cred

Report generated by Tenable Nessus™ Mon, 31 Mar 2025 15:01:18 GMT Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.230.146

12	39	5	0	173
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Mon Mar 31 14:41:44 2025
End time: Mon Mar 31 15:01:17 2025

Host Information

Netbios Name: WINDOWS11
IP: 192.168.230.146
MAC Address: 6C:A1:00:53:70:73 08:00:27:11:82:D0
OS: Microsoft Windows 11 Home Build 26100

Vulnerabilities

210851 - KB5046617: Windows 11 Version 24H2 / Windows Server 2025 Security Update (November 2024)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5046617 and Hot Patch 5046696. It is, therefore, affected by multiple vulnerabilities

- Windows Kerberos Remote Code Execution Vulnerability (CVE-2024-43639)

- Windows NT OS Kernel Elevation of Privilege Vulnerability (CVE-2024-43623)

- Windows Telephony Service Elevation of Privilege Vulnerability (CVE-2024-43626)

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://support.microsoft.com/help/5046617

https://support.microsoft.com/help/5046696

Solution

Apply Security Update 5046617 or Hot Patch 5046696

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

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

10.0

EPSS Score

0.8703

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

8.7 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-38203
CVE	CVE-2024-38264
CVE	CVE-2024-43449
CVE	CVE-2024-43450
CVE	CVE-2024-43451
CVE	CVE-2024-43452
CVE	CVE-2024-43620
CVE	CVE-2024-43621
CVE	CVE-2024-43622
CVE	CVE-2024-43623

CVE	CVE-2024-43624
CVE	CVE-2024-43625
CVE	CVE-2024-43626
CVE	CVE-2024-43627
CVE	CVE-2024-43628
CVE	CVE-2024-43629
CVE	CVE-2024-43630
CVE	CVE-2024-43631
CVE	CVE-2024-43633
CVE	CVE-2024-43634
CVE	CVE-2024-43635
CVE	CVE-2024-43636
CVE	CVE-2024-43637
CVE	CVE-2024-43638
CVE	CVE-2024-43639
CVE	CVE-2024-43641
CVE	CVE-2024-43642
CVE	CVE-2024-43643
CVE	CVE-2024-43644
CVE	CVE-2024-43646
CVE	CVE-2024-49019
CVE	CVE-2024-49039
CVE	CVE-2024-49046
MSKB	5046617
MSKB	5046696
XREF	MSFT:MS24-5046617
XREF	MSFT:MS24-5046696
XREF	CISA-KNOWN-EXPLOITED:2024/12/03
XREF	IAVA:2024-A-0729-S
XREF	IAVA:2024-A-0730-S

Plugin Information

Published: 2024/11/12, Modified: 2025/01/23

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5046617
  - 5046696

  - C:\WINDOWS\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.26100.1742
    Should be      : 10.0.26100.2314
```

214124 - KB5050009: Windows 11 Version 24H2 / Windows Server 2025 Security Update (January 2025)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5050009. It is, therefore, affected by multiple vulnerabilities

- Windows NTLM V1 Elevation of Privilege Vulnerability (CVE-2025-21311)

- Windows Telephony Service Remote Code Execution Vulnerability (CVE-2025-21223, CVE-2025-21233, CVE-2025-21236, CVE-2025-21237, CVE-2025-21238, CVE-2025-21239, CVE-2025-21240, CVE-2025-21241, CVE-2025-21243, CVE-2025-21244, CVE-2025-21245, CVE-2025-21246, CVE-2025-21248, CVE-2025-21250, CVE-2025-21252, CVE-2025-21266, CVE-2025-21273, CVE-2025-21282, CVE-2025-21286, CVE-2025-21302, CVE-2025-21303, CVE-2025-21305, CVE-2025-21306, CVE-2025-21339, CVE-2025-21409, CVE-2025-21411, CVE-2025-21413, CVE-2025-21417)

- Windows BitLocker Information Disclosure Vulnerability (CVE-2025-21210, CVE-2025-21214)

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://support.microsoft.com/help/5050009

Solution

Apply Security Update 5050009

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

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.4

EPSS Score

0.4332

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

8.7 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-7344
CVE	CVE-2025-21189
CVE	CVE-2025-21193
CVE	CVE-2025-21202
CVE	CVE-2025-21207
CVE	CVE-2025-21210
CVE	CVE-2025-21211
CVE	CVE-2025-21213
CVE	CVE-2025-21214
CVE	CVE-2025-21215
CVE	CVE-2025-21217
CVE	CVE-2025-21218
CVE	CVE-2025-21219
CVE	CVE-2025-21220
CVE	CVE-2025-21223
CVE	CVE-2025-21224
CVE	CVE-2025-21225
CVE	CVE-2025-21226
CVE	CVE-2025-21227
CVE	CVE-2025-21228
CVE	CVE-2025-21229
CVE	CVE-2025-21230
CVE	CVE-2025-21231
CVE	CVE-2025-21232
CVE	CVE-2025-21233
CVE	CVE-2025-21234
CVE	CVE-2025-21235

CVE	CVE-2025-21236
CVE	CVE-2025-21237
CVE	CVE-2025-21238
CVE	CVE-2025-21239
CVE	CVE-2025-21240
CVE	CVE-2025-21241
CVE	CVE-2025-21242
CVE	CVE-2025-21243
CVE	CVE-2025-21244
CVE	CVE-2025-21245
CVE	CVE-2025-21246
CVE	CVE-2025-21248
CVE	CVE-2025-21249
CVE	CVE-2025-21250
CVE	CVE-2025-21251
CVE	CVE-2025-21252
CVE	CVE-2025-21255
CVE	CVE-2025-21256
CVE	CVE-2025-21257
CVE	CVE-2025-21258
CVE	CVE-2025-21260
CVE	CVE-2025-21261
CVE	CVE-2025-21263
CVE	CVE-2025-21265
CVE	CVE-2025-21266
CVE	CVE-2025-21268
CVE	CVE-2025-21269
CVE	CVE-2025-21270
CVE	CVE-2025-21272
CVE	CVE-2025-21273
CVE	CVE-2025-21274
CVE	CVE-2025-21275
CVE	CVE-2025-21276
CVE	CVE-2025-21277
CVE	CVE-2025-21278
CVE	CVE-2025-21280
CVE	CVE-2025-21281
CVE	CVE-2025-21282
CVE	CVE-2025-21284
CVE	CVE-2025-21285
CVE	CVE-2025-21286
CVE	CVE-2025-21287
CVE	CVE-2025-21288

CVE	CVE-2025-21289
CVE	CVE-2025-21290
CVE	CVE-2025-21292
CVE	CVE-2025-21293
CVE	CVE-2025-21294
CVE	CVE-2025-21295
CVE	CVE-2025-21296
CVE	CVE-2025-21297
CVE	CVE-2025-21298
CVE	CVE-2025-21299
CVE	CVE-2025-21300
CVE	CVE-2025-21301
CVE	CVE-2025-21302
CVE	CVE-2025-21303
CVE	CVE-2025-21305
CVE	CVE-2025-21306
CVE	CVE-2025-21307
CVE	CVE-2025-21308
CVE	CVE-2025-21309
CVE	CVE-2025-21310
CVE	CVE-2025-21311
CVE	CVE-2025-21313
CVE	CVE-2025-21314
CVE	CVE-2025-21315
CVE	CVE-2025-21316
CVE	CVE-2025-21317
CVE	CVE-2025-21318
CVE	CVE-2025-21319
CVE	CVE-2025-21320
CVE	CVE-2025-21321
CVE	CVE-2025-21323
CVE	CVE-2025-21324
CVE	CVE-2025-21325
CVE	CVE-2025-21326
CVE	CVE-2025-21327
CVE	CVE-2025-21328
CVE	CVE-2025-21329
CVE	CVE-2025-21330
CVE	CVE-2025-21332
CVE	CVE-2025-21333
CVE	CVE-2025-21334
CVE	CVE-2025-21335
CVE	CVE-2025-21336

CVE	CVE-2025-21338
CVE	CVE-2025-21339
CVE	CVE-2025-21340
CVE	CVE-2025-21341
CVE	CVE-2025-21343
CVE	CVE-2025-21370
CVE	CVE-2025-21372
CVE	CVE-2025-21374
CVE	CVE-2025-21378
CVE	CVE-2025-21382
CVE	CVE-2025-21389
CVE	CVE-2025-21409
CVE	CVE-2025-21411
CVE	CVE-2025-21413
CVE	CVE-2025-21417
MSKB	5050009
XREF	MSFT:MS25-5050009
XREF	CISA-KNOWN-EXPLOITED:2025/02/04
XREF	IAVA:2025-A-0034-S
XREF	IAVA:2025-A-0033-S

Plugin Information

Published: 2025/01/14, Modified: 2025/02/14

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5050009

  - C:\WINDOWS\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.26100.1742
    Should be      : 10.0.26100.2894
```

193282 - Microsoft Edge (Chromium) < 123.0.2420.97 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 123.0.2420.97. It is, therefore, affected by multiple vulnerabilities as referenced in the April 12, 2024 advisory.

