21203
CVE	CVE-2024-21212
CVE	CVE-2024-21213
CVE	CVE-2024-21218
CVE	CVE-2024-21219
CVE	CVE-2024-21230
CVE	CVE-2024-21231
CVE	CVE-2024-21236
CVE	CVE-2024-21237
CVE	CVE-2024-21238

CVE	CVE-2024-21239
CVE	CVE-2024-21241
CVE	CVE-2024-21247
CVE	CVE-2024-7264
CVE	CVE-2024-5535
CVE	CVE-2024-37371
CVE	CVE-2025-21494
CVE	CVE-2025-21504
CVE	CVE-2025-21521
CVE	CVE-2025-21525
CVE	CVE-2025-21534
CVE	CVE-2025-21536
XREF	IAVA:2025-A-0050

Plugin Information

Published: 2024/10/17, Modified: 2025/04/18

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /usr/local/mysql/bin
Installed version : 8.0.36
Fixed version     : 8.0.40
```

233646 (1) - Mozilla Firefox < 137.0

Synopsis

A web browser installed on the remote macOS or Mac OS X host is affected by multiple vulnerabilities.

Description

The version of Firefox installed on the remote macOS or Mac OS X host is prior to 137.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2025-20 advisory.

- Memory safety bugs present in Firefox 136 and Thunderbird 136. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2025-3034)

- JavaScript code running while transforming a document with the XSLTProcessor could lead to a use-after-free. (CVE-2025-3028)

- An attacker could read 32 bits of values spilled onto the stack in a JIT compiled function.

(CVE-2025-3031)

- Leaking of file descriptors from the fork server to web content processes could allow for privilege escalation attacks. (CVE-2025-3032)

- A crafted URL containing specific Unicode characters could have hidden the true origin of the page, resulting in a potential spoofing attack. (CVE-2025-3029)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2025-20/

Solution

Upgrade to Mozilla Firefox version 137.0 or later.

Risk Factor

High

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

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-3028
CVE	CVE-2025-3029
CVE	CVE-2025-3030
CVE	CVE-2025-3031
CVE	CVE-2025-3032
CVE	CVE-2025-3033
CVE	CVE-2025-3034
CVE	CVE-2025-3035
XREF	IAVA:2025-A-0211-S

Plugin Information

Published: 2025/04/01, Modified: 2025/05/05

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /Applications/Firefox.app
Installed version : 136.0.1
Fixed version     : 137.0
```

238071 (1) - Mozilla Firefox < 139.0.4

Synopsis

A web browser installed on the remote macOS or Mac OS X host is affected by multiple vulnerabilities.

Description

The version of Firefox installed on the remote macOS or Mac OS X host is prior to 139.0.4. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2025-47 advisory.

- An integer overflow was present in <code>OrderedHashTable</code> used by the JavaScript engine (CVE-2025-49710)

- Certain canvas operations could have lead to memory corruption. (CVE-2025-49709)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2025-47/

Solution

Upgrade to Mozilla Firefox version 139.0.4 or later.

Risk Factor

High

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

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-49709
CVE	CVE-2025-49710
XREF	IAVA:2025-A-0409

Plugin Information

Published: 2025/06/10, Modified: 2025/06/13

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /Applications/Firefox.app
Installed version : 136.0.1
Fixed version     : 139.0.4
```

240333 (1) - Mozilla Firefox < 140.0

Synopsis

A web browser installed on the remote macOS or Mac OS X host is affected by multiple vulnerabilities.

Description

The version of Firefox installed on the remote macOS or Mac OS X host is prior to 140.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2025-51 advisory.

- Memory safety bugs present in Firefox 139 and Thunderbird 139. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2025-6436)

- A use-after-free in FontFaceSet resulted in a potentially exploitable crash. (CVE-2025-6424)

- An attacker who enumerated resources from the WebCompat extension could have obtained a persistent UUID that identified the browser, and persisted between containers and normal/private browsing mode, but not profiles. (CVE-2025-6425)

- The executable file warning did not warn users before opening files with the <code>terminal</code>

extension. This bug only affects Firefox for macOS. Other versions of Firefox are unaffected.

(CVE-2025-6426)

- An attacker was able to bypass the <code>connect-src</code> directive of a Content Security Policy by manipulating subdocuments. This would have also hidden the connections from the Network tab in Devtools.

(CVE-2025-6427)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2025-51/

Solution

Upgrade to Mozilla Firefox version 140.0 or later.

Risk Factor

High

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

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-6424
CVE	CVE-2025-6425
CVE	CVE-2025-6426
CVE	CVE-2025-6427
CVE	CVE-2025-6428
CVE	CVE-2025-6429
CVE	CVE-2025-6430
CVE	CVE-2025-6431
CVE	CVE-2025-6432
CVE	CVE-2025-6433
CVE	CVE-2025-6434
CVE	CVE-2025-6435
CVE	CVE-2025-6436
XREF	IAVA:2025-A-0451

Plugin Information

Published: 2025/06/24, Modified: 2025/07/08

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /Applications/Firefox.app
Installed version : 136.0.1
Fixed version     : 140.0
```

242556 (1) - Mozilla Firefox < 141.0

Synopsis

A web browser installed on the remote macOS or Mac OS X host is affected by multiple vulnerabilities.

Description

The version of Firefox installed on the remote macOS or Mac OS X host is prior to 141.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2025-56 advisory.

- Memory safety bugs present in Firefox 140 and Thunderbird 140. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2025-8044)

- On 64-bit platforms IonMonkey-JIT only wrote 32 bits of the 64-bit return value space on the stack.

Baseline-JIT, however, read the entire 64 bits. (CVE-2025-8027)

- On arm64, a WASM <code>brtable</code> instruction with a lot of entries could lead to the label being too far from the instruction causing truncation and incorrect computation of the branch address.

(CVE-2025-8028)

- In the address bar, Firefox for Android truncated the display of URLs from the end instead of prioritizing the origin. (CVE-2025-8041)

- Firefox for Android allowed a sandboxed iframe without the <code>allow-downloads</code> attribute to start downloads. (CVE-2025-8042)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/

Solution

Upgrade to Mozilla Firefox version 141.0 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

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

VPR Score

7.4

EPSS Score

0.0005

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

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

STIG Severity

I

References

CVE	CVE-2025-8027
CVE	CVE-2025-8028
CVE	CVE-2025-8029
CVE	CVE-2025-8030
CVE	CVE-2025-8031
CVE	CVE-2025-8032
CVE	CVE-2025-8033
CVE	CVE-2025-8034
CVE	CVE-2025-8035
CVE	CVE-2025-8036
CVE	CVE-2025-8037
CVE	CVE-2025-8038
CVE	CVE-2025-8039
CVE	CVE-2025-8040
CVE	CVE-2025-8041
CVE	CVE-2025-8042
CVE	CVE-2025-8043
CVE	CVE-2025-8044
CVE	CVE-2025-8364
XREF	IAVA:2025-A-0543

Plugin Information

Published: 2025/07/22, Modified: 2025/07/30

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /Applications/Firefox.app
Installed version : 136.0.1
Fixed version     : 141.0
```

171595 (1) - Node.js 14.x < 14.21.3 / 16.x < 16.19.1 / 18.x < 18.14.1 / 19.x < 19.6.1 Multiple Vulnerabilities (Thursday February 16 2023 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 14.21.3, 16.19.1, 18.14.1, 19.6.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Thursday February 16 2023 Security Releases advisory.

- It was possible to bypass Permissions and access non authorized modules by using process.mainModule.require(). This only affects users who had enabled the experimental permissions option with --experimental-policy. Thank you, to @goums for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. Impacts: (CVE-2023-23918)

- In some cases Node.js did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. Thank you, to Morgan Jones and Ryan Dorrity from Viasat Secure Mobile for reporting and discovering this vulnerability and thank you Rafael Gonzaga for fixing it. Impacts: (CVE-2023-23919)

- The fetch API in Node.js did not prevent CRLF injection in the 'host' header potentially allowing attacks such as HTTP response splitting and HTTP header injection. Thank you, to Zhipeng Zhang (@timon8) for reporting this vulnerability and thank you Robert Nagy for fixing it. Impacts: (CVE-2023-23936)

- The Headers.set() and Headers.append() methods in the fetch API in Node.js where vulnerable to Regular a Expression Denial of Service (ReDoS) attacks. Thank you, to Carter Snook for reporting this vulnerability and thank you Rich Trott for fixing it. Impacts: (CVE-2023-24807)

- Node.js would search and potentially load ICU data when running with elevated priviledges. Node.js was modified to build with ICU_NO_USER_DATA_OVERRIDE to avoid this. Thank you, to Ben Noordhuis for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. Impacts: (CVE-2023-23920)

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?461376f3

Solution

Upgrade to Node.js version 14.21.3 / 16.19.1 / 18.14.1 / 19.6.1 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:H/I:N/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0419

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-23918
CVE	CVE-2023-23919
CVE	CVE-2023-23920
CVE	CVE-2023-23936
CVE	CVE-2023-24807
XREF	IAVB:2023-B-0013

Plugin Information

Published: 2023/02/17, Modified: 2024/01/09

Plugin Output

127.0.0.1 (tcp/0)