- Out of bounds memory access in Compositing in Google Chrome prior to 123.0.6312.122 allowed a remote attacker who had compromised the GPU process to potentially perform a sandbox escape via specific UI gestures. (Chromium security severity: High) (CVE-2024-3157)

- Use after free in Dawn in Google Chrome prior to 123.0.6312.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-3515)

- Heap buffer overflow in ANGLE in Google Chrome prior to 123.0.6312.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-3516)

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?abaee145

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3157

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3515

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3516

Solution

Upgrade to Microsoft Edge version 123.0.2420.97 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.3

EPSS Score

0.0068

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)

References

CVE	CVE-2024-3157
CVE	CVE-2024-3515
CVE	CVE-2024-3516

Plugin Information

Published: 2024/04/12, Modified: 2024/12/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 123.0.2420.97
```

197287 - Microsoft Edge (Chromium) < 124.0.2478.109 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 124.0.2478.109. It is, therefore, affected by multiple vulnerabilities as referenced in the May 16, 2024 advisory.

- Microsoft Edge (Chromium-based) Information Disclosure Vulnerability (CVE-2024-30056)

- Type Confusion in V8 in Google Chrome prior to 125.0.6422.60 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) (CVE-2024-4947)

- Use after free in Dawn in Google Chrome prior to 125.0.6422.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-4948)

- Use after free in V8 in Google Chrome prior to 125.0.6422.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-4949)

- Inappropriate implementation in Downloads in Google Chrome prior to 125.0.6422.60 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-4950)

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?ca40dca9

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4947

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4948

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4949

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4950

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30056

Solution

Upgrade to Microsoft Edge version 124.0.2478.109 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.2

EPSS Score

0.2346

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-2024-4947
CVE	CVE-2024-4948
CVE	CVE-2024-4949
CVE	CVE-2024-4950
CVE	CVE-2024-30056
XREF	CISA-KNOWN-EXPLOITED:2024/06/10
XREF	IAVA:2024-A-0306-S

Plugin Information

Published: 2024/05/17, Modified: 2024/11/28

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 124.0.2478.109
```

195318 - Microsoft Edge (Chromium) < 124.0.2478.97 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 124.0.2478.97. It is, therefore, affected by multiple vulnerabilities as referenced in the May 10, 2024 advisory.

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2024-30055)

- Use after free in ANGLE in Google Chrome prior to 124.0.6367.155 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-4558)

- Heap buffer overflow in WebAudio in Google Chrome prior to 124.0.6367.155 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-4559)

- Use after free in Visuals in Google Chrome prior to 124.0.6367.201 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

(Chromium security severity: High) (CVE-2024-4671)

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?8823f93e

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30055

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4558

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4559

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4671

Solution

Upgrade to Microsoft Edge version 124.0.2478.97 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.1

EPSS Score

0.0614

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-2024-4558
CVE	CVE-2024-4559
CVE	CVE-2024-4671
CVE	CVE-2024-30055
XREF	CISA-KNOWN-EXPLOITED:2024/06/03
XREF	IAVA:2024-A-0274-S

Plugin Information

Published: 2024/05/10, Modified: 2024/05/24

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 124.0.2478.97
```

202467 - Microsoft Edge (Chromium) < 125.0.2535.67 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 125.0.2535.67. It is, therefore, affected by multiple vulnerabilities as referenced in the May 16, 2024 advisory.

- Use after free in Scheduling in Google Chrome prior to 125.0.6422.76 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5157)

- Type Confusion in V8 in Google Chrome prior to 125.0.6422.76 allowed a remote attacker to potentially perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5158)

- Heap buffer overflow in ANGLE in Google Chrome prior to 125.0.6422.76 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5159)

- Heap buffer overflow in Dawn in Google Chrome prior to 125.0.6422.76 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5160)

- Type Confusion in V8. (CVE-2024-5274)

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?4c157b4b

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5157

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5158

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5159

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5160

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5274

Solution

Upgrade to Microsoft Edge version 125.0.2535.67 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.1

EPSS Score

0.3449

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)

References

CVE	CVE-2024-5157
CVE	CVE-2024-5158
CVE	CVE-2024-5159
CVE	CVE-2024-5160
CVE	CVE-2024-5274
XREF	CISA-KNOWN-EXPLOITED:2024/06/18

Plugin Information

Published: 2024/07/16, Modified: 2024/11/28

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 125.0.2535.67
```

202635 - Microsoft Edge (Chromium) < 126.0.2592.113 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 126.0.2592.113. It is, therefore, affected by multiple vulnerabilities as referenced in the July 18, 2024 advisory.

- Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6772)

- Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6773)

- Use after free in Screen Capture in Google Chrome prior to 126.0.6478.182 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6774)

- Use after free in Media Stream in Google Chrome prior to 126.0.6478.182 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6775)

- Use after free in Audio in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6776)

- Use after free in Navigation in Google Chrome prior to 126.0.6478.182 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High) (CVE-2024-6777)

- Race in DevTools in Google Chrome prior to 126.0.6478.182 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: High) (CVE-2024-6778)

- Out of bounds memory access in V8 in Google Chrome prior to 126.0.6478.182 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6779)

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?b16da4f7

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6772

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6773

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6774

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6775

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6776
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6777
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6778
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6779

Solution

Upgrade to Microsoft Edge version 126.0.2592.113 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

EPSS Score

0.3959

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)

References

CVE	CVE-2024-6772
CVE	CVE-2024-6773
CVE	CVE-2024-6774
CVE	CVE-2024-6775
CVE	CVE-2024-6776
CVE	CVE-2024-6777
CVE	CVE-2024-6778
CVE	CVE-2024-6779

Plugin Information

Published: 2024/07/18, Modified: 2024/12/31

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 126.0.2592.113
```

205222 - Microsoft Edge (Chromium) < 127.0.2651.98 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 127.0.2651.98. It is, therefore, affected by multiple vulnerabilities as referenced in the August 8, 2024 advisory.

- Out of bounds memory access in ANGLE in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) (CVE-2024-7532)

- Use after free in Sharing in Google Chrome on iOS prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7533)

- Heap buffer overflow in Layout in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7534)

- Inappropriate implementation in V8 in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7535)

- Use after free in WebAudio in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7536)

- Type Confusion in V8 in Google Chrome prior to 127.0.6533.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7550)

- Microsoft Edge (HTML-based) Memory Corruption Vulnerability (CVE-2024-38218)

- Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability (CVE-2024-38219)

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?61fb8dc0

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38218

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38219

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7532

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7533

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7534

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7535

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7536

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7550

Solution

Upgrade to Microsoft Edge version 127.0.2651.98 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.3

EPSS Score

0.004

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-2024-7532
CVE	CVE-2024-7533
CVE	CVE-2024-7534
CVE	CVE-2024-7535
CVE	CVE-2024-7536
CVE	CVE-2024-7550
CVE	CVE-2024-38218
CVE	CVE-2024-38219

XREF IAVA:2024-A-0489-S

Plugin Information

Published: 2024/08/08, Modified: 2024/08/30

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 127.0.2651.98
```

206172 - Microsoft Edge (Chromium) < 128.0.2739.42 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 128.0.2739.42. It is, therefore, affected by multiple vulnerabilities as referenced in the August 22, 2024 advisory.

- Microsoft Edge (HTML-based) Memory Corruption Vulnerability (CVE-2024-38207)

- Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability (CVE-2024-38209, CVE-2024-38210)

- Use after free in Passwords in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7964)

- Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7965)

- Out of bounds memory access in Skia in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who had compromised the renderer process to perform out of bounds memory access via a crafted HTML page.

(Chromium security severity: High) (CVE-2024-7966)

- Heap buffer overflow in Fonts in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7967)

- Use after free in Autofill in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who had convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7968)

- Type Confusion in V8 in Google Chrome prior to 128.0.6613.113 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7969)

- Type confusion in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7971)

- Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity:

Medium) (CVE-2024-7972)

- Heap buffer overflow in PDFium in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file. (Chromium security severity: Medium) (CVE-2024-7973)

- Insufficient data validation in V8 API in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity:

Medium) (CVE-2024-7974)

- Inappropriate implementation in Permissions in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-7975)

- Inappropriate implementation in FedCM in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-7976)

- Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: Medium) (CVE-2024-7977)

- Insufficient policy enforcement in Data Transfer in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-7978)

- Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a crafted symbolic link. (Chromium security severity: Medium) (CVE-2024-7979, CVE-2024-7980)

- Inappropriate implementation in Views in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-7981)

- Inappropriate implementation in WebApp Installs in Google Chrome on Windows prior to 128.0.6613.84 allowed an attacker who convinced a user to install a malicious application to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-8033)

- Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-8034)

- Inappropriate implementation in Extensions in Google Chrome on Windows prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-8035)

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?fcd44e19

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38207

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38209

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38210

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7964

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7965

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7966

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7967

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7968

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7969

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7971

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7972
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7973
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7974
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7975
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7976
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7977
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7978
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7979
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7980
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7981
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-8033
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-8034
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-8035

Solution

Upgrade to Microsoft Edge version 128.0.2739.42 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.2

EPSS Score

0.806

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-2024-7964
CVE	CVE-2024-7965
CVE	CVE-2024-7966
CVE	CVE-2024-7967
CVE	CVE-2024-7968
CVE	CVE-2024-7969
CVE	CVE-2024-7971
CVE	CVE-2024-7972
CVE	CVE-2024-7973
CVE	CVE-2024-7974
CVE	CVE-2024-7975
CVE	CVE-2024-7976
CVE	CVE-2024-7977
CVE	CVE-2024-7978
CVE	CVE-2024-7979
CVE	CVE-2024-7980
CVE	CVE-2024-7981
CVE	CVE-2024-8033
CVE	CVE-2024-8034
CVE	CVE-2024-8035
CVE	CVE-2024-38207
CVE	CVE-2024-38209
CVE	CVE-2024-38210
XREF	CISA-KNOWN-EXPLOITED:2024/09/18
XREF	CISA-KNOWN-EXPLOITED:2024/09/16
XREF	IAVA:2024-A-0524-S

Plugin Information

Published: 2024/08/23, Modified: 2024/11/28

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 128.0.2739.42
```

208101 - Microsoft Edge (Chromium) < 129.0.2792.79 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 129.0.2792.79. It is, therefore, affected by multiple vulnerabilities as referenced in the October 3, 2024 advisory.

- Integer overflow in Layout. (CVE-2024-7025)

- Insufficient data validation in Mojo. (CVE-2024-9369)

- Inappropriate implementation in V8. (CVE-2024-9370)

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?d78e7347

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7025

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9369

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9370

Solution

Upgrade to Microsoft Edge version 129.0.2792.79 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.1

EPSS Score

0.001

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-7025
CVE	CVE-2024-9369
CVE	CVE-2024-9370

Plugin Information

Published: 2024/10/03, Modified: 2025/01/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 129.0.2792.79
```

209257 - Microsoft Edge (Chromium) < 130.0.2849.46 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 130.0.2849.46. It is, therefore, affected by multiple vulnerabilities as referenced in the October 17, 2024 advisory.

- Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability (CVE-2024-43566, CVE-2024-43578, CVE-2024-43579, CVE-2024-43587, CVE-2024-43595, CVE-2024-43596, CVE-2024-49023)

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2024-43577, CVE-2024-43580)

- Use after free in AI in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-9954)

- Use after free in WebAuthentication in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-9955)

- Inappropriate implementation in WebAuthentication in Google Chrome on Android prior to 130.0.6723.58 allowed a local attacker to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-9956)

- Use after free in UI in Google Chrome on iOS prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-9957)

- Inappropriate implementation in PictureInPicture in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-9958)

- Use after free in DevTools in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted Chrome Extension.

(Chromium security severity: Medium) (CVE-2024-9959)

- Use after free in Dawn in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-9960)

- Use after free in ParcelTracking in Google Chrome on iOS prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-9961)

- Inappropriate implementation in Permissions in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-9962)

- Insufficient data validation in Downloads in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-9963)

- Inappropriate implementation in Payments in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Low) (CVE-2024-9964)

- Insufficient data validation in DevTools in Google Chrome on Windows prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-9965)

- Inappropriate implementation in Navigations in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-9966)

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?32eca5fa

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9954

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9955

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9956

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9957

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9958

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9959

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9960

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9961

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9962

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9963

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9964

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9965

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9966

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43566

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43577

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43578

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43579

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43580

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43587

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43595

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43596

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49023

Solution

Upgrade to Microsoft Edge version 130.0.2849.46 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

0.5095

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-2024-9954
CVE	CVE-2024-9955
CVE	CVE-2024-9956
CVE	CVE-2024-9957
CVE	CVE-2024-9958
CVE	CVE-2024-9959
CVE	CVE-2024-9960
CVE	CVE-2024-9961
CVE	CVE-2024-9962
CVE	CVE-2024-9963
CVE	CVE-2024-9964
CVE	CVE-2024-9965
CVE	CVE-2024-9966

CVE	CVE-2024-43566
CVE	CVE-2024-43577
CVE	CVE-2024-43578
CVE	CVE-2024-43579
CVE	CVE-2024-43580
CVE	CVE-2024-43587
CVE	CVE-2024-43595
CVE	CVE-2024-43596
CVE	CVE-2024-49023
XREF	IAVA:2024-A-0681-S

Plugin Information

Published: 2024/10/17, Modified: 2025/01/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 130.0.2849.46
```

216341 - Microsoft Edge (Chromium) < 133.0.3065.69 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 133.0.3065.69. It is, therefore, affected by multiple vulnerabilities as referenced in the February 14, 2025 advisory.

- Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability (CVE-2025-21401)

- Use after free in V8. (CVE-2025-0995)

- Inappropriate implementation in Browser UI. (CVE-2025-0996)

- Use after free in Navigation. (CVE-2025-0997)

- Out of bounds memory access in V8. (CVE-2025-0998)

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?4cca50d0

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0995

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0996

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0997

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0998

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21401

Solution

Upgrade to Microsoft Edge version 133.0.3065.69 or later.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.3

EPSS Score

0.0008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-0995
CVE	CVE-2025-0996
CVE	CVE-2025-0997
CVE	CVE-2025-0998
CVE	CVE-2025-21401
XREF	IAVA:2025-A-0124-S

Plugin Information

Published: 2025/02/14, Modified: 2025/03/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 133.0.3065.69
```

208302 - KB5044284: Windows 11 Version 24H2 / Windows Server 2025 Security Update (October 2024)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5044284. It is, therefore, affected by multiple vulnerabilities

- libcurl's ASN1 parser has this utf8asn1str() function used for parsing an ASN.1 UTF-8 string. Itcan detect an invalid field and return error. Unfortunately, when doing so it also invokes `free()` on a 4 byte localstack buffer. Most modern malloc implementations detect this error and immediately abort. Some however accept the input pointer and add that memory to its list of available chunks. This leads to the overwriting of nearby stack memory. The content of the overwrite is decided by the `free()` implementation; likely to be memory pointers and a set of flags. The most likely outcome of exploting this flaw is a crash, although it cannot be ruled out that more serious results can be had in special circumstances. (CVE-2024-6197)

- Remote Desktop Client Remote Code Execution Vulnerability (CVE-2024-43599)

- An attacker could exploit a use after free vulnerability within the OS SAPI component to execute arbitrary code in the context of the compromised user to disclose sensitive information, compromise system integrity or impact the availability of the victim's system. (CVE-2024-43574)

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://support.microsoft.com/help/5044284

Solution

Apply Security Update 5044284

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.6

EPSS Score

0.7122

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

8.7 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-6197
CVE	CVE-2024-20659
CVE	CVE-2024-30092
CVE	CVE-2024-37976
CVE	CVE-2024-37982
CVE	CVE-2024-37983
CVE	CVE-2024-38149
CVE	CVE-2024-43500
CVE	CVE-2024-43501
CVE	CVE-2024-43506
CVE	CVE-2024-43508
CVE	CVE-2024-43509
CVE	CVE-2024-43511
CVE	CVE-2024-43513
CVE	CVE-2024-43514
CVE	CVE-2024-43515
CVE	CVE-2024-43516
CVE	CVE-2024-43517
CVE	CVE-2024-43518
CVE	CVE-2024-43519
CVE	CVE-2024-43520
CVE	CVE-2024-43523
CVE	CVE-2024-43524
CVE	CVE-2024-43525
CVE	CVE-2024-43526
CVE	CVE-2024-43527