```
  Path              : /usr/local/bin/node
  Installed version : 18.12.1
```

```
  Fixed version     : 18.14.1
```

177518 (1) - Node.js 16.x < 16.20.1 / 18.x < 18.16.1 / 20.x < 20.3.1 Multiple Vulnerabilities (Tuesday June 20 2023 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 16.20.1, 18.16.1, 20.3.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Tuesday June 20 2023 Security Releases advisory.

- The use of proto in process.mainModule.proto.require() can bypass the policy mechanism and require modules outside of the policy.json definition. This vulnerability affects all users using the experimental policy mechanism in all active release lines: 16.x, 18.x and, 20.x. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js. Thank you, to Axel Chong for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. (CVE-2023-30581)

- A vulnerability has been discovered in Node.js version 20, specifically within the experimental permission model. This flaw relates to improper handling of path traversal bypass when verifying file permissions.

This vulnerability affects all users using the experimental permission model in Node.js 20. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Axel Chong for reporting this vulnerability and thank you Rafael Gonzaga for fixing it.

(CVE-2023-30584)

- A vulnerability in Node.js version 20 allows for bypassing restrictions set by the --experimental-permission flag using the built-in inspector module (node:inspector). By exploiting the Worker class's ability to create an internal worker with the kIsInternal Symbol, attackers can modify the isInternal value when an inspector is attached within the Worker constructor before initializing a new WorkerImpl.

This vulnerability exclusively affects Node.js users employing the permission model mechanism in Node.js 20. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to mattaustin for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. (CVE-2023-30587)

- A vulnerability has been identified in Node.js version 20, affecting users of the experimental permission model when the --allow-fs-read flag is used with a non-* argument. This flaw arises from an inadequate permission model that fails to restrict file watching through the fs.watchFile API. As a result, malicious actors can monitor files that they do not have explicit read access to. This vulnerability affects all users using the experimental permission model in Node.js 20. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thanks to Colin Ihrig for reporting this vulnerability and to Rafael Gonzaga for fixing it. (CVE-2023-30582)

- fs.openAsBlob() can bypass the experimental permission model when using the file system read restriction with the --allow-fs-read flag in Node.js 20. This flaw arises from a missing check in the fs.openAsBlob() API. This vulnerability affects all users using the experimental permission model in Node.js 20. Thanks to Colin Ihrig for reporting this vulnerability and to Rafael Gonzaga for fixing it. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. (CVE-2023-30583)

- A vulnerability has been identified in the Node.js (.msi version) installation process, specifically affecting Windows users who install Node.js using the .msi installer. This vulnerability emerges during the repair operation, where the msiexec.exe process, running under the NT AUTHORITY\SYSTEM context, attempts to read the %USERPROFILE% environment variable from the current user's registry. The issue arises when

the path referenced by the %USERPROFILE% environment variable does not exist. In such cases, the msiexec.exe process attempts to create the specified path in an unsafe manner, potentially leading to the creation of arbitrary folders in arbitrary locations. The severity of this vulnerability is heightened by the fact that the %USERPROFILE% environment variable in the Windows registry can be modified by standard (or non-privileged) users. Consequently, unprivileged actors, including malicious entities or trojans, can manipulate the environment variable key to deceive the privileged msiexec.exe process. This manipulation can result in the creation of folders in unintended and potentially malicious locations. It is important to note that this vulnerability is specific to Windows users who install Node.js using the .msi installer. Users who opt for other installation methods are not affected by this particular issue.

This affects all active Node.js versions: v16, v18, and, v20. Thank you, to @sim0nsecurity for reporting this vulnerability and thank you Tobias Nieen for fixing it. (CVE-2023-30585)

- Node.js 20 allows loading arbitrary OpenSSL engines when the experimental permission model is enabled, which can bypass and/or disable the permission model. The crypto.setEngine() API can be used to bypass the permission model when called with a compatible OpenSSL engine. The OpenSSL engine can, for example, disable the permission model in the host process by manipulating the process's stack memory to locate the permission model Permission::enabled_ in the host process's heap memory. This vulnerability affects all users using the experimental permission model in Node.js 20. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thanks to Tobias Nieen for reporting this vulnerability and fixing it. (CVE-2023-30586)

- When an invalid public key is used to create an x509 certificate using the crypto.X509Certificate() API a non-expect termination occurs making it susceptible to DoS attacks when the attacker could force interruptions of application processing, as the process terminates when accessing public key info of provided certificates from user code. The current context of the users will be gone, and that will cause a DoS scenario. This vulnerability affects all active Node.js versions v16, v18, and, v20. Thank you, to Marc Schnefeld for reporting this vulnerability and thank you Tobias Nieen for fixing it.

(CVE-2023-30588)

- The llhttp parser in the http module in Node.js does not strictly use the CRLF sequence to delimit HTTP requests. This can lead to HTTP Request Smuggling (HRS). The CR character (without LF) is sufficient to delimit HTTP header fields in the llhttp parser. According to RFC7230 section 3, only the CRLF sequence should delimit each header-field. This vulnerability impacts all Node.js active versions: v16, v18, and, v20. Thank you, to Yadhu Krishna M(Team bi0s & CRED Security team) for reporting this vulnerability and thank you Paolo Insogna for fixing it. (CVE-2023-30589)

- The generateKeys() API function returned from crypto.createDiffieHellman() only generates missing (or outdated) keys, that is, it only generates a private key if none has been set yet. However, the documentation says this API call: Generates private and public Diffie-Hellman key values. The documented behavior is different from the actual behavior, and this difference could easily lead to security issues in applications that use these APIs as the DiffieHellman may be used as the basis for application-level security. Please note that this is a documentation change an the vulnerability has been classified under CWE-1068 - Inconsistency Between Implementation and Documented Design. This change applies to all Node.js active versions: v16, v18, and, v20. Thanks to Ben Smyth for reporting this vulnerability and to Tobias Nieen for fixing it. (CVE-2023-30590)

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/june-2023-security-releases/

Solution

Upgrade to Node.js version 16.20.1 / 18.16.1 / 20.3.1 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:H/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.0946

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-30581
CVE	CVE-2023-30582
CVE	CVE-2023-30583
CVE	CVE-2023-30584
CVE	CVE-2023-30585
CVE	CVE-2023-30586
CVE	CVE-2023-30587
CVE	CVE-2023-30588
CVE	CVE-2023-30589
CVE	CVE-2023-30590
XREF	IAVB:2023-B-0042-S

Plugin Information

Published: 2023/06/22, Modified: 2024/01/09

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /usr/local/bin/node
Installed version : 18.12.1
Fixed version     : 18.16.1
```

192945 (1) - 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

0.6865

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

127.0.0.1 (tcp/0)

```
Path              : /usr/local/bin/node
Installed version : 18.12.1
Fixed version     : 18.20.1
```

201969 (1) - 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

127.0.0.1 (tcp/0)

```
Path              : /usr/local/bin/node
Installed version : 18.12.1
Fixed version     : 18.20.4
```

214404 (1) - 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)

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

6.0

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-2025-23085
XREF	IAVB:2025-B-0012-S

Plugin Information

Published: 2025/01/21, Modified: 2025/08/05

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /usr/local/bin/node
Installed version : 18.12.1
Fixed version     : 18.20.6
```

222492 (1) - VMware Fusion 13.x < 13.6.3 HGFS Information Disclosure (VMSA-2025-0004)

Synopsis

A virtualization application installed on the remote macOS host is affected by an information disclosure vulnerability.

Description

The version of VMware Fusion installed on the remote macOS host is 13.x prior to 13.6.3. It is, therefore, affected by an information disclosure vulnerability:

- VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. (CVE-2025-22226)

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?15790ced

Solution

Update to VMware Fusion version 13.6.3, or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.1

EPSS Score

0.081

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-22226
XREF	VMSA:2025-0004
XREF	CISA-KNOWN-EXPLOITED:2025/03/25
XREF	IAVA:2025-A-0148-S

Plugin Information

Published: 2025/03/04, Modified: 2025/05/27

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /Applications/VMware Fusion.app
Installed version : 13.6.0
Fixed version     : 13.6.3
```

234434 (1) - Mozilla Firefox < 137.0.2

Synopsis

A web browser installed on the remote macOS or Mac OS X host is affected by a vulnerability.

Description

The version of Firefox installed on the remote macOS or Mac OS X host is prior to 137.0.2. It is, therefore, affected by a vulnerability as referenced in the mfsa2025-25 advisory.

- A race condition existed in nsHttpTransaction that could have been exploited to cause memory corruption, potentially leading to an exploitable condition. (CVE-2025-3608)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2025-25/

Solution

Upgrade to Mozilla Firefox version 137.0.2 or later.

Risk Factor

Medium

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

5.0

EPSS Score

0.0002

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-2025-3608
XREF	IAVA:2025-A-0280-S

Plugin Information

Published: 2025/04/15, Modified: 2025/05/05

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /Applications/Firefox.app
Installed version : 136.0.1
Fixed version     : 137.0.2
```

234925 (1) - Mozilla Firefox < 138.0

Synopsis

A web browser installed on the remote macOS or Mac OS X host is affected by multiple vulnerabilities.

Description

The version of Firefox installed on the remote macOS or Mac OS X host is prior to 138.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2025-28 advisory.

- Memory safety bugs present in Firefox 137, Thunderbird 137, Firefox ESR 128.9, and Thunderbird 128.9. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2025-4091)

- Mozilla Firefox's update mechanism allowed a medium-integrity user process to interfere with the SYSTEM- level updater by manipulating the file-locking behavior. By injecting code into the user-privileged process, an attacker could bypass intended access controls, allowing SYSTEM-level file operations on paths controlled by a non-privileged user and enabling privilege escalation. (CVE-2025-2817)

- Modification of specific WebGL shader attributes could trigger an out-of-bounds read, which, when chained with other vulnerabilities, could be used to escalate privileges. This bug only affects Firefox for macOS.

Other versions of Firefox are unaffected. (CVE-2025-4082)

- A process isolation vulnerability in Firefox stemmed from improper handling of javascript: URIs, which could allow content to execute in the top-level document's process instead of the intended frame, potentially enabling a sandbox escape. (CVE-2025-4083)

- An attacker with control over a content process could potentially leverage the privileged UITour actor to leak sensitive information or escalate privileges. (CVE-2025-4085)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2025-28/

Solution

Upgrade to Mozilla Firefox version 138.0 or later.

Risk Factor

Medium

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

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

VPR Score

6.7

EPSS Score

0.0005

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-2025-2817
CVE	CVE-2025-4082
CVE	CVE-2025-4083
CVE	CVE-2025-4085
CVE	CVE-2025-4086
CVE	CVE-2025-4087
CVE	CVE-2025-4088
CVE	CVE-2025-4089
CVE	CVE-2025-4090
CVE	CVE-2025-4091
CVE	CVE-2025-4092
XREF	IAVA:2025-A-0307-S

Plugin Information

Published: 2025/04/29, Modified: 2025/05/22

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /Applications/Firefox.app
Installed version : 136.0.1
Fixed version     : 138.0
```

236891 (1) - Mozilla Firefox < 138.0.4

Synopsis

A web browser installed on the remote macOS or Mac OS X host is affected by multiple vulnerabilities.

Description

The version of Firefox installed on the remote macOS or Mac OS X host is prior to 138.0.4. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2025-36 advisory.

- An attacker was able to perform an out-of-bounds read or write on a JavaScript object by confusing array index sizes. (CVE-2025-4919)

- An attacker was able to perform an out-of-bounds read or write on a JavaScript `Promise` object.

(CVE-2025-4918)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2025-36/

Solution

Upgrade to Mozilla Firefox version 138.0.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

EPSS Score

0.0002

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-2025-4918
CVE	CVE-2025-4919
XREF	IAVA:2025-A-0362-S

Plugin Information

Published: 2025/05/17, Modified: 2025/05/29

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /Applications/Firefox.app
Installed version : 136.0.1
Fixed version     : 138.0.4
```

237299 (1) - Mozilla Firefox < 139.0

Synopsis

A web browser installed on the remote macOS or Mac OS X host is affected by multiple vulnerabilities.

Description

The version of Firefox installed on the remote macOS or Mac OS X host is prior to 139.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2025-42 advisory.

- In certain cases, SNI could have been sent unencrypted even when encrypted DNS was enabled.
(CVE-2025-5270)

- A double-free could have occurred in `vpxcodecencinitmulti` after a failed allocation when initializing the encoder for WebRTC. This could have caused memory corruption and a potentially exploitable crash.
(CVE-2025-5283)

- Error handling for script execution was incorrectly isolated from web content, which could have allowed cross-origin leak attacks. (CVE-2025-5263)

- Due to insufficient escaping of the newline character in the Copy as cURL feature, an attacker could trick a user into using this command, potentially leading to local code execution on the user's system.
(CVE-2025-5264)

- Due to insufficient escaping of the ampersand character in the Copy as cURL feature, an attacker could trick a user into using this command, potentially leading to local code execution on the user's system.
This bug only affects Firefox for Windows. Other versions of Firefox are unaffected. (CVE-2025-5265)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2025-42/

Solution

Upgrade to Mozilla Firefox version 139.0 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:H/I:N/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0009

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-5263
CVE	CVE-2025-5264
CVE	CVE-2025-5265
CVE	CVE-2025-5266
CVE	CVE-2025-5267
CVE	CVE-2025-5268
CVE	CVE-2025-5270
CVE	CVE-2025-5271
CVE	CVE-2025-5272
CVE	CVE-2025-5283
XREF	IAVA:2025-A-0386

Plugin Information

Published: 2025/05/27, Modified: 2025/06/12

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /Applications/Firefox.app
Installed version : 136.0.1
Fixed version     : 139.0
```

243030 (1) - macOS 15.x < 15.6 Multiple Vulnerabilities (124149)

Synopsis

The remote host is missing a macOS update that fixes multiple vulnerabilities

Description

The remote host is running a version of macOS / Mac OS X that is 15.x prior to 15.6. It is, therefore, affected by multiple vulnerabilities:

- A flaw was found in the libxslt library. The same memory field, psvi, is used for both stylesheet and input data, which can lead to type confusion during XML transformations. This vulnerability allows an attacker to crash the application or corrupt memory. In some cases, it may lead to denial of service or unexpected behavior. (CVE-2025-7424)

- Insufficient validation of untrusted input in ANGLE and GPU in Google Chrome prior to 138.0.7204.157 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) (CVE-2025-6558)

- A flaw was found in libxslt where the attribute type, atype, flags are modified in a way that corrupts internal memory management. When XSLT functions, such as the key() process, result in tree fragments, this corruption prevents the proper cleanup of ID attributes. As a result, the system may access freed memory, causing crashes or enabling attackers to trigger heap corruption. (CVE-2025-7425)

- This issue was addressed by adding an additional prompt for user consent. (CVE-2025-24188, CVE-2025-31273, CVE-2025-31275, CVE-2025-31277, CVE-2025-31279, CVE-2025-31280, CVE-2025-31281, CVE-2025-43185, CVE-2025-43186, CVE-2025-43188, CVE-2025-43189, CVE-2025-43193, CVE-2025-43195, CVE-2025-43198, CVE-2025-43199, CVE-2025-43215, CVE-2025-43216, CVE-2025-43218, CVE-2025-43219, CVE-2025-43221, CVE-2025-43222, CVE-2025-43223, CVE-2025-43224, CVE-2025-43225, CVE-2025-43226, CVE-2025-43227, CVE-2025-43229, CVE-2025-43230, CVE-2025-43232, CVE-2025-43233, CVE-2025-43234, CVE-2025-43235, CVE-2025-43236, CVE-2025-43237, CVE-2025-43238, CVE-2025-43239, CVE-2025-43240, CVE-2025-43241, CVE-2025-43243, CVE-2025-43244, CVE-2025-43245, CVE-2025-43246, CVE-2025-43247, CVE-2025-43248, CVE-2025-43249, CVE-2025-43250, CVE-2025-43251, CVE-2025-43252, CVE-2025-43254, CVE-2025-43255, CVE-2025-43256, CVE-2025-43257, CVE-2025-43259, CVE-2025-43260, CVE-2025-43261, CVE-2025-43264, CVE-2025-43265, CVE-2025-43266, CVE-2025-43267, CVE-2025-43268, CVE-2025-43270, CVE-2025-43273, CVE-2025-43274, CVE-2025-43275, CVE-2025-43276, CVE-2025-43277)

- An integer overflow was addressed with improved input validation. (CVE-2025-31243, CVE-2025-43187, CVE-2025-43191, CVE-2025-43192, CVE-2025-43194, CVE-2025-43196, CVE-2025-43197, CVE-2025-43206, CVE-2025-43210, CVE-2025-43220, CVE-2025-43253)

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

See Also

https://support.apple.com/en-us/124149

Solution

Upgrade to macOS 15.6 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.4

EPSS Score

0.0009

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-24188
CVE	CVE-2025-31243
CVE	CVE-2025-31273
CVE	CVE-2025-31275
CVE	CVE-2025-31277
CVE	CVE-2025-31278
CVE	CVE-2025-31279
CVE	CVE-2025-31280
CVE	CVE-2025-31281
CVE	CVE-2025-43185
CVE	CVE-2025-43186
CVE	CVE-2025-43187
CVE	CVE-2025-43188

CVE	CVE-2025-43189
CVE	CVE-2025-43191
CVE	CVE-2025-43192
CVE	CVE-2025-43193
CVE	CVE-2025-43194
CVE	CVE-2025-43195
CVE	CVE-2025-43196
CVE	CVE-2025-43197
CVE	CVE-2025-43198
CVE	CVE-2025-43199
CVE	CVE-2025-43202
CVE	CVE-2025-43206
CVE	CVE-2025-43209
CVE	CVE-2025-43210
CVE	CVE-2025-43211
CVE	CVE-2025-43212
CVE	CVE-2025-43213
CVE	CVE-2025-43214
CVE	CVE-2025-43215
CVE	CVE-2025-43216
CVE	CVE-2025-43218
CVE	CVE-2025-43219
CVE	CVE-2025-43220
CVE	CVE-2025-43221
CVE	CVE-2025-43222
CVE	CVE-2025-43223
CVE	CVE-2025-43224
CVE	CVE-2025-43225
CVE	CVE-2025-43226
CVE	CVE-2025-43227
CVE	CVE-2025-43229
CVE	CVE-2025-43230
CVE	CVE-2025-43232
CVE	CVE-2025-43233
CVE	CVE-2025-43234
CVE	CVE-2025-43235
CVE	CVE-2025-43236
CVE	CVE-2025-43237
CVE	CVE-2025-43238
CVE	CVE-2025-43239
CVE	CVE-2025-43240
CVE	CVE-2025-43241
CVE	CVE-2025-43243

CVE	CVE-2025-43244
CVE	CVE-2025-43245
CVE	CVE-2025-43246
CVE	CVE-2025-43247
CVE	CVE-2025-43248
CVE	CVE-2025-43249
CVE	CVE-2025-43250
CVE	CVE-2025-43251
CVE	CVE-2025-43252
CVE	CVE-2025-43253
CVE	CVE-2025-43254
CVE	CVE-2025-43255
CVE	CVE-2025-43256
CVE	CVE-2025-43257
CVE	CVE-2025-43259
CVE	CVE-2025-43260
CVE	CVE-2025-43261
CVE	CVE-2025-43264
CVE	CVE-2025-43265
CVE	CVE-2025-43266
CVE	CVE-2025-43267
CVE	CVE-2025-43268
CVE	CVE-2025-43270
CVE	CVE-2025-43273
CVE	CVE-2025-43274
CVE	CVE-2025-43275
CVE	CVE-2025-43276
CVE	CVE-2025-43277
CVE	CVE-2025-6558
CVE	CVE-2025-7424
CVE	CVE-2025-7425
XREF	APPLE-SA:124149
XREF	CISA-KNOWN-EXPLOITED:2025/08/12
XREF	IAVA:2025-A-0555

Plugin Information

Published: 2025/07/30, Modified: 2025/08/01

Plugin Output

127.0.0.1 (tcp/0)

```
  Installed version : 15.5
```

```
  Fixed version     : macOS Sequoia 15.6
```

242630 (3) - Ruby REXML < 3.3.6 DoS vulnerability

Synopsis

The remote host has an application installed that is affected by a DoS vulnerability.

Description

The version of the REXML Ruby library installed on the remote host is prior to 3.3.6. It is, therefore, affected by a DoS vulnerability. The vulnerability lies when it parses an XML that has many deep elements that have same local name attributes.

If you need to parse untrusted XMLs with tree parser API like REXML::Document.new, you may be impacted to this vulnerability. If you use other parser APIs such as stream parser API and SAX2 parser API, this vulnerability is not affected.

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://github.com/ruby/rexml/security/advisories/GHSA-vmwr-mc7x-5vc3

Solution

Upgrade to REXML version 3.3.6 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

VPR Score

3.6

EPSS Score

0.0032

CVSS v2.0 Base Score

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

STIG Severity

II

References

CVE	CVE-2024-43398
XREF	IAVB:2024-B-0124

Plugin Information

Published: 2025/07/23, Modified: 2025/07/23

Plugin Output

127.0.0.1 (tcp/0)

```
  Path              : /Library/Ruby/Gems/2.6.0/specifications/default/rexml-3.1.9.1.gemspec
  Installed version : 3.1.9.1
  Fixed version     : 3.3.6
```

127.0.0.1 (tcp/0)

```
  Path              : /opt/metasploit-framework/embedded/lib/ruby/gems/3.1.0/specifications/
rexml-3.2.5.gemspec
  Installed version : 3.2.5
  Fixed version     : 3.3.6
```

127.0.0.1 (tcp/0)

```
  Path              : /opt/metasploit-framework/embedded/lib/ruby/gems/3.2.0/specifications/
rexml-3.3.2.gemspec
  Installed version : 3.3.2
  Fixed version     : 3.3.6
```

240854 (2) - Ruby WEBrick < 1.8.2 HTTP Request Smuggling

Synopsis

The remote host has an application installed that is affected by an HTTP request smuggling vulnerability

Description

The version of the WEBrick Ruby library installed on the remote host is prior to 1.8.2. It is, therefore, affected by an HTTP request smuggling vulnerability in the read_header. This vulnerability allows remote attackers to smuggle arbitrary HTTP requests on affected installations of Ruby WEBrick. This issue is exploitable when the product is deployed behind an HTTP proxy that fulfills specific conditions. The specific flaw exists within the read_headers method. The issue results from the inconsistent parsing of terminators of HTTP headers. An attacker can leverage this vulnerability to smuggle arbitrary HTTP requests.

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?824008ea

https://www.zerodayinitiative.com/advisories/ZDI-25-414/

Solution

Upgrade to WEBrick version 1.8.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.2

EPSS Score

0.0005

CVSS v2.0 Base Score

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

STIG Severity

I

References

CVE	CVE-2025-6442
XREF	IAVA:2025-A-0449
XREF	ZDI:ZDI-25-414

Plugin Information

Published: 2025/06/27, Modified: 2025/07/08

Plugin Output

127.0.0.1 (tcp/0)

```
  Path              : /Library/Ruby/Gems/2.6.0/specifications/default/webrick-1.4.4.gemspec
  Installed version : 1.4.4
  Fixed version     : 1.8.2
```

127.0.0.1 (tcp/0)

```
  Path              : /opt/metasploit-framework/embedded/lib/ruby/gems/3.1.0/specifications/
webrick-1.8.1.gemspec
  Installed version : 1.8.1
  Fixed version     : 1.8.2
```

51192 (1) - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

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

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

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

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

See Also

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

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

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

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

Plugin Output

127.0.0.1 (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=Anikets-MacBook-
Air-718.local
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus
 Certification Authority
```

193568 (1) - Oracle MySQL Server 8.0.x < 8.0.37 (January 2025 CPU)

Synopsis

The remote host is affected by multiple vulnerabilities

Description

The versions of MySQL Server installed on the remote host are affected by multiple vulnerabilities as referenced in the January 2025 CPU advisory.

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging (OpenSSL)).

Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. (CVE-2023-6129)

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. (CVE-2024-21015)

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2024-20998)

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

See Also

https://www.oracle.com/security-alerts/cpuapr2024.html

https://www.oracle.com/docs/tech/security-alerts/cpuapr2024csaf.json

https://www.oracle.com/security-alerts/cpujul2024.html

https://www.oracle.com/docs/tech/security-alerts/cpujul2024csaf.json

https://www.oracle.com/security-alerts/cpujan2025.html

https://www.oracle.com/docs/tech/security-alerts/cpujan2025csaf.json

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.0191

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-6129
CVE	CVE-2024-20994
CVE	CVE-2024-20998
CVE	CVE-2024-21000
CVE	CVE-2024-21008
CVE	CVE-2024-21009
CVE	CVE-2024-21013
CVE	CVE-2024-21047
CVE	CVE-2024-21054
CVE	CVE-2024-21060
CVE	CVE-2024-21062
CVE	CVE-2024-21069
CVE	CVE-2024-21087
CVE	CVE-2024-21096
CVE	CVE-2024-21102

CVE	CVE-2024-21135
CVE	CVE-2024-21159
CVE	CVE-2024-21160
CVE	CVE-2024-21166
CVE	CVE-2024-21157
CVE	CVE-2025-21492
XREF	IAVA:2025-A-0050
XREF	IAVA:2025-A-0272

Plugin Information

Published: 2024/04/19, Modified: 2025/04/18

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /usr/local/mysql/bin
Installed version : 8.0.36
Fixed version     : 8.0.37
```

202616 (1) - Oracle MySQL Server 8.0.x < 8.0.38 (July 2024 CPU)

Synopsis

The remote host is affected by multiple vulnerabilities

Description

The versions of MySQL Server installed on the remote host are affected by multiple vulnerabilities as referenced in the July 2024 CPU advisory.