CVE	CVE-2024-43528
CVE	CVE-2024-43529
CVE	CVE-2024-43532
CVE	CVE-2024-43533
CVE	CVE-2024-43534
CVE	CVE-2024-43535
CVE	CVE-2024-43536
CVE	CVE-2024-43537
CVE	CVE-2024-43538
CVE	CVE-2024-43540
CVE	CVE-2024-43542
CVE	CVE-2024-43543
CVE	CVE-2024-43546
CVE	CVE-2024-43547
CVE	CVE-2024-43550
CVE	CVE-2024-43551
CVE	CVE-2024-43552
CVE	CVE-2024-43553
CVE	CVE-2024-43554
CVE	CVE-2024-43555
CVE	CVE-2024-43556
CVE	CVE-2024-43557
CVE	CVE-2024-43558
CVE	CVE-2024-43559
CVE	CVE-2024-43560
CVE	CVE-2024-43561
CVE	CVE-2024-43562
CVE	CVE-2024-43563
CVE	CVE-2024-43565
CVE	CVE-2024-43570
CVE	CVE-2024-43571
CVE	CVE-2024-43572
CVE	CVE-2024-43573
CVE	CVE-2024-43574
CVE	CVE-2024-43581
CVE	CVE-2024-43582
CVE	CVE-2024-43583
CVE	CVE-2024-43584
CVE	CVE-2024-43585
CVE	CVE-2024-43599
CVE	CVE-2024-43615
MSKB	5044284
XREF	MSFT:MS24-5044284

XREF	CISA-KNOWN-EXPLOITED:2024/10/29
XREF	IAVA:2024-A-0628
XREF	IAVA:2024-A-0631-S
XREF	IAVA:2024-A-0630-S

Plugin Information

Published: 2024/10/08, Modified: 2024/11/19

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5044284

  - C:\WINDOWS\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.26100.1742
    Should be      : 10.0.26100.2033
```

212224 - KB5048667: Windows 11 Version 24H2 / Windows Server 2025 Security Update (December 2024)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5048667 or hotpatch 5048794. It is, therefore, affected by multiple vulnerabilities

- Input Method Editor (IME) Remote Code Execution Vulnerability (CVE-2024-49079)

- Windows Common Log File System Driver Elevation of Privilege Vulnerability (CVE-2024-49090)

- Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability (CVE-2024-49112)

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://support.microsoft.com/help/5048667

https://support.microsoft.com/help/5048794

Solution

Apply Security Update 5048667 or hotpatch 5048794

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.6

EPSS Score

0.6435

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

8.7 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

CVE	CVE-2024-49072
CVE	CVE-2024-49073
CVE	CVE-2024-49075
CVE	CVE-2024-49076
CVE	CVE-2024-49077
CVE	CVE-2024-49078
CVE	CVE-2024-49079
CVE	CVE-2024-49080
CVE	CVE-2024-49081
CVE	CVE-2024-49082
CVE	CVE-2024-49083
CVE	CVE-2024-49084
CVE	CVE-2024-49085
CVE	CVE-2024-49086
CVE	CVE-2024-49087
CVE	CVE-2024-49088
CVE	CVE-2024-49089
CVE	CVE-2024-49090
CVE	CVE-2024-49091
CVE	CVE-2024-49092
CVE	CVE-2024-49093
CVE	CVE-2024-49094
CVE	CVE-2024-49095
CVE	CVE-2024-49096
CVE	CVE-2024-49097
CVE	CVE-2024-49098
CVE	CVE-2024-49099
CVE	CVE-2024-49101
CVE	CVE-2024-49102
CVE	CVE-2024-49103
CVE	CVE-2024-49104

CVE	CVE-2024-49106
CVE	CVE-2024-49107
CVE	CVE-2024-49108
CVE	CVE-2024-49109
CVE	CVE-2024-49110
CVE	CVE-2024-49111
CVE	CVE-2024-49112
CVE	CVE-2024-49113
CVE	CVE-2024-49114
CVE	CVE-2024-49115
CVE	CVE-2024-49116
CVE	CVE-2024-49117
CVE	CVE-2024-49118
CVE	CVE-2024-49119
CVE	CVE-2024-49120
CVE	CVE-2024-49121
CVE	CVE-2024-49122
CVE	CVE-2024-49123
CVE	CVE-2024-49124
CVE	CVE-2024-49125
CVE	CVE-2024-49126
CVE	CVE-2024-49127
CVE	CVE-2024-49128
CVE	CVE-2024-49129
CVE	CVE-2024-49132
CVE	CVE-2024-49138
MSKB	5048667
MSKB	5048794
XREF	MSFT:MS24-5048667
XREF	MSFT:MS24-5048794
XREF	CISA-KNOWN-EXPLOITED:2024/12/31
XREF	IAVA:2024-A-0812-S
XREF	IAVA:2024-A-0811-S

Plugin Information

Published: 2024/12/10, Modified: 2025/02/05

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5048667
```

```
- 5048794

- C:\WINDOWS\system32\ntoskrnl.exe has not been patched.
  Remote version : 10.0.26100.1742
  Should be      : 10.0.26100.2605
```

216132 - KB5051987: Windows 11 Version 24H2 / Windows Server 2025 Security Update (February 2025)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5051987 or hotpatch 5052105. It is, therefore, affected by multiple vulnerabilities

- Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability (CVE-2025-21208, CVE-2025-21410)

- Windows Telephony Service Remote Code Execution Vulnerability (CVE-2025-21190, CVE-2025-21200, CVE-2025-21371, CVE-2025-21406, CVE-2025-21407)

- Microsoft Digest Authentication Remote Code Execution Vulnerability (CVE-2025-21368, CVE-2025-21369)

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://support.microsoft.com/help/5051987

Solution

Apply Security Update 5051987

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

EPSS Score

0.359

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-2025-21179
CVE	CVE-2025-21181
CVE	CVE-2025-21182
CVE	CVE-2025-21183
CVE	CVE-2025-21184
CVE	CVE-2025-21190
CVE	CVE-2025-21200
CVE	CVE-2025-21201
CVE	CVE-2025-21208
CVE	CVE-2025-21212
CVE	CVE-2025-21216
CVE	CVE-2025-21254
CVE	CVE-2025-21337
CVE	CVE-2025-21347
CVE	CVE-2025-21349
CVE	CVE-2025-21350
CVE	CVE-2025-21351
CVE	CVE-2025-21352
CVE	CVE-2025-21358
CVE	CVE-2025-21359
CVE	CVE-2025-21367
CVE	CVE-2025-21368
CVE	CVE-2025-21369
CVE	CVE-2025-21371
CVE	CVE-2025-21373
CVE	CVE-2025-21375
CVE	CVE-2025-21376
CVE	CVE-2025-21377
CVE	CVE-2025-21379
CVE	CVE-2025-21391
CVE	CVE-2025-21406

CVE	CVE-2025-21407
CVE	CVE-2025-21410
CVE	CVE-2025-21414
CVE	CVE-2025-21418
CVE	CVE-2025-21419
CVE	CVE-2025-21420
MSKB	5051987
MSKB	5052105
XREF	MSFT:MS25-5051987
XREF	MSFT:MS25-5052105
XREF	CISA-KNOWN-EXPLOITED:2025/03/04
XREF	IAVA:2025-A-0109-S
XREF	IAVA:2025-A-0110-S

Plugin Information

Published: 2025/02/11, Modified: 2025/03/21

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5051987
  - 5052105

  - C:\WINDOWS\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.26100.1742
    Should be      : 10.0.26100.3194
```

232616 - KB5053598: Windows 11 Version 24H2 / Windows Server 2025 Security Update (March 2025)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5053598. It is, therefore, affected by multiple vulnerabilities

- Relative path traversal in Remote Desktop Client allows an unauthorized attacker to execute code over a network. (CVE-2025-26645)

- Sensitive data storage in improperly locked memory in Windows Remote Desktop Services allows an unauthorized attacker to execute code over a network. (CVE-2025-24035, CVE-2025-24045)

- ** UNSUPPORTED WHEN ASSIGNED ** A privilege escalation vulnerability in CxUIUSvc64.exe and CxUIUSvc32.exe of Synaptics audio drivers allows a local authorized attacker to load a DLL in a privileged process. Out of an abundance of caution, this CVE ID is being assigned to better serve our customers and ensure all who are still running this product understand that the product is End-of-Life and should be removed. For more information on this, refer to the CVE Record's reference information. (CVE-2024-9157)

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://support.microsoft.com/help/5053598

Solution

Apply Security Update 5053598

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

EPSS Score

0.1318

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-2024-9157
CVE	CVE-2025-21180
CVE	CVE-2025-21247
CVE	CVE-2025-24035
CVE	CVE-2025-24044
CVE	CVE-2025-24045
CVE	CVE-2025-24046
CVE	CVE-2025-24048
CVE	CVE-2025-24050
CVE	CVE-2025-24051
CVE	CVE-2025-24054
CVE	CVE-2025-24055
CVE	CVE-2025-24056
CVE	CVE-2025-24059
CVE	CVE-2025-24061
CVE	CVE-2025-24064
CVE	CVE-2025-24066
CVE	CVE-2025-24067
CVE	CVE-2025-24071
CVE	CVE-2025-24072
CVE	CVE-2025-24076
CVE	CVE-2025-24084
CVE	CVE-2025-24984
CVE	CVE-2025-24985
CVE	CVE-2025-24987
CVE	CVE-2025-24988
CVE	CVE-2025-24991

CVE	CVE-2025-24992
CVE	CVE-2025-24993
CVE	CVE-2025-24994
CVE	CVE-2025-24995
CVE	CVE-2025-24996
CVE	CVE-2025-24997
CVE	CVE-2025-25008
CVE	CVE-2025-26633
CVE	CVE-2025-26645
MSKB	5053598
XREF	CISA-KNOWN-EXPLOITED:2025/04/01
XREF	MSFT:MS25-5053598
XREF	IAVA:2025-A-0182
XREF	IAVA:2025-A-0181

Plugin Information

Published: 2025/03/11, Modified: 2025/03/14

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5053598

  - C:\WINDOWS\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.26100.1742
    Should be      : 10.0.26100.3476
```

192634 - Microsoft Edge (Chromium) < 122.0.2365.113 / 123.0.2420.65 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 122.0.2365.113 / 123.0.2420.65. It is, therefore, affected by multiple vulnerabilities as referenced in the March 27, 2024 advisory.

- Use after free in ANGLE in Google Chrome prior to 123.0.6312.86 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) (CVE-2024-2883)

- Use after free in Dawn in Google Chrome prior to 123.0.6312.86 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-2885)

- Use after free in WebCodecs in Google Chrome prior to 123.0.6312.86 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High) (CVE-2024-2886)

- Type Confusion in WebAssembly in Google Chrome prior to 123.0.6312.86 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) (CVE-2024-2887)

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?0feebe50

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2883

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2885

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2886

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2887

Solution

Upgrade to Microsoft Edge version 122.0.2365.113 / 123.0.2420.65 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0724

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-2024-2883
CVE	CVE-2024-2885
CVE	CVE-2024-2886
CVE	CVE-2024-2887
XREF	IAVA:2024-A-0177-S

Plugin Information

Published: 2024/03/27, Modified: 2024/12/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 123.0.2420.65
```

192932 - Microsoft Edge (Chromium) < 122.0.2365.120 / 123.0.2420.81 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 122.0.2365.120 / 123.0.2420.81. It is, therefore, affected by multiple vulnerabilities as referenced in the April 4, 2024 advisory.

- Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability (CVE-2024-29049)

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2024-29981)

- Inappropriate implementation in V8 in Google Chrome prior to 123.0.6312.105 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2024-3156)

- Use after free in Bookmarks in Google Chrome prior to 123.0.6312.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-3158)

- Out of bounds memory access in V8 in Google Chrome prior to 123.0.6312.105 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High) (CVE-2024-3159)

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?edee90bc

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29049

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29981

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3156

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3158

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3159

Solution

Upgrade to Microsoft Edge version 122.0.2365.120 / 123.0.2420.81 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0073

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-2024-3156
CVE	CVE-2024-3158
CVE	CVE-2024-3159
CVE	CVE-2024-29049
CVE	CVE-2024-29981
XREF	IAVA:2024-A-0204-S

Plugin Information

Published: 2024/04/04, Modified: 2024/05/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 123.0.2420.81
```

192478 - Microsoft Edge (Chromium) < 123.0.2420.53 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 123.0.2420.53. It is, therefore, affected by multiple vulnerabilities as referenced in the March 22, 2024 advisory.

- Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability (CVE-2024-26247)

- Object lifecycle issue in V8 in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-2625)

- Out of bounds read in Swiftshader in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-2626)

- Use after free in Canvas in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-2627)

- Inappropriate implementation in Downloads in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted URL. (Chromium security severity: Medium) (CVE-2024-2628)

- Incorrect security UI in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-2629)

- Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-2630)

- Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-2631)

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2024-29057)

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?e927e481

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26247

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2625

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2626

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2627

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2628

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2629

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2630

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-2631
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29057

Solution

Upgrade to Microsoft Edge version 123.0.2420.53 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.012

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-2024-2625
CVE	CVE-2024-2626
CVE	CVE-2024-2627
CVE	CVE-2024-2628
CVE	CVE-2024-2629
CVE	CVE-2024-2630
CVE	CVE-2024-2631

CVE	CVE-2024-26247
CVE	CVE-2024-29057
XREF	IAVA:2024-A-0177-S

Plugin Information

Published: 2024/03/22, Modified: 2024/05/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 123.0.2420.53
```

197034 - Microsoft Edge (Chromium) < 124.0.2478.105 (CVE-2024-4761)

Synopsis

The remote host has an web browser installed that is affected by a vulnerability.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 124.0.2478.105. It is, therefore, affected by a vulnerability as referenced in the May 14, 2024 advisory.

- Out of bounds write in V8 in Google Chrome prior to 124.0.6367.207 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High) (CVE-2024-4761)

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?62d1a061

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4761

Solution

Upgrade to Microsoft Edge version 124.0.2478.105 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.3894

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)

References

CVE	CVE-2024-4761
XREF	CISA-KNOWN-EXPLOITED:2024/06/06

Plugin Information

Published: 2024/05/14, Modified: 2024/05/21

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 124.0.2478.105
```

193518 - Microsoft Edge (Chromium) < 124.0.2478.51 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 124.0.2478.51. It is, therefore, affected by multiple vulnerabilities as referenced in the April 18, 2024 advisory.

- Microsoft Edge for Android (Chromium-based) Information Disclosure Vulnerability (CVE-2024-29986)

- Microsoft Edge (Chromium-based) Information Disclosure Vulnerability (CVE-2024-29987)

- Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability (CVE-2024-29991)

- Object corruption in V8 in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-3832)

- Object corruption in WebAssembly in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-3833)

- Use after free in Downloads in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-3834)

- Use after free in QUIC in Google Chrome prior to 124.0.6367.60 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-3837)

- Inappropriate implementation in Autofill in Google Chrome prior to 124.0.6367.60 allowed an attacker who convinced a user to install a malicious app to perform UI spoofing via a crafted app. (Chromium security severity: Medium) (CVE-2024-3838)

- Out of bounds read in Fonts in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-3839)

- Insufficient policy enforcement in Site Isolation in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-3840)

- Insufficient data validation in Browser Switcher in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to inject scripts or HTML into a privileged page via a malicious file. (Chromium security severity: Medium) (CVE-2024-3841)

- Insufficient data validation in Downloads in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-3843)

- Inappropriate implementation in Extensions in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Low) (CVE-2024-3844)

- Inappropriate implementation in Networks in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to bypass mixed content policy via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-3845)

- Inappropriate implementation in Prompts in Google Chrome prior to 124.0.6367.60 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page.

(Chromium security severity: Low) (CVE-2024-3846)

- Insufficient policy enforcement in WebUI in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-3847)

- Use after free in V8 in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-3914)

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?9bfb7f33

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3832

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3833

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3834

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3837

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3838

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3839

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3840

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3841

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3843

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3844

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3845

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3846

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3847

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-3914

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29986

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29987

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29991

Solution

Upgrade to Microsoft Edge version 124.0.2478.51 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

EPSS Score

0.0149

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-2024-3832
CVE	CVE-2024-3833
CVE	CVE-2024-3834
CVE	CVE-2024-3837
CVE	CVE-2024-3838
CVE	CVE-2024-3839
CVE	CVE-2024-3840
CVE	CVE-2024-3841
CVE	CVE-2024-3843
CVE	CVE-2024-3844
CVE	CVE-2024-3845
CVE	CVE-2024-3846
CVE	CVE-2024-3847
CVE	CVE-2024-3914
CVE	CVE-2024-29986

CVE	CVE-2024-29987
CVE	CVE-2024-29991
XREF	IAVA:2024-A-0253-S

Plugin Information

Published: 2024/04/18, Modified: 2024/12/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 124.0.2478.51
```

193962 - Microsoft Edge (Chromium) < 124.0.2478.67 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 124.0.2478.67. It is, therefore, affected by multiple vulnerabilities as referenced in the April 26, 2024 advisory.

- Type confusion in ANGLE in Google Chrome prior to 124.0.6367.78 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) (CVE-2024-4058)

- Out of bounds read in V8 API in Google Chrome prior to 124.0.6367.78 allowed a remote attacker to leak cross-site data via a crafted HTML page. (Chromium security severity: High) (CVE-2024-4059)

- Use after free in Dawn in Google Chrome prior to 124.0.6367.78 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-4060)

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?ac27ffe8

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4058

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4059

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4060

Solution

Upgrade to Microsoft Edge version 124.0.2478.67 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0056

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)

References

CVE	CVE-2024-4058
CVE	CVE-2024-4059
CVE	CVE-2024-4060

Plugin Information

Published: 2024/04/26, Modified: 2024/12/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 124.0.2478.67
```

194943 - Microsoft Edge (Chromium) < 124.0.2478.80 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 124.0.2478.80. It is, therefore, affected by multiple vulnerabilities as referenced in the May 2, 2024 advisory.