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2024-21177)

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2024-21171)

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.37 and prior and 8.4.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. (CVE-2024-21163)

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

See Also

https://www.oracle.com/security-alerts/cpujul2024.html

https://www.oracle.com/docs/tech/security-alerts/cpujul2024csaf.json

Solution

Apply the appropriate patch according to the July 2024 Oracle Critical Patch Update advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.2

EPSS Score

0.0025

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-20996
CVE	CVE-2024-21125
CVE	CVE-2024-21127
CVE	CVE-2024-21129
CVE	CVE-2024-21130
CVE	CVE-2024-21134
CVE	CVE-2024-21142
CVE	CVE-2024-21162
CVE	CVE-2024-21163
CVE	CVE-2024-21165
CVE	CVE-2024-21171
CVE	CVE-2024-21173
CVE	CVE-2024-21177
CVE	CVE-2024-21179

Plugin Information

Published: 2024/07/18, Modified: 2025/04/18

Plugin Output

127.0.0.1 (tcp/0)

```
  Path              : /usr/local/mysql/bin
  Installed version : 8.0.36
```

```
  Fixed version     : 8.0.38
```

202620 (1) - Oracle MySQL Server 8.0.x < 8.0.39 (October 2024 CPU)

Synopsis

The remote host is affected by a denial of service vulnerability

Description

The versions of MySQL Server installed on the remote host are affected by a vulnerability as referenced in the October 2024 CPU advisory.

- Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39, 8.4.1 and 9.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server.

(CVE-2024-21185)

- Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.38 and prior, 8.4.1 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2024-21207)

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

See Also

https://www.oracle.com/security-alerts/cpujul2024.html

https://www.oracle.com/docs/tech/security-alerts/cpujul2024csaf.json

https://www.oracle.com/security-alerts/cpuoct2024.html

https://www.oracle.com/docs/tech/security-alerts/cpuoct2024csaf.json

Solution

Apply the appropriate patch according to the October 2024 Oracle Critical Patch Update advisory.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0016

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-21185
CVE	CVE-2024-21207
XREF	IAVA:2024-A-0658

Plugin Information

Published: 2024/07/18, Modified: 2025/04/18

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /usr/local/mysql/bin
Installed version : 8.0.36
Fixed version     : 8.0.39
```

214534 (1) - Oracle MySQL Server 8.0.x < 8.0.41 (January 2025 CPU)

Synopsis

The remote host is affected by multiple vulnerabilities

Description

The versions of MySQL Server installed on the remote host are affected by multiple vulnerabilities as referenced in the January 2025 CPU advisory.

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2025-21522)

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2025-21518)

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.40 and prior, 8.4.3 and prior and 9.1.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2025-21501)

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

See Also

https://www.oracle.com/security-alerts/cpujan2025.html

https://www.oracle.com/docs/tech/security-alerts/cpujan2025csaf.json

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0009

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-37519
CVE	CVE-2024-11053
CVE	CVE-2025-21490
CVE	CVE-2025-21491
CVE	CVE-2025-21495
CVE	CVE-2025-21497
CVE	CVE-2025-21500
CVE	CVE-2025-21501
CVE	CVE-2025-21503
CVE	CVE-2025-21505
CVE	CVE-2025-21518
CVE	CVE-2025-21519
CVE	CVE-2025-21520
CVE	CVE-2025-21522
CVE	CVE-2025-21523
CVE	CVE-2025-21529
CVE	CVE-2025-21531
CVE	CVE-2025-21540
CVE	CVE-2025-21543
CVE	CVE-2025-21546
CVE	CVE-2025-21555
CVE	CVE-2025-21559

XREF	IAVA:2025-A-0050
XREF	IAVA:2025-A-0272

Plugin Information

Published: 2025/01/23, Modified: 2025/04/18

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /usr/local/mysql/bin
Installed version : 8.0.36
Fixed version     : 8.0.41
```

236961 (1) - VMware Fusion 13.0.x < 13.6.3 Multiple Vulnerabilities (VMSA-2025-0010)

Synopsis

A virtualization application installed on the remote macOS or Mac OS X host is affected by multiple vulnerabilities

Description

The version of VMware Fusion installed on the remote macOS or Mac OS X host is 13.0.x prior to 13.6.3. It is, therefore, affected by multiple vulnerabilities.

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?c8ce45e5

Solution

Update to VMware Fusion version 13.6.3, or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0003

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-41225
CVE	CVE-2025-41226
CVE	CVE-2025-41227
CVE	CVE-2025-41228
XREF	VMSA:2025-0010
XREF	IAVA:2025-A-0367

Plugin Information

Published: 2025/05/20, Modified: 2025/05/23

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /Applications/VMware Fusion.app
Installed version : 13.6.0
Fixed version     : 13.6.3
```

242313 (1) - Oracle MySQL Server 8.0.x < 8.0.43 (July 2025 CPU)

Synopsis

The remote host is affected by multiple vulnerabilities

Description

The versions of MySQL Server installed on the remote host are affected by a multiple vulnerabilities as referenced in the July 2025 CPU advisory.

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2025-50101)

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2025-50102)

- Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.0-8.0.42, 8.4.0-8.4.5 and 9.0.0-9.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. (CVE-2025-50104)

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

See Also

https://www.oracle.com/security-alerts/cpujul2025.html

https://www.oracle.com/docs/tech/security-alerts/cpujul2025csaf.json

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.0

EPSS Score

0.0004

CVSS v2.0 Base Score

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

STIG Severity

II

References

CVE	CVE-2025-5399
CVE	CVE-2025-50077
CVE	CVE-2025-50078
CVE	CVE-2025-50079
CVE	CVE-2025-50080
CVE	CVE-2025-50081
CVE	CVE-2025-50082
CVE	CVE-2025-50083
CVE	CVE-2025-50084
CVE	CVE-2025-50085
CVE	CVE-2025-50086
CVE	CVE-2025-50087
CVE	CVE-2025-50091
CVE	CVE-2025-50092
CVE	CVE-2025-50093
CVE	CVE-2025-50094
CVE	CVE-2025-50096
CVE	CVE-2025-50097
CVE	CVE-2025-50098
CVE	CVE-2025-50099
CVE	CVE-2025-50100
CVE	CVE-2025-50101
CVE	CVE-2025-50102
CVE	CVE-2025-50104
XREF	IAVA:2025-A-0518

Plugin Information

Published: 2025/07/18, Modified: 2025/07/18

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /usr/local/mysql/bin
Installed version : 8.0.36
Fixed version     : 8.0.43
```

242314 (1) - Oracle MySQL Server 8.0.x < 8.0.42 (July 2025 CPU)

Synopsis

The remote host is affected by a DoS vulnerability

Description

The versions of MySQL Server installed on the remote host are affected by a DoS vulnerability as referenced in the July 2025 CPU advisory.

- Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.0-8.0.41, 8.4.0-8.4.4 and 9.0.0-9.2.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. (CVE-2025-50088)

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

See Also

https://www.oracle.com/security-alerts/cpujul2025.html

https://www.oracle.com/docs/tech/security-alerts/cpujul2025csaf.json

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.4

EPSS Score

0.0004

CVSS v2.0 Base Score

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

STIG Severity

II

References

CVE	CVE-2025-50088
XREF	IAVA:2025-A-0518

Plugin Information

Published: 2025/07/18, Modified: 2025/07/18

Plugin Output

127.0.0.1 (tcp/0)

```
Path              : /usr/local/mysql/bin
Installed version : 8.0.36
Fixed version     : 8.0.42
```

14272 (26) - 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

127.0.0.1 (udp/137)

```
Port 137/udp was found to be open
```

127.0.0.1 (udp/138)

```
Port 138/udp was found to be open
```

127.0.0.1 (tcp/5000/www)

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

127.0.0.1 (udp/5353/mdns)

```
Port 5353/udp was found to be open
```

127.0.0.1 (tcp/7000/www)

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

127.0.0.1 (tcp/8834/www)

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

127.0.0.1 (udp/49556)

```
Port 49556/udp was found to be open
```

127.0.0.1 (udp/49620)

```
Port 49620/udp was found to be open
```

127.0.0.1 (udp/50326)

```
Port 50326/udp was found to be open
```

127.0.0.1 (udp/53578)

```
Port 53578/udp was found to be open
```

127.0.0.1 (tcp/53846)

```
Port 53846/tcp was found to be open
```

127.0.0.1 (udp/54637)

```
Port 54637/udp was found to be open
```

127.0.0.1 (udp/55720)

```
Port 55720/udp was found to be open
```

127.0.0.1 (udp/55794)

```
Port 55794/udp was found to be open
```

127.0.0.1 (udp/55874)

```
Port 55874/udp was found to be open
```

127.0.0.1 (udp/56838)

```
Port 56838/udp was found to be open
```

127.0.0.1 (udp/57844)

```
Port 57844/udp was found to be open
```

127.0.0.1 (udp/59344)

```
Port 59344/udp was found to be open
```

127.0.0.1 (udp/60416)

```
Port 60416/udp was found to be open
```

127.0.0.1 (udp/61242)

```
Port 61242/udp was found to be open
```

127.0.0.1 (udp/61767)

```
Port 61767/udp was found to be open
```

127.0.0.1 (udp/62826)

```
Port 62826/udp was found to be open
```

127.0.0.1 (udp/64143)

```
Port 64143/udp was found to be open
```

127.0.0.1 (udp/64209)

```
Port 64209/udp was found to be open
```

127.0.0.1 (udp/64400)

```
Port 64400/udp was found to be open
```

127.0.0.1 (udp/64954)

```
Port 64954/udp was found to be open
```

99265 (13) - macOS Remote Listeners Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/10, Modified: 2025/07/28

Plugin Output

127.0.0.1 (udp/137)

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

127.0.0.1 (udp/137)

```
The process 'netbiosd' running under the user '_netbios' is listening on this port (pid 1094).
```

127.0.0.1 (udp/138)

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

127.0.0.1 (udp/138)

```
The process 'netbiosd' running under the user '_netbios' is listening on this port (pid 1094).
```

127.0.0.1 (tcp/5000/www)

```
The process 'ControlCenter' running under the user 'aniketpandey' is listening on this port (pid
 673).
```

127.0.0.1 (udp/5353/mdns)

```
The process 'mDNSResponder' running under the user '_mdnsresponder' is listening on this port (pid
 433).
```

127.0.0.1 (tcp/7000/www)

```
The process 'ControlCenter' running under the user 'aniketpandey' is listening on this port (pid
 673).
```

127.0.0.1 (tcp/8834/www)

```
The process 'nessusd' running under the user 'root' is listening on this port (pid 5894).
```

127.0.0.1 (udp/49620)

```
The process 'zen' running under the user 'aniketpandey' is listening on this port (pid 4781).
```

127.0.0.1 (udp/50326)

```
The process 'plugin-container' running under the user 'aniketpandey' is listening on this port (pid
 4782).
```

127.0.0.1 (tcp/53846)

```
The process 'rapportd' running under the user 'aniketpandey' is listening on this port (pid 642).
```

127.0.0.1 (udp/55874)

```
The process 'plugin-container' running under the user 'aniketpandey' is listening on this port (pid
 4782).
```

127.0.0.1 (udp/64954)

```
The process 'replicatord' running under the user 'aniketpandey' is listening on this port (pid 701).
```

22964 (4) - 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

127.0.0.1 (tcp/5000/www)

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

127.0.0.1 (tcp/7000/www)

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

127.0.0.1 (tcp/8834/www)

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

127.0.0.1 (tcp/8834/www)

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

10107 (3) - 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

127.0.0.1 (tcp/5000/www)

```
The remote web server type is :

AirTunes/860.7.1
```

127.0.0.1 (tcp/7000/www)

```
The remote web server type is :

AirTunes/860.7.1
```

127.0.0.1 (tcp/8834/www)

```
The remote web server type is :

NessusWWW
```

24260 (3) - 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

127.0.0.1 (tcp/5000/www)

```
Response Code : HTTP/1.1 403 Forbidden

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

  Content-Length: 0
  Server: AirTunes/860.7.1
  X-Apple-ProcessingTime: 0
  X-Apple-RequestReceivedTimestamp: 8042937

Response Body :
```

127.0.0.1 (tcp/7000/www)

```
Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
```

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

  Content-Length: 0
  Server: AirTunes/860.7.1
  X-Apple-ProcessingTime: 0
  X-Apple-RequestReceivedTimestamp: 8051027

Response Body :
```

127.0.0.1 (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: 862b32cacee1122de9c3c75a392c0d0d
  Connection: close
  X-XSS-Protection: 1; mode=block
  Server: NessusWWW
  Date: Fri, 08 Aug 2025 12:18:26 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=1753222061535" 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=1753222061535"></script>
```

```
        <script src="p [...]
```

86383 (3) - Microsoft Office Installed (Mac OS X)

Synopsis

Microsoft Office and associated applications are installed on the remote Mac OS X host.

Description

Microsoft Office and associated applications are installed on the remote Mac OS X host.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0505

Plugin Information

Published: 2015/10/14, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/Microsoft Excel.app
Version : 16.99.2
```

127.0.0.1 (tcp/0)

```
Path    : /Applications/Microsoft PowerPoint.app
Version : 16.99.2
```

127.0.0.1 (tcp/0)

```
Path    : /Applications/Microsoft Word.app
Version : 16.99.2
```

10147 (1) - 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

127.0.0.1 (tcp/8834/www)

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

10863 (1) - 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

127.0.0.1 (tcp/8834/www)

```
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: Anikets-MacBook-Air-718.local

Issuer Name:

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

Serial Number: 00 A5 01

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Aug 08 11:46:58 2025 GMT
Not Valid After: Aug 07 11:46:58 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
```

```
Public Key: 00 90 F7 07 91 79 EF 5F 1D 04 44 44 7A D1 5D 0C 94 DC 85 17
            68 85 25 80 B2 E2 A7 52 54 B3 0B 50 47 97 66 39 00 06 CE 59
            A3 A7 40 0A 45 0A D6 F3 6C 9C 2E E7 80 99 1E B2 F2 A8 0D 75
            78 78 9F 69 9D E4 D0 D1 0D DC 62 75 99 3B F9 AB 55 2B C0 A9
            72 92 48 6A 94 AD 4E DA 89 3D 6D F6 D6 1F EB 11 D6 EB C6 2F
            3E 2E 4F A0 92 AD 6C 93 1A 37 3A 45 0B 28 FB 53 C7 DA C6 CA
            17 22 00 9F 70 E5 06 FE 21 78 BC CB 98 71 30 C2 DC A3 49 5D
            26 2B 9D AA 9E 2E 9B 68 AE 4F D6 7F F6 E7 50 05 1D 78 A8 FA
            9D 68 A6 AA 4E DB ED 0C 0A 67 1D CD 75 2C 2A 9F 33 65 80 14
            BD 85 42 29 97 A4 91 8B AA E2 2A 21 86 11 BA E5 85 ED 68 1A
            D9 B8 FA DA E5 88 F6 79 08 EE 51 D2 24 9A 15 8D 1C F2 35 7F
            2D F4 0D A8 32 65 EE 89 1C 28 35 B5 69 38 59 9B 65 0A D4 6D
            EA 4A FE 73 03 82 EE 75 19 9B 1A 42 71 49 05 1E 4F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 69 CD B7 98 7B 62 C1 B5 60 CF 34 92 2D AF 19 9D 93 86 BB
           A1 BB CA 1D 2B 84 65 54 AF 86 36 26 9C 2B CF 5E 2F B6 CE B3
           BC 34 B5 15 C4 1F 06 B4 A1 02 8D AA 44 AB 00 1C 77 38 8D 79
           CA 8C CC E5 D3 6A A0 F0 B7 7E 14 A8 53 0F DA E6 AF D6 DC 71
           BA 33 94 F6 B6 B8 10 CD 81 BC CD D6 1C DF B9 C2 13 AD 24 9C
           E7 45 12 84 72 7D C3 62 51 52 5D 17 57 D4 1E F8 7C 9A 8E FB
     [...]
```

11154 (1) - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

127.0.0.1 (tcp/53846)

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

  Port    : 53846
  Type    : spontaneous
  Banner :
0x00:  01 00 00 00                                        ....
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

127.0.0.1 (tcp/0)

```
Remote operating system : Mac OS X 15.5
Confidence level : 100
Method : uname


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

12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

127.0.0.1 (tcp/0)

```
127.0.0.1 resolves as localhost.
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/06/25

Plugin Output

127.0.0.1 (tcp/0)

```
Information about this scan :

Nessus version : 10.9.2
Nessus build : 20017
Plugin feed version : 202508080131
Scanner edition used : Nessus Home
Scanner OS : DARWIN
Scanner distribution : macosx
Scan type : Normal
```

```
Scan name : My Basic Network Scan
Scan policy used : Basic Network Scan
Scanner IP : 127.0.0.1
Ping RTT : Unavailable
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes (on the localhost)
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/8/8 17:44 IST (UTC +05:30)
Scan duration : 1028 sec
Scan for malware : no
```

21643 (1) - 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

127.0.0.1 (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}
```

22869 (1) - 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

127.0.0.1 (tcp/0)

```
Here is the list of packages installed on the remote Mac OS X system :

  Keychain Access 11.0
  Ticket Viewer 4.1
  Wireless Diagnostics 11.0
  iOS App Installer 1.0
  Finder 15.5
  AirDrop 15.5
  Computer 15.5
  Network 15.5
  Recents 15.5
  iCloud Drive 15.5
  ClassroomStudentMenuExtra 1.0
  Display Calibrator 4.19
  AOSUIPrefPaneLauncher 1.0
  AVB Configuration 1320.3
  AddPrinter 607
  AddressBookUrlForwarder 14.0
  AirPlayUIAgent 2.0
  AirPort Base Station Agent 2.2.1
  Apple Diagnostics 1.0
```

```
AppleScript Utility 1.1.2
AskToMessagesHost 1.0
Automator Application Stub 1.3
Automator Installer 2.10
Batteries 1.0
Bluetooth Setup Assistant 9.0
BluetoothUIServer 9.0
BluetoothUIService 1.0
CalendarFileHandler 8.0
Captive Network Assistant 5.0
Certificate Assistant 5.0
Control Center 1.0
ControlStrip 1.0
CoreLocationAgent 2964.0.4
CoreServicesUIAgent 369
Coverage Details 1.0
Database Events 1.0.6
Diagnostics Reporter 1.0
DiscHelper 1.0
DiskImageMounter 1.0
Dock 1.8
Dwell Control 1.0
Enhanced Logging 1.0
Erase Assistant 1.0
EscrowSecurityAlert 1.0
Family 1.0
FileProvider-Feedback 1.0
FolderActionsDispatcher 1.0
Game Center 1.0
IOUIAgent 1.0
Image Events 1.1.6
Install Command Line Developer Tools 2409
Install in Progress 3.0
Installer Progress 1.0
Installer 6.2.0
JavaLauncher 325
KeyboardAccessAgent 10
KeyboardSetupAssistant 1.0
Keychain Circle Notification 1.0
Language Chooser 1.0
MTLReplayer 304.7
ManagedClient 17.1
MediaMLPluginApp 1.0
Memory Slot Utility 1.5.3
Music Recognition 1.0
NetAuthAgent 6.2
Notification Center 1.0
NowPlayingTouchUI 1.0
OBEXAgent 9.0
ODSAgent 1.9
OSDUIHelper 1.0
PIPAgent 1.0
Paired Devices 6.6.0
Pass Viewer 1.0
PeopleMessageService 1.0
Contacts 1.0
PowerChime 1.0
PreviewShell 16.0
Pro Display Calibrator 211.0.1
Problem Reporter 10.13
Profile Installer 1.0
RapportUIAgent 6.6.0
RegisterPluginIMApp 26.200
ARDAgent 3.9.8
Remote Desktop Message 3.9.8
SSMenuAgent 3.9. [...]
```

25202 (1) - 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

127.0.0.1 (tcp/0)

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

 - ::1 (on interface lo0)
 - fe80::1 (on interface lo0)
 - fe80::846:3259:96fe:462b (on interface en0)
 - fe80::1835:43ff:fe6d:8aac (on interface awdl0)
 - fe80::1835:43ff:fe6d:8aac (on interface llw0)
 - fe80::5ab9:4358:7de5:cef7 (on interface utun0)
 - fe80::14ab:321f:c435:ce0a (on interface utun1)
 - fe80::221a:8b7e:8c60:5314 (on interface utun2)
 - fe80::ce81:b1c:bd2c:69e (on interface utun3)
 - fe80::fce2:6cff:fea0:b364 (on interface bridge100)
 - fdb2:2c26:f4e4::1 (on interface bridge100)
 - fe80::fce2:6cff:fea0:b365 (on interface bridge101)
 - fdb2:2c26:f4e4:1::1 (on interface bridge101)
```

25203 (1) - 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

127.0.0.1 (tcp/0)

```
The following IPv4 addresses are set on the remote host :

 - 127.0.0.1 (on interface lo0)
 - 10.102.143.44 (on interface en0)
 - 10.211.55.2 (on interface bridge100)
 - 10.37.129.2 (on interface bridge101)
```

33276 (1) - 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

127.0.0.1 (tcp/0)

```
The following MAC addresses exist on the remote host :

  - 06:9c:0c:63:86:73 (interface vmenet2)
  - 1a:35:43:6d:8a:ac (interfaces awdl0 & llw0)
  - d6:33:52:ba:a3:00 (interface vmenet0)
  - ba:2f:9b:2f:ae:12 (interface ap1)
  - 16:a6:61:93:f3:fb (interface en0)
  - 5a:a1:58:82:e8:96 (interface anpi0)
  - fe:e2:6c:a0:b3:64 (interface bridge100)
  - 36:2e:1e:ca:15:c4 (interface en2)
  - 36:2e:1e:ca:15:c0 (interfaces en1 & bridge0)
  - fe:e2:6c:a0:b3:65 (interface bridge101)
  - 5a:a1:58:82:e8:76 (interface en3)
  - 5a:a1:58:82:e8:77 (interface en4)
  - 5a:a1:58:82:e8:97 (interface anpi1)
  - 46:00:3f:26:1c:34 (interface vmenet1)
```

42822 (1) - 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

127.0.0.1 (tcp/8834/www)