- Use after free in Picture In Picture in Google Chrome prior to 124.0.6367.118 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-4331)

- Use after free in Dawn in Google Chrome prior to 124.0.6367.118 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-4368)

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?2e10e71d

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4331

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-4368

Solution

Upgrade to Microsoft Edge version 124.0.2478.80 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0096

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)

References

CVE	CVE-2024-4331
CVE	CVE-2024-4368

Plugin Information

Published: 2024/05/02, Modified: 2024/12/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 124.0.2478.80
```

200060 - Microsoft Edge (Chromium) < 125.0.2535.85 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 125.0.2535.85. It is, therefore, affected by multiple vulnerabilities as referenced in the June 3, 2024 advisory.

- Heap buffer overflow in WebRTC in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5493)

- Use after free in Dawn in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5494, CVE-2024-5495)

- Use after free in Media Session in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5496)

- Out of bounds memory access in Keyboard Inputs in Google Chrome prior to 125.0.6422.141 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5497)

- Use after free in Presentation API in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5498)

- Out of bounds write in Streams API in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5499)

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?4de2cc67

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5493

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5494

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5495

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5496

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5497

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5498

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5499

Solution

Upgrade to Microsoft Edge version 125.0.2535.85 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0074

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-2024-5493
CVE	CVE-2024-5494
CVE	CVE-2024-5495
CVE	CVE-2024-5496
CVE	CVE-2024-5497
CVE	CVE-2024-5498
CVE	CVE-2024-5499
XREF	IAVA:2024-A-0342-S
XREF	IAVA:2024-A-0371-S

Plugin Information

Published: 2024/06/03, Modified: 2025/01/01

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 125.0.2535.85
```

200498 - Microsoft Edge (Chromium) < 126.0.2592.56 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 126.0.2592.56. It is, therefore, affected by multiple vulnerabilities as referenced in the June 13, 2024 advisory.

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2024-30058, CVE-2024-38083)

- Type Confusion in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5830)

- Use after free in Dawn in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5831, CVE-2024-5832)

- Type Confusion in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5833, CVE-2024-5837)

- Inappropriate implementation in Dawn in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5834)

- Heap buffer overflow in Tab Groups in Google Chrome prior to 126.0.6478.54 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5835)

- Inappropriate Implementation in DevTools in Google Chrome prior to 126.0.6478.54 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: High) (CVE-2024-5836)

- Type Confusion in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2024-5838)

- Inappropriate Implementation in Memory Allocator in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity:

Medium) (CVE-2024-5839)

- Policy bypass in CORS in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-5840)

- Use after free in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-5841)

- Use after free in Browser UI in Google Chrome prior to 126.0.6478.54 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-5842)

- Inappropriate implementation in Downloads in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to obfuscate security UI via a malicious file. (Chromium security severity: Medium) (CVE-2024-5843)

- Heap buffer overflow in Tab Strip in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-5844)

- Use after free in Audio in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium) (CVE-2024-5845)

- Use after free in PDFium in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium) (CVE-2024-5846, CVE-2024-5847)

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?0a56865e

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30058

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38083

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5830

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5831

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5832

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5833

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5834

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5835

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5836

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5837

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5838

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5839

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5840

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5841

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5842

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5843

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5844

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5845

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5846

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-5847

Solution

Upgrade to Microsoft Edge version 126.0.2592.56 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

EPSS Score

0.1901

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-2024-5830
CVE	CVE-2024-5831
CVE	CVE-2024-5832
CVE	CVE-2024-5833
CVE	CVE-2024-5834
CVE	CVE-2024-5835
CVE	CVE-2024-5836
CVE	CVE-2024-5837
CVE	CVE-2024-5838
CVE	CVE-2024-5839
CVE	CVE-2024-5840
CVE	CVE-2024-5841
CVE	CVE-2024-5842

CVE	CVE-2024-5843
CVE	CVE-2024-5844
CVE	CVE-2024-5845
CVE	CVE-2024-5846
CVE	CVE-2024-5847
CVE	CVE-2024-30058
CVE	CVE-2024-38083
XREF	IAVA:2024-A-0342-S
XREF	IAVA:2024-A-0371-S

Plugin Information

Published: 2024/06/13, Modified: 2024/08/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 126.0.2592.56
```

200793 - Microsoft Edge (Chromium) < 126.0.2592.68 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 126.0.2592.68. It is, therefore, affected by multiple vulnerabilities as referenced in the June 20, 2024 advisory.

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2024-38082, CVE-2024-38093)

- Type Confusion in V8 in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6100)

- Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6101)

- Out of bounds memory access in Dawn in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6102)

- Use after free in Dawn in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6103)

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?a8434d6b

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38082

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38093

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6100

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6101

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6102

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6103

Solution

Upgrade to Microsoft Edge version 126.0.2592.68 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0179

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-2024-6100
CVE	CVE-2024-6101
CVE	CVE-2024-6102
CVE	CVE-2024-6103
CVE	CVE-2024-38082
CVE	CVE-2024-38093
XREF	IAVA:2024-A-0365-S
XREF	IAVA:2024-A-0371-S

Plugin Information

Published: 2024/06/20, Modified: 2024/07/12

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Microsoft\Edge\Application
  Installed version : 122.0.2365.106
```

```
  Fixed version     : 126.0.2592.68
```

201115 - Microsoft Edge (Chromium) < 126.0.2592.81 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 126.0.2592.81. It is, therefore, affected by multiple vulnerabilities as referenced in the June 27, 2024 advisory.

- Acrobat for Edge versions 126.0.2592.68 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure.

An attacker could leverage this vulnerability to execute code in the context of the current user.

Exploitation of this issue requires user interaction in that a victim must open a malicious file.

(CVE-2024-34122)

- Use after free in Dawn in Google Chrome prior to 126.0.6478.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6290, CVE-2024-6292, CVE-2024-6293)

- Use after free in Swiftshader in Google Chrome prior to 126.0.6478.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-6291)

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?5bf00176

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-34122

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6290

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6291

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6292

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6293

Solution

Upgrade to Microsoft Edge version 126.0.2592.81 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0059

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-2024-6290
CVE	CVE-2024-6291
CVE	CVE-2024-6292
CVE	CVE-2024-6293
CVE	CVE-2024-34122
XREF	IAVA:2024-A-0401-S

Plugin Information

Published: 2024/06/27, Modified: 2024/12/31

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 126.0.2592.81
```

205697 - Microsoft Edge (Chromium) < 127.0.2651.105 (CVE-2024-43472)

Synopsis

The remote host has an web browser installed that is affected by a vulnerability.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 127.0.2651.105. It is, therefore, affected by a vulnerability as referenced in the August 15, 2024 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability (CVE-2024-43472)

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?e6c2ddd3

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43472

Solution

Upgrade to Microsoft Edge version 127.0.2651.105 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.1

EPSS Score

0.0022

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-43472
XREF	IAVA:2024-A-0511

Plugin Information

Published: 2024/08/16, Modified: 2024/08/29

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 127.0.2651.105
```

204747 - Microsoft Edge (Chromium) < 127.0.2651.74 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 127.0.2651.74. It is, therefore, affected by multiple vulnerabilities as referenced in the July 25, 2024 advisory.

- Microsoft Edge (Chromium-based) Information Disclosure Vulnerability (CVE-2024-38103)

- Use after free in Downloads. (CVE-2024-6988)

- Use after free in Loader. (CVE-2024-6989)

- Use after free in Dawn. (CVE-2024-6991)

- The vulnerability exists due to a boundary error when processing untrusted input in ANGLE. A remote attacker can create a specially crafted web page, trick the victim into visiting it, trigger out-of-bounds write and execute arbitrary code on the target system. (CVE-2024-6992)

- The vulnerability exists due to inappropriate implementation in Canvas. A remote attacker can create a specially crafted web page, trick the victim into visiting it and gain unauthorized access to the system. (CVE-2024-6993)

- Heap buffer overflow in Layout. (CVE-2024-6994)

- Inappropriate implementation in Fullscreen. (CVE-2024-6995)

- Race in Frames. (CVE-2024-6996)

- Use after free in Tabs. (CVE-2024-6997)

- Use after free in User Education. (CVE-2024-6998)

- Inappropriate implementation in FedCM. (CVE-2024-6999, CVE-2024-7003)

- Use after free in CSS. (CVE-2024-7000)

- Inappropriate implementation in HTML. (CVE-2024-7001)

- Insufficient validation of untrusted input in Safe Browsing. (CVE-2024-7004, CVE-2024-7005)

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?7cb6545b

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38103

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-39379

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6988

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6989
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6991
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6992
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6993
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6994
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6995
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6996
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6997
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6998
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6999
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7000
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7001
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7003
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7004
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7005

Solution

Upgrade to Microsoft Edge version 127.0.2651.74 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0033

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-2024-6988
CVE	CVE-2024-6989
CVE	CVE-2024-6991
CVE	CVE-2024-6992
CVE	CVE-2024-6993
CVE	CVE-2024-6994
CVE	CVE-2024-6995
CVE	CVE-2024-6996
CVE	CVE-2024-6997
CVE	CVE-2024-6998
CVE	CVE-2024-6999
CVE	CVE-2024-7000
CVE	CVE-2024-7001
CVE	CVE-2024-7003
CVE	CVE-2024-7004
CVE	CVE-2024-7005
CVE	CVE-2024-38103
CVE	CVE-2024-39379
XREF	IAVA:2024-A-0452-S

Plugin Information

Published: 2024/07/25, Modified: 2024/08/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 127.0.2651.74
```

204961 - Microsoft Edge (Chromium) < 127.0.2651.86 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 127.0.2651.86. It is, therefore, affected by multiple vulnerabilities as referenced in the August 1, 2024 advisory.

- Uninitialized Use in Dawn in Google Chrome on Android prior to 127.0.6533.88 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Critical) (CVE-2024-6990)

- Out of bounds read in WebTransport in Google Chrome prior to 127.0.6533.88 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7255)

- Insufficient data validation in Dawn in Google Chrome on Android prior to 127.0.6533.88 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) (CVE-2024-7256)

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?32856b94

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6990

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7255

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-7256

Solution

Upgrade to Microsoft Edge version 127.0.2651.86 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0024

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)

References

CVE	CVE-2024-6990
CVE	CVE-2024-7255
CVE	CVE-2024-7256

Plugin Information

Published: 2024/08/01, Modified: 2025/01/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 127.0.2651.86
```

207516 - Microsoft Edge (Chromium) < 128.0.2739.90 / 129.0.2792.52 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 128.0.2739.90 / 129.0.2792.52. It is, therefore, affected by multiple vulnerabilities as referenced in the September 19, 2024 advisory.

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2024-38221)

- Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability (CVE-2024-43489, CVE-2024-43496)

- Type Confusion in V8 in Google Chrome prior to 129.0.6668.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-8904)

- Inappropriate implementation in V8 in Google Chrome prior to 129.0.6668.58 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-8905)

- Incorrect security UI in Downloads in Google Chrome prior to 129.0.6668.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page.

(Chromium security severity: Medium) (CVE-2024-8906)

- Insufficient data validation in Omnibox in Google Chrome on Android prior to 129.0.6668.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to inject arbitrary scripts or HTML (XSS) via a crafted set of UI gestures. (Chromium security severity: Medium) (CVE-2024-8907)

- Inappropriate implementation in Autofill in Google Chrome prior to 129.0.6668.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-8908)

- Inappropriate implementation in UI in Google Chrome on iOS prior to 129.0.6668.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-8909)

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?f38754a9

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38221

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43489

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43496

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-8904

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-8905

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-8906
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-8907
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-8908
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-8909

Solution

Upgrade to Microsoft Edge version 128.0.2739.90 / 129.0.2792.52 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0027

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-2024-8904
CVE	CVE-2024-8905
CVE	CVE-2024-8906
CVE	CVE-2024-8907

CVE	CVE-2024-8908
CVE	CVE-2024-8909
CVE	CVE-2024-38221
CVE	CVE-2024-43489
CVE	CVE-2024-43496
XREF	IAVA:2024-A-0597-S

Plugin Information

Published: 2024/09/20, Modified: 2025/01/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 129.0.2792.52
```

207866 - Microsoft Edge (Chromium) < 128.0.2739.97 / 129.0.2792.65 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 128.0.2739.97 / 129.0.2792.65. It is, therefore, affected by multiple vulnerabilities as referenced in the September 26, 2024 advisory.

- Use after free in Dawn in Google Chrome on Windows prior to 129.0.6668.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-9120)

- Inappropriate implementation in V8 in Google Chrome prior to 129.0.6668.70 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2024-9121)

- Type Confusion in V8 in Google Chrome prior to 129.0.6668.70 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2024-9122)

- Integer overflow in Skia in Google Chrome prior to 129.0.6668.70 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High) (CVE-2024-9123)

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?b7f5a96d

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9120

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9121

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9122

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9123

Solution

Upgrade to Microsoft Edge version 128.0.2739.97 / 129.0.2792.65 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.004

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)

References

CVE	CVE-2024-9120
CVE	CVE-2024-9121
CVE	CVE-2024-9122
CVE	CVE-2024-9123

Plugin Information

Published: 2024/09/27, Modified: 2025/01/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 129.0.2792.65
```

208710 - Microsoft Edge (Chromium) < 129.0.2792.89 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 129.0.2792.89. It is, therefore, affected by multiple vulnerabilities as referenced in the October 10, 2024 advisory.

- Type Confusion in V8 in Google Chrome prior to 129.0.6668.100 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High) (CVE-2024-9602)

- Type Confusion in V8 in Google Chrome prior to 129.0.6668.100 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-9603)

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?e8753453

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9602

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-9603

Solution

Upgrade to Microsoft Edge version 129.0.2792.89 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0017

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)

References

CVE	CVE-2024-9602
CVE	CVE-2024-9603

Plugin Information

Published: 2024/10/10, Modified: 2025/01/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 129.0.2792.89
```

212712 - Microsoft Edge (Chromium) < 130.0.2849.116 / 131.0.2903.99 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 130.0.2849.116 / 131.0.2903.99. It is, therefore, affected by multiple vulnerabilities as referenced in the December 12, 2024 advisory.

- Use after free in Translate in Google Chrome prior to 131.0.6778.139 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-12382)

- Type Confusion in V8 in Google Chrome prior to 131.0.6778.139 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-12381)

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?adf4f087

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-12381

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-12382

Solution

Upgrade to Microsoft Edge version 130.0.2849.116 / 131.0.2903.99 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0009

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-12381
CVE	CVE-2024-12382

Plugin Information

Published: 2024/12/12, Modified: 2024/12/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 131.0.2903.99
```

213260 - Microsoft Edge (Chromium) < 130.0.2849.123 / 131.0.2903.112 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 130.0.2849.123 / 131.0.2903.112. It is, therefore, affected by multiple vulnerabilities as referenced in the December 19, 2024 advisory.

- Out of bounds write in V8 in Google Chrome prior to 131.0.6778.204 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) (CVE-2024-12695)

- Type Confusion in V8 in Google Chrome prior to 131.0.6778.204 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-12692)

- Out of bounds memory access in V8 in Google Chrome prior to 131.0.6778.204 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) (CVE-2024-12693)

- Use after free in Compositing in Google Chrome prior to 131.0.6778.204 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-12694)

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?825099d8

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-12692

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-12693

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-12694

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-12695

Solution

Upgrade to Microsoft Edge version 130.0.2849.123 / 131.0.2903.112 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0015

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-12692
CVE	CVE-2024-12693
CVE	CVE-2024-12694
CVE	CVE-2024-12695

Plugin Information

Published: 2024/12/19, Modified: 2025/02/12

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 131.0.2903.112
```

210016 - Microsoft Edge (Chromium) < 130.0.2849.68 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 130.0.2849.68. It is, therefore, affected by multiple vulnerabilities as referenced in the October 31, 2024 advisory.

- Out of bounds write in Dawn in Google Chrome prior to 130.0.6723.92 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Critical) (CVE-2024-10487)

- Use after free in WebRTC in Google Chrome prior to 130.0.6723.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-10488)

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?2aa6a17b

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-10487

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-10488

Solution

Upgrade to Microsoft Edge version 130.0.2849.68 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0014

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-10487
CVE	CVE-2024-10488

Plugin Information

Published: 2024/10/31, Modified: 2025/01/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 130.0.2849.68
```

210592 - Microsoft Edge (Chromium) < 130.0.2849.80 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 130.0.2849.80. It is, therefore, affected by multiple vulnerabilities as referenced in the November 7, 2024 advisory.