```
The STS header line is :

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

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

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

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

Following application CPE's matched on the remote system :

  cpe:/a:anydesk:anydesk:9.1.1 -> Anydesk Anydesk for Windows
  cpe:/a:apache:http_server:2.4.62 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apple:keynote:14.4 -> Apple Keynote
  cpe:/a:apple:pages:14.4 -> Apple Pages
  cpe:/a:apple:safari:18.5 -> Apple Safari
  cpe:/a:c-ares_project:c-ares:1.34.5 -> C-ares Project C-ares
  cpe:/a:docker:docker:4.41.2 -> Docker
  cpe:/a:google:chrome:139.0.7258.66 -> Google Chrome
  cpe:/a:google:protobuf:1.24.0 -> Google Protobuf
  cpe:/a:iterm2:iterm2:1.1 -> iTerm2
  cpe:/a:iterm2:iterm2:3.5.14 -> iTerm2
```

```
cpe:/a:microsoft:autoupdate:4.79.25033028 -> Microsoft AutoUpdate for MacOS
cpe:/a:microsoft:office:excel -> Microsoft Office
cpe:/a:microsoft:office:powerpoint -> Microsoft Office
cpe:/a:microsoft:office:word -> Microsoft Office
cpe:/a:mongodb:compass:1.46.7 -> MongoDB Compass
cpe:/a:mozilla:firefox:136.0.1 -> Mozilla Firefox
cpe:/a:mozilla:firefox:136.0.1.. -> Mozilla Firefox
cpe:/a:mysql:mysql:8.0.36 -> MySQL MySQL
cpe:/a:nodejs:node.js:18.12.1 -> Nodejs Node.js
cpe:/a:openvpn:openvpn:2.6.14 -> OpenVPN
cpe:/a:ruby-lang:ruby:2.6.10 -> Ruby-lang Ruby
cpe:/a:teamviewer:teamviewer:15.68.5 -> TeamViewer
cpe:/a:tenable:nessus -> Tenable Nessus
cpe:/a:tenable:nessus:10.9.2 -> Tenable Nessus
cpe:/a:vmware:fusion:13.6.0 -> VMware Fusion
cpe:/a:wireshark:wireshark:4.4.5 -> Wireshark
cpe:/a:xmlsoft:libxml2:2.13.8 -> XMLSoft Libxml2
x-cpe:/a:anysphere:cursor:1.4.2
x-cpe:/a:apple:xprotect:5309
x-cpe:/a:google:chrome_remote_desktop:139.0.7258
x-cpe:/a:handbrake:handbrake:1.9.2
x-cpe:/a:microsoft:visual_studio_code:1.103.0
x-cpe:/a:ollama:ollama:0.11.2
x-cpe:/a:openai:chatgpt_app:1.2025.175
```

46180 (1) - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

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

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

See Also

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

Solution

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

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

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

Plugin Output

127.0.0.1 (tcp/0)

```
The following hostnames point to the remote host :
  - anikets-macbook-air-718.local
```

50828 (1) - VMware Fusion Version Detection (Mac OS X)

Synopsis

The remote Mac OS X host has a copy of VMware Fusion installed.

Description

The remote host is running VMware Fusion, a popular desktop virtualization software.

Solution

Make sure use of this program agrees with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0735

Plugin Information

Published: 2010/11/29, Modified: 2023/11/27

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/VMware Fusion.app
Version : 13.6.0
```

54615 (1) - 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

127.0.0.1 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 100
```

55417 (1) - Firefox Installed (Mac OS X)

Synopsis

The remote Mac OS X host contains a web browser.

Description

Mozilla Firefox is installed on the remote Mac OS X host.

See Also

https://www.mozilla.org/en-US/firefox/new/

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0510

Plugin Information

Published: 2011/06/24, Modified: 2024/10/16

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/Firefox.app
Version : 136.0.1
```

55472 (1) - 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: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Hostname : Anikets-MacBook-Air-718.local
  Anikets-MacBook-Air-718 (LocalHostName)
  Anikets-MacBook-Air-718.local (hostname command)
  Aniket's MacBook Air (ComputerName)
```

56468 (1) - 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

127.0.0.1 (tcp/0)

```
reboot time                               Tue Jul 29 18:32
reboot time                               Fri Aug  8 15:29
shutdown time                             Fri Aug  8 00:46
reboot time                               Tue Aug  5 23:16
shutdown time                             Tue Aug  5 01:31
reboot time                               Sun Aug  3 14:18
reboot time                               Sat Aug  2 18:57
shutdown time                             Sat Aug  2 01:05
reboot time                               Fri Aug  1 17:23
reboot time                               Thu Jul 31 18:58
shutdown time                             Thu Jul 31 00:05

wtmp begins Mon Jul 28 18:05:14 IST 2025
```

56567 (1) - Mac OS X XProtect Detection

Synopsis

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

Description

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/20, Modified: 2025/07/30

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Library/Apple/System/Library/CoreServices/XProtect.bundle
Version : 5309
```

56984 (1) - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

127.0.0.1 (tcp/8834/www)

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

57041 (1) - 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

127.0.0.1 (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}
```

58180 (1) - Mac OS X DNS Server Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

127.0.0.1 (tcp/0)

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

10.94.8.11
10.94.8.12
8.8.8.8
```

60019 (1) - Mac OS X Admin Group User List

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

127.0.0.1 (tcp/0)

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

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

64582 (1) - 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

127.0.0.1 (tcp/0)

66334 (1) - 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: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

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

[ Mozilla Firefox < 141.0 (242556) ]

+ Action to take : Upgrade to Mozilla Firefox version 141.0 or later.

+Impact : Taking this action will resolve 66 different vulnerabilities (CVEs).


[ 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). (214404) ]

+ Action to take : Upgrade to Node.js version 18.20.6 / 20.18.2 / 22.13.1 / 23.6.1 or later.

+Impact : Taking this action will resolve 44 different vulnerabilities (CVEs).


[ Oracle MySQL Server 8.0.x < 8.0.42 (July 2025 CPU) (242314) ]

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

```
+Impact : Taking this action will resolve 89 different vulnerabilities (CVEs).


[ Oracle MySQL Server 8.0.x < 8.0.43 (July 2025 CPU) (242313) ]

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

+Impact : Taking this action will resolve 24 different vulnerabilities (CVEs).


[ Ruby REXML < 3.3.6 DoS vulnerability (242630) ]

+ Action to take : Upgrade to REXML version 3.3.6 or later.


[ Ruby WEBrick < 1.8.2 HTTP Request Smuggling (240854) ]

+ Action to take : Upgrade to WEBrick version 1.8.2 or later.


[ VMware Fusion 13.0.x < 13.6.3 Multiple Vulnerabilities (VMSA-2025-0010) (236961) ]

+ Action to take : Update to VMware Fusion version 13.6.3, or later.

+Impact : Taking this action will resolve 25 different vulnerabilities (CVEs).
```

66717 (1) - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

127.0.0.1 (udp/5353/mdns)

```
Nessus was able to extract the following information :

  - mDNS hostname       : Anikets-MacBook-Air-718.local.

  - Advertised services :
    o Service name      : Aniket's MacBook Air._airplay._tcp.local.
      Port number       : 7000
    o Service name      : 9A6DDFB5FE38@Aniket's MacBook Air._raop._tcp.local.
      Port number       : 7000
    o Service name      : Aniket's MacBook Air._companion-link._tcp.local.
      Port number       : 53846
```

70610 (1) - Apple Keynote Detection (Mac OS X)

Synopsis

A presentation software application is installed on the remote Mac OS X host.

Description

Apple Keynote is installed on the remote Mac OS X host. It is an application for creating and delivering presentations.

See Also

https://www.apple.com/keynote/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/25, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/Keynote.app
Version : 14.4
```

70890 (1) - Google Chrome Installed (Mac OS X)

Synopsis

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

Description

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

See Also

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0511

Plugin Information

Published: 2013/11/13, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/Google Chrome.app
Version : 139.0.7258.66
```

72280 (1) - Apple Pages Installed (Mac OS X)

Synopsis

The remote host has an application for word processing and desktop publishing.

Description

Apple Pages is installed on the remote Mac OS X host. It is a tool for word processing and desktop publishing.

See Also

https://www.apple.com/pages/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2014/02/04, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/Pages.app
Version : 14.4
```

83991 (1) - List Installed Mac OS X Software

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0503

Plugin Information

Published: 2015/06/04, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
System Profiler managed applications:

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

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

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

ACAI_0_1_0 [version 5.7.0.1307]
  Location: /Library/Application Support/Adobe/Uninstall/ACAI_0_1_0.app

Accelerate [version 4.2.3]
  Location: /Applications/Accelerate.app

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

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

ACR_9_6 [version 5.7.0.1307]
  Location: /Library/Application Support/Adobe/Uninstall/ACR_9_6.app

Acrobat Update Helper [version 1 . 2 . 0]
  Location: /Library/Application Support/Adobe/ARMDC/Application/Acrobat Update Helper.app

AcroLicApp [version 23.006.20320]
  Location: /Library/Application Support/Adobe/Acrobat DC Helper Frameworks/OOBE/AcroLicApp.app

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

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

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

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

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

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

Adobe Acrobat Updater [version 1 . 2 . 0]
  Location: /Library/Application Support/Adobe/ARMDC/Application/Adobe  [...]
```

84503 (1) - Wireshark Installed (Mac OS X)

Synopsis

A packet capture utility is installed on the remote host.

Description

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

See Also

https://www.wireshark.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0746

Plugin Information

Published: 2015/07/02, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/Wireshark.app
Version : 4.4.5
```

86420 (1) - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2025/06/10

Plugin Output

127.0.0.1 (tcp/0)

```
The following is a consolidated list of detected MAC addresses:
  - 06:9C:0C:63:86:73
  - 1A:35:43:6D:8A:AC
  - D6:33:52:BA:A3:00
  - BA:2F:9B:2F:AE:12
  - 16:A6:61:93:F3:FB
  - 5A:A1:58:82:E8:96
  - FE:E2:6C:A0:B3:64
  - 36:2E:1E:CA:15:C4
  - 36:2E:1E:CA:15:C0
  - FE:E2:6C:A0:B3:65
  - 5A:A1:58:82:E8:76
  - 5A:A1:58:82:E8:77
  - 5A:A1:58:82:E8:97
  - 46:00:3F:26:1C:34
```

95929 (1) - macOS and Mac OS X User List Enumeration

Synopsis

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

Description

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

Solution

None

Risk Factor

None

Plugin Information

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

Plugin Output

127.0.0.1 (tcp/0)

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

User   : arsh
Groups : _appserverusr
         admin
         _appserveradm

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

User   : daemon

User   : aniketpandey
Groups : _lpadmin
         _appserverusr
         admin
         access_bpf
         _appserveradm
```

```
User   : nobody

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

User   : _timezone

User   : _mdnsresponder

User   : _cvmsroot

User   : _backgroundassets
Groups : _backgroundassets

User   : _calendar
Groups : _postgres
         certusers
         _keytabusers

User   : _qtss

User   : _krb_changepw

User   : _modelmanagerd
Groups : _modelmanagerd

User   : _sntpd
Groups : _sntpd

User   : _launchservicesd

User   : _kadmin_admin

User   : _mailman

User   : _reportsystemmemory
Groups : _reportsystemmemory

User   : _postgres

User   : _appinstalld
Groups : _appinstalld

User   : _lda

User   : _corespeechd
Groups : _corespeechd

User   : _aonsensed
Groups : _aonsensed

User   : _diskimagesiod
Groups : _diskimagesiod

User   : _coremediaiod

User   : _gamecontrollerd

User   : _installer

User   : _screensaver

User   : _nearbyd
Groups : _nearbyd

User   : _krb_kerberos

User   : _securityagent

User   : _neuralengine
```

```
Groups : _neuralengine

User   : _biome
Groups : _biome

User   : _coreaudiod

User   : _notification_proxy

User   : _mysql

User   : _cyrus
Groups : certusers

User   : _unknown

User   : _accessoryupdater
Groups : _accessoryupdater

User   : _oahd
Groups : _oahd

User   : _appstore
Groups : _appstore

User   : _krb_krbtgt

User   : _ces

User   : _driverkit
Groups : _driverkit

User   : _www

User   : _coreml
Groups : _coreml

User   : _findmydevice

User   : _windowserver

User   : _appowner

User   : _cvs

User   : _diagnosticservicesd
Groups : _diagnosticservicesd

User   : _ondemand

User   : _datadetectors

User   : _mobileasset

User   : _xserverdocs
Groups :  [...]
```

97993 (1) - 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

127.0.0.1 (tcp/0)

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

The output of "uname -a" is :
Darwin Anikets-MacBook-Air-718.local 24.5.0 Darwin Kernel Version 24.5.0: Tue Apr 22 19:48:46 PDT
 2025; root:xnu-11417.121.6~2/RELEASE_ARM64_T8103 arm64

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

OS Security Patch Assessment is available for this host.
Runtime : 1.641423 seconds
```

100129 (1) - HandBrake Installed (macOS)

Synopsis

An open source video transcoding tool is installed on the remote host.

Description

HandBrake, an open source video transcoding tool, is installed on the remote macOS or Mac OS X host.

See Also

https://handbrake.fr/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/11, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/HandBrake.app
Version : 1.9.2
```

105111 (1) - TeamViewer Installed (macOS)

Synopsis

A remote control service is installed on the remote macOS or Mac OS X host.

Description

TeamViewer, a remote management application, is installed on the remote macOS or Mac OS X host.

See Also

https://www.teamviewer.com/en-us/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/12/08, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

```
Nessus detected 2 installs of TeamViewer:

  Path    : /Library/Application Support/TeamViewer/TeamViewerUninstaller.app
  Version : 15.68.5

  Path    : /Applications/TeamViewer.app
  Version : 15.68.5
```

109279 (1) - FileVault Detection (Mac OS X)

Synopsis

Obtains Mac OS X FileVault encryption status.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/04/23, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

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

110095 (1) - 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

127.0.0.1 (tcp/0)

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

110483 (1) - 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

127.0.0.1 (tcp/0)

```
USER               PID  %CPU %MEM      VSZ    RSS   TT  STAT STARTED      TIME COMMAND
root              5894  97.0  2.1 412912048 347648   ??  R     5:23PM  15:30.50 nessusd -q
aniketpandey      4977  20.1  2.1 425910560 347248   ??  S     4:43PM  12:05.40 /Applications/
Zen.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container -isForBrowser -
prefsHandle 0:43867 -prefMapHandle 1:279510 -jsInitHandle 2:242012 -sbStartup -sbAppPath /
Applications/Zen.app -sbLevel 3 -parentBuildID 20250805051727 -ipcHandle 0 -initialChannelId
 {d374e51e-052b-4b3f-a5a2-c746bc67632a} -parentPid 4781 -greomni /Applications/Zen.app/Contents/
Resources/omni.ja -appomni /Applications/Zen.app/Contents/Resources/browser/omni.ja -appDir /
Applications/Zen.app/Contents/Resources/browser -profile /Users/aniketpandey/Library/Application
 Support/zen/Profiles/1cs5t0e0.Default (release) org.mozilla.machname.461231399 30 tab
aniketpandey      4781  11.4  3.5 423875232 588976   ??  S     4:38PM   9:59.88 /Applications/
Zen.app/Contents/MacOS/zen
_windowserver      402   7.0  0.8 414060528 130480   ??  Ss    3:29PM  21:36.78 /System/Library/
PrivateFrameworks/SkyLight.framework/Resources/WindowServer -daemon
aniketpandey      4782   6.2  0.2 410341760  36544   ??  S     4:38PM   4:42.23 /Applications/
Zen.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container -parentBuildID
 20250805051727 -prefsHandle 0:39140 -prefMapHandle 1:279510 -sbStartup -sbAppPath /Applications/
Zen.app -ipcHandle 0 -initialChannelId {1a9f8050-87c8-4371-82f8-f3748018afc6} -parentPid 4781
 -appDir /Applications/Zen.app/Contents/Resources/browser -profile /Users/aniketpandey/Library/
Application Support/zen/Profiles/1cs5t0e0.Default (release) org.mozilla.machname.1405678326 1 socket
root              6257   6.2 18.8 414253552 3154912   ??  S     5:34PM   5:47.65 /Applications/
Parallels Desktop.app/Contents/MacOS//Parallels VM.app/Contents/MacOS/prl_vm_app --vm-name CentOS
 Linux --uuid {424c4d17-d6cf-4d76-bd54-b0c53e8e221e} --dir-uuid {f6ff6cf2-6e5a-43a0-8 [...]
```

117887 (1) - 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

127.0.0.1 (tcp/0)

```
OS Security Patch Assessment is available.

Protocol : LOCAL
```

125406 (1) - Apple Safari Installed (macOS)

Synopsis

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

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/05/28, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

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

129055 (1) - Microsoft Visual Studio Code Installed (Mac OS X)

Synopsis

A code editor is installed on the remote host.

Description

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

See Also

https://code.visualstudio.com/

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/09/19, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/Visual Studio Code.app
Version : 1.103.0
```

131568 (1) - Serial Number Identification (macOS)

Synopsis

Detects the serial number of the remote macOS host.

Description

The Serial Number was detected on the remote macOS host.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/12/03, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Serial Number : C02H907NQ6M1
```

133180 (1) - Google Chrome Browser Extension Enumeration (macOS)

Synopsis

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

Description

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

See Also

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

Solution

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

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

Risk Factor

None

Plugin Information

Published: 2020/01/23, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

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

    Name        : Pesticide
    Description : A CSS debugging tool that inserts outlines onto all elements to help with
 debugging layout issues
    Version     : 2.0.0
    Path        : /Users/aniketpandey/Library/Application Support/Google/Chrome/Default/Extensions/
bakpbgckdnepkmkeaiomhmfcnejndkbi/2.0.0_0/

    Name        : __MSG_extName__
    Description : Autofill the matched code
    Version     : 8.0.1
    Path        : /Users/aniketpandey/Library/Application Support/Google/Chrome/Default/Extensions/
bhghoamapcdpbohphigoooaddinpkbai/8.0.1_0/

    Name        : __MSG_extName__
    Description : __MSG_extShortDesc__
```

```
    Version     : 1.3.2.1
    Path        : /Users/aniketpandey/Library/Application Support/Google/Chrome/Default/Extensions/
chnccghejnflbccphgkncbmllhfljdfa/1.3.2.1_0/

    Name        : NeoExamShield
    Description : Prevents malpractice by identifying and blocking third-party browser extensions
 during tests on the Iamneo portal.
    Version     : 3.3
    Path        : /Users/aniketpandey/Library/Application Support/Google/Chrome/Default/Extensions/
deojfdehldjjfmcjcfaojgaibalafifc/3.3_0/

    Name        : HTML Tree Generator
    Description : Html is really a tree of elements, css is what defines the layout. This extension
 displays any page as a tree.
    Version     : 1.0
    Path        : /Users/aniketpandey/Library/Application Support/Google/Chrome/Default/Extensions/
dlbbmhhaadfnbbdnjalilhdakfmiffeg/1.0_0/

    Name    : JSON Viewer Pro
    Version : 1.0.6
    Path    : /Users/aniketpandey/Library/Application Support/Google/Chrome/Default/Extensions/
eifflpmocdbdmepbjaopkkhbfmdgijcc/1.0.6_0/

    Name        : Polypane helper
    Description : Open current tab in Polypane
    Version     : 2.0.0
    Path        : /Users/aniketpandey/Library/Application Support/Google/Chrome/Default/Extensions/
eofbapfmbfmpeplodnehlkkgpkklmapp/2.0.0_0/

    Name        : __MSG_extName__
    Description : __MSG_extDesc__
    Version     : 1.90.1
 [...]
```

136318 (1) - 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

127.0.0.1 (tcp/8834/www)

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

138330 (1) - 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

127.0.0.1 (tcp/8834/www)

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

141118 (1) - 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

127.0.0.1 (tcp/0)

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

141394 (1) - 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: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

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

Configs found :

Loaded modules :
```

142902 (1) - MySQL Installed (Mac OS X)

Synopsis

MySQL is installed on the remote Mac OS X host.

Description

MySQL, a database management system, is installed on the remote Mac OS X host.

See Also

https://www.mysql.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/11/16, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /usr/local/mysql/bin
Version : 8.0.36
```

142903 (1) - Node.js Installed (macOS)

Synopsis

Node.js is installed on the remote macOS host.

Description

Node.js is installed on the remote macOS host.

See Also

https://nodejs.org/en/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/11/16, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /usr/local/bin/node
Version : 18.12.1
```

152743 (1) - Unix Software Discovery Commands Not Available

Synopsis

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

Description

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

Details of the issues encountered are reported by this plugin.

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

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

* Inadequate scan user permissions,

* Failed privilege escalation,

* Intermittent network disruption, or

* Missing or corrupt executables on the target host.

Please address the issues reported here and redo the scan.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

127.0.0.1 (tcp/0)

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

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


Protocol : LOCAL
```

163326 (1) - 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: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /opt/nessus
Version : 10.9.2
Build   : 20017
```

168392 (1) - Tenable Nessus Installed (macOS)

Synopsis

Tenable Nessus is installed on the remote macOS host.

Description

Tenable Nessus is installed on the remote macOS host.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/12/05, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Path           : /Library/Nessus/run/sbin/nessusd
Version        : 10.9.2
Build          : 20017
Version Source : /Library/Nessus/run/var/nessus/nessus.version
```

168980 (1) - 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: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

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

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

170170 (1) - 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

127.0.0.1 (tcp/0)

```
bridge101:
  MAC : fe:e2:6c:a0:b3:65
  Status :  active
  IPv4:
    - Address : 10.37.129.2
        Netmask : 255.255.255.0
        Broadcast : 10.37.129.255
  IPv6:
    - Address : fe80::fce2:6cff:fea0:b365
        Prefixlen : 64
        Scope : bridge101
        ScopeID : 0x17
    - Address : fdb2:2c26:f4e4:1::1
        Prefixlen : 64
bridge100:
  MAC : fe:e2:6c:a0:b3:64
  Status :  active
  IPv4:
    - Address : 10.211.55.2
        Netmask : 255.255.255.0
        Broadcast : 10.211.55.255
  IPv6:
    - Address : fe80::fce2:6cff:fea0:b364
        Prefixlen : 64
        Scope : bridge100
        ScopeID : 0x15
    - Address : fdb2:2c26:f4e4::1
        Prefixlen : 64
utun0:
  IPv6:
    - Address : fe80::5ab9:4358:7de5:cef7
```

```
        Prefixlen : 64
        Scope : utun0
        ScopeID : 0xf
lo0:
  IPv4:
    - Address : 127.0.0.1
        Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
        Prefixlen : 128
    - Address : fe80::1
        Prefixlen : 64
        Scope : lo0
        ScopeID : 0x1
vmenet0:
  MAC : d6:33:52:ba:a3:00
  Status :  active
utun2:
  IPv6:
    - Address : fe80::221a:8b7e:8c60:5314
        Prefixlen : 64
        Scope : utun2
        ScopeID : 0x11
en0:
  MAC : 16:a6:61:93:f3:fb
  Status :  active
  IPv4:
    - Address : 10.102.143.44
        Netmask : 255.255.248.0
        Broadcast : 10.102.143.255
  IPv6:
    - Address : fe80::846:3259:96fe:462b
        Prefixlen : 64
        Scope : en0
        ScopeID : 0xb
vmenet2:
  MAC : 06:9c:0c:63:86:73
  Status :  active
en2:
  MAC : 36:2e:1e:ca:15:c4
  Status :  inactive
anpi1:
  MAC : 5a:a1:58:82:e8:97
  Status :  inactive
stf0:
anpi0:
  MAC : 5a:a1:58:82:e8:96
  Status :  inactive
en3:
  MAC : 5a:a1:58:82:e8:76
  Status :  inactive
utun3:
  IPv6:
    - Address : fe80::ce81:b1c:bd2c:69e
        Prefixlen : 64
        Scope : utun3
        ScopeID : 0x12
utun1:
  IPv6:
    - Address : fe80::14ab:321f:c435:ce0a
        Prefixlen : 64
        Scope : utun1
        ScopeID : 0x10
en1:
  MAC : 36:2e:1e:ca:15:c0
  Status :  inactive
llw0:
  MAC : 1a:35:4 [...]
```

174736 (1) - Netstat Ingress Connections

Synopsis

External connections are enumerated via the 'netstat' command.

Description

This plugin runs 'netstat' to enumerate any non-private connections to the scan target.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/04/25, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

```
Netstat output indicated the following connections from non-private IP addresses:

101.6.15.130 connected to port 54637 on the scan target.

NOTE: This list may be truncated depending on the scan verbosity settings.
```

176073 (1) - Google Protobuf Go Module Installed (macOS)

Synopsis

Google Protobuf module for Go is installed on the remote macOS host

Description

Google Protobuf module for Go is installed on the remote macOS host

See Also

https://pkg.go.dev/google.golang.org/protobuf

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/05/18, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
  Path    : /Users/aniketpandey/go/pkg/mod/google.golang.org/protobuf@v1.24.0/internal/version/
version.go
  Version : 1.24.0
```

179200 (1) - 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

127.0.0.1 (tcp/0)

```
Gateway Routes:
  en0:
    ipv4_gateways:
      10.102.136.1:
        subnets:
         - 0.0.0.0/0
  utun0:
    ipv6_gateways:
      fe80::%utun0:
        subnets:
         - ::/0
  utun1:
    ipv6_gateways:
      fe80::%utun1:
        subnets:
         - ::/0
  utun2:
    ipv6_gateways:
      fe80::%utun2:
        subnets:
         - ::/0
  utun3:
    ipv6_gateways:
      fe80::%utun3:
        subnets:
         - ::/0
Interface Routes:
  bridge100:
    ipv4_subnets:
     - 0.0.0.0/0
     - 10.211.55.0/24
```

```
    ipv6_subnets:
     - fdb2:2c26:f4e4::/64
     - fe80::/64
  bridge101:
    ipv4_subnets:
     - 0.0.0.0/0
     - 10.37.129.0/24
    ipv6_subnets:
     - fdb2:2c26:f4e4:1::/64
     - fe80::/64
  en0:
    ipv4_subnets:
     - 10.102.136.0/21
     - 169.254.0.0/16
    ipv6_subnets:
     - fe80::/64
  lo0:
    ipv4_subnets:
     - 127.0.0.0/8
    ipv6_subnets:
     - fe80::/64
  utun0:
    ipv6_subnets:
     - fe80::/64
  utun1:
    ipv6_subnets:
     - fe80::/64
  utun2:
    ipv6_subnets:
     - fe80::/64
  utun3:
    ipv6_subnets:
     - fe80::/64
```

180577 (1) - Docker Installed (macOS)

Synopsis

Docker is installed on the remote macOS host.

Description

Docker is installed on the remote macOS host.

See Also

https://www.docker.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/07, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/Docker.app
Version : 4.41.2
```

187860 (1) - MacOS NetBIOS Identity Information

Synopsis

Detects NetBIOS identity for macOS systems

Description

Detects NetBIOS identity for macOS systems

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/10, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
NetBIOSName        : MACBOOKAIR-00B3
LocalKerberosRealm : LKDC:SHA1.F7E0786ECFBC714A1333FB9BBCE07D607E89049D
ServerDescription  : Aniket's MacBook Air
DOSCodePage        : 437
```

189955 (1) - AnyDesk Installed (macOS)

Synopsis

AnyDesk is installed on the remote macOS host.

Description

AnyDesk is installed on the remote macOS host.

See Also

https://anydesk.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/02/02, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/AnyDesk.app
Version : 9.1.1
```

191144 (1) - Ruby Programming Language Installed (macOS)

Synopsis

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

Description

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

See Also

https://ruby.org/en/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/02/29, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

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

193143 (1) - 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

127.0.0.1 (tcp/0)

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

207916 (1) - iTerm2 Installed (macOS)

Synopsis

iTerm2, a terminal emulator, is installed on the remote macOS host.

Description

iTerm2, a terminal emulator, is installed on the remote macOS host.

See Also

https://iterm2.com/downloads.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/09/30, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

```
Nessus detected 2 installs of iTerm2:

  Path    : /Applications/iTerm.app
  Version : 3.5.14

  Path    : /Applications/iTermAI.app
  Version : 1.1
```

209654 (1) - 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

127.0.0.1 (tcp/0)

```
Following OS Fingerprints were found

Remote operating system : Mac OS X 15.5
Confidence level : 100
Method : uname
Type : general-purpose
Fingerprint : uname:Darwin Anikets-MacBook-Air-718.local 24.5.0 Darwin Kernel Version 24.5.0: Tue
 Apr 22 19:48:46 PDT 2025; root:xnu-11417.121.6~2/RELEASE_ARM64_T8103 arm64


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

SSLcert:!:i/CN:Nessus Certification Authorityi/O:Nessus Users Unitedi/OU:Nessus Certification
 Authoritys/CN:Anikets-MacBook-Air-718.locals/O:Nessus Users Uniteds/OU:Nessus Server
28899592dfb36aebe32c81720c598a66d878b50d
```

232694 (1) - Google Chrome Remote Desktop Installed (macOS)

Synopsis

Google Chrome Remote Desktop is installed on the remote macOS host.

Description

Google Chrome Remote Desktop is installed on the remote macOS host.

See Also

https://remotedesktop.google.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/03/13, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Library/PrivilegedHelperTools/ChromeRemoteDesktopHost.app
Version : 139.0.7258
```

232857 (1) - OpenVPN Installed (macOS)

Synopsis

OpenVPN is installed on the remote macOS host.

Description

OpenVPN is installed on the remote macOS 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: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /opt/homebrew/Cellar/openvpn/2.6.14/sbin/openvpn
Version : 2.6.14
```

233957 (1) - Microsoft AutoUpdate Installed (macOS)

Synopsis

Microsoft AutoUpdate is installed on the remote macOS host.

Description

Microsoft AutoUpdate is installed on the remote macOS host.

See Also

https://rustdesk.com/

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

127.0.0.1 (tcp/0)

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

234216 (1) - MongoDB Compass Installed (macOS)

Synopsis

MongoDB Compass is installed on the remote macOS host.

Description

MongoDB Compass is installed on the remote macOS host.

See Also

https://www.mongodb.com/products/tools/compass

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/04/11, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/MongoDB Compass.app
Version : 1.46.7
```

234804 (1) - c-ares Installed (macOS)

Synopsis

c-ares is installed on the remote macOS host.

Description

c-ares is installed on the remote macOS host.

See Also

https://formulae.brew.sh/formula/c-ares

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/04/24, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /opt/homebrew/Cellar/c-ares/1.34.5
Version : 1.34.5
```

234892 (1) - libxml2 Installed (macOS)

Synopsis

libxml2 is installed on the remote macOS host.

Description

libxml2 is installed on the remote macOS host.

See Also

https://formulae.brew.sh/formula/libxml2

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/04/28, Modified: 2025/07/14

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /opt/homebrew/Cellar/libxml2/2.13.8
Version : 2.13.8
```

240646 (1) - Ruby Gem Modules Installed (macOS)

Synopsis

Nessus was able to enumerate one or more Ruby Gem modules installed on the remote host.

Description

Nessus was able to enumerate one or more Ruby Gem modules installed on the remote host.
Note that 'Perform thorough tests' may be required for an in-depth search of all Ruby Gem modules.

See Also

http://www.nessus.org/u?26bc7c8b

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/06/26, Modified: 2025/07/28

Plugin Output

127.0.0.1 (tcp/0)

```
690 Installed Ruby Gems :

name: Ascii85
version: 2.0.1
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.2.0/specifications/Ascii85-2.0.1.gemspec

name: Ascii85
version: 1.1.1
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.2.0/specifications/Ascii85-1.1.1.gemspec

name: aarch64
version: 2.1.0
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.2.0/specifications/aarch64-2.1.0.gemspec

name: abbrev
version: 0.1.1
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.2.0/specifications/default/
abbrev-0.1.1.gemspec

name: abbrev
version: 0.1.0
```

```
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.1.0/specifications/default/
abbrev-0.1.0.gemspec

name: abbrev
version: 0.1.2
path: /opt/homebrew/Library/Homebrew/vendor/portable-ruby/3.3.7/lib/ruby/gems/3.3.0/specifications/
default/abbrev-0.1.2.gemspec

name: actionpack
version: 7.0.8.6
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.2.0/specifications/
actionpack-7.0.8.6.gemspec

name: actionpack
version: 7.0.8.7
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.2.0/specifications/
actionpack-7.0.8.7.gemspec

name: actionpack
version: 7.0.8.4
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.1.0/specifications/
actionpack-7.0.8.4.gemspec

name: actionview
version: 7.0.8.6
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.2.0/specifications/
actionview-7.0.8.6.gemspec

name: actionview
version: 7.0.8.7
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.2.0/specifications/
actionview-7.0.8.7.gemspec

name: actionview
version: 7.0.8.4
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.1.0/specifications/
actionview-7.0.8.4.gemspec

name: activemodel
version: 7.0.8.6
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.2.0/specifications/
activemodel-7.0.8.6.gemspec

name: activemodel
version: 7.0.8.7
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.2.0/specifications/
activemodel-7.0.8.7.gemspec

name: activemodel
version: 7.0.8.4
path: /opt/metasploit-framework/embedded/lib/ruby/gems/3.1.0/specifi [...]
```

243922 (1) - Anysphere Cursor Installed (macOS)

Synopsis

Anysphere Cursor is installed on the remote macOS host.

Description

Anysphere Cursor is installed on the remote macOS host.

See Also

https://cursor.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/08/06, Modified: 2025/08/06

Plugin Output

127.0.0.1 (tcp/0)

```
Path    : /Applications/Cursor.app
Version : 1.4.2
```