- Use after free in Family Experiences in Google Chrome on Android prior to 130.0.6723.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity:

High) (CVE-2024-10826)

- Use after free in Serial in Google Chrome prior to 130.0.6723.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-10827)

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?582f084c

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-10826

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-10827

Solution

Upgrade to Microsoft Edge version 130.0.2849.80 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0046

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-2024-10826
CVE	CVE-2024-10827
XREF	IAVA:2024-A-0719-S

Plugin Information

Published: 2024/11/08, Modified: 2025/01/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 130.0.2849.80
```

211402 - Microsoft Edge (Chromium) < 131.0.2903.48 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 131.0.2903.48. It is, therefore, affected by multiple vulnerabilities as referenced in the November 14, 2024 advisory.

- Inappropriate implementation in Extensions in Google Chrome prior to 131.0.6778.69 allowed a remote attacker to bypass site isolation via a crafted Chrome Extension. (Chromium security severity: High) (CVE-2024-11110)

- Inappropriate implementation in Autofill in Google Chrome prior to 131.0.6778.69 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page.

(Chromium security severity: Medium) (CVE-2024-11111)

- Use after free in Media in Google Chrome on Windows prior to 131.0.6778.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-11112)

- Use after free in Accessibility in Google Chrome prior to 131.0.6778.69 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-11113)

- Inappropriate implementation in Views in Google Chrome on Windows prior to 131.0.6778.69 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-11114)

- Insufficient policy enforcement in Navigation in Google Chrome on iOS prior to 131.0.6778.69 allowed a remote attacker to perform privilege escalation via a series of UI gestures. (Chromium security severity:

Medium) (CVE-2024-11115)

- Inappropriate implementation in Blink in Google Chrome prior to 131.0.6778.69 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page.

(Chromium security severity: Medium) (CVE-2024-11116)

- Inappropriate implementation in FileSystem in Google Chrome prior to 131.0.6778.69 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-11117)

- Microsoft Edge (Chromium-based) Information Disclosure Vulnerability (CVE-2024-49025)

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?a9b9d7d8

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-11110
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-11111
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-11112
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-11113
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-11114
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-11115
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-11116
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-11117
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49025

Solution

Upgrade to Microsoft Edge version 131.0.2903.48 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.3

EPSS Score

0.0022

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-2024-11110
CVE	CVE-2024-11111
CVE	CVE-2024-11112
CVE	CVE-2024-11113
CVE	CVE-2024-11114
CVE	CVE-2024-11115
CVE	CVE-2024-11116
CVE	CVE-2024-11117
CVE	CVE-2024-49025
XREF	IAVA:2024-A-0753-S

Plugin Information

Published: 2024/11/15, Modified: 2025/01/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 131.0.2903.48
```

211720 - Microsoft Edge (Chromium) < 131.0.2903.63 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 131.0.2903.63. It is, therefore, affected by multiple vulnerabilities as referenced in the November 21, 2024 advisory.

- Type Confusion in V8 in Google Chrome prior to 131.0.6778.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-11395)

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?c158b3b5

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-11395

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49054

Solution

Upgrade to Microsoft Edge version 131.0.2903.63 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

5.9

EPSS Score

0.0013

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-11395
CVE	CVE-2024-49054
XREF	IAVA:2024-A-0753-S

Plugin Information

Published: 2024/11/22, Modified: 2024/12/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 131.0.2903.63
```

214350 - Microsoft Edge (Chromium) < 132.0.2957.115 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 132.0.2957.115. It is, therefore, affected by multiple vulnerabilities as referenced in the January 14, 2025 advisory.

- Out of bounds read in Metrics in Google Chrome prior to 132.0.6834.83 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2025-0437)

- Type Confusion in V8 in Google Chrome prior to 131.0.6778.264 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High) (CVE-2025-0291)

- Out of bounds memory access in V8 in Google Chrome prior to 132.0.6834.83 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2025-0434)

- Inappropriate implementation in Navigation in Google Chrome on Android prior to 132.0.6834.83 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: High) (CVE-2025-0435)

- Integer overflow in Skia in Google Chrome prior to 132.0.6834.83 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2025-0436)

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?224d9eab

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0291

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0434

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0435

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0436

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0437

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0438

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0439

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0440

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0441

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0442

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0443

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0446

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0447
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0448
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21185
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21399

Solution

Upgrade to Microsoft Edge version 132.0.2957.115 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0018

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-0291
CVE	CVE-2025-0434
CVE	CVE-2025-0435
CVE	CVE-2025-0436

CVE	CVE-2025-0437
CVE	CVE-2025-0438
CVE	CVE-2025-0439
CVE	CVE-2025-0440
CVE	CVE-2025-0441
CVE	CVE-2025-0442
CVE	CVE-2025-0443
CVE	CVE-2025-0446
CVE	CVE-2025-0447
CVE	CVE-2025-0448
CVE	CVE-2025-21185
CVE	CVE-2025-21399
XREF	IAVA:2025-A-0041-S

Plugin Information

Published: 2025/01/18, Modified: 2025/01/30

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 132.0.2957.115
```

214822 - Microsoft Edge (Chromium) < 132.0.2957.140 (CVE-2025-0762)

Synopsis

The remote host has an web browser installed that is affected by a vulnerability.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 132.0.2957.140. It is, therefore, affected by a vulnerability as referenced in the January 30, 2025 advisory.

- Use after free in DevTools in Google Chrome prior to 132.0.6834.159 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: Medium) (CVE-2025-0762)

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?031a09a7

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0762

Solution

Upgrade to Microsoft Edge version 132.0.2957.140 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

5.9

EPSS Score

0.0008

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)

References

CVE	CVE-2025-0762

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 132.0.2957.140
```

215070 - Microsoft Edge (Chromium) < 133.0.3065.51 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 133.0.3065.51. It is, therefore, affected by multiple vulnerabilities as referenced in the February 6, 2025 advisory.

- Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability (CVE-2025-21279, CVE-2025-21283, CVE-2025-21342, CVE-2025-21408)

- Use after free in Skia in Google Chrome prior to 133.0.6943.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2025-0444)

- Use after free in V8 in Google Chrome prior to 133.0.6943.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2025-0445)

- Inappropriate implementation in Extensions API in Google Chrome prior to 133.0.6943.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Medium) (CVE-2025-0451)

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2025-21267, CVE-2025-21404)

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?9645df4d

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0444

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0445

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0451

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21267

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21279

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21283

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21342

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21404

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21408

Solution

Upgrade to Microsoft Edge version 133.0.3065.51 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0017

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-0444
CVE	CVE-2025-0445
CVE	CVE-2025-0451
CVE	CVE-2025-21267
CVE	CVE-2025-21279
CVE	CVE-2025-21283
CVE	CVE-2025-21342
CVE	CVE-2025-21404
CVE	CVE-2025-21408
XREF	IAVA:2025-A-0103-S

Plugin Information

Published: 2025/02/06, Modified: 2025/02/21

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 133.0.3065.51
```

216623 - Microsoft Edge (Chromium) < 133.0.3065.82 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 133.0.3065.82. It is, therefore, affected by multiple vulnerabilities as referenced in the February 21, 2025 advisory.

- Heap buffer overflow in GPU in Google Chrome on Android prior to 133.0.6943.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2025-1426)

- Heap buffer overflow in V8 in Google Chrome prior to 133.0.6943.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2025-0999)

- Use after free in Network in Google Chrome prior to 133.0.6943.126 allowed a remote attacker to potentially exploit heap corruption via a crafted web app. (Chromium security severity: Medium) (CVE-2025-1006)

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?79426f24

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0999

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1006

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1426

Solution

Upgrade to Microsoft Edge version 133.0.3065.82 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

6.7

EPSS Score

0.0007

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)

References

CVE	CVE-2025-0999
CVE	CVE-2025-1006
CVE	CVE-2025-1426

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 133.0.3065.82
```

232658 - Microsoft Edge (Chromium) < 134.0.3124.66 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 134.0.3124.66. It is, therefore, affected by multiple vulnerabilities as referenced in the March 12, 2025 advisory.

- Out of bounds read in V8 in Google Chrome prior to 134.0.6998.88 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium) (CVE-2025-2137)

- Use after free in Inspector in Google Chrome prior to 134.0.6998.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2025-2136)

- Type Confusion in V8 in Google Chrome prior to 134.0.6998.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2025-1920, CVE-2025-2135)

- An out-of-bounds write issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in visionOS 2.3.2, iOS 18.3.2 and iPadOS 18.3.2, macOS Sequoia 15.3.2, Safari 18.3.1.

Maliciously crafted web content May be able to break out of Web Content sandbox. This is a supplementary fix for an attack that was blocked in iOS 17.2. (Apple is aware of a report that this issue May have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 17.2.). (CVE-2025-24201)

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?c9fba8c3

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1920

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-2135

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-2136

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-2137

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24201

Solution

Upgrade to Microsoft Edge version 134.0.3124.66 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

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

VPR Score

9.2

EPSS Score

0.0013

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

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

References

CVE	CVE-2025-1920
CVE	CVE-2025-2135
CVE	CVE-2025-2136
CVE	CVE-2025-2137
CVE	CVE-2025-24201
XREF	CISA-KNOWN-EXPLOITED:2025/04/03

Plugin Information

Published: 2025/03/12, Modified: 2025/03/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 134.0.3124.66
```

233201 - Microsoft Edge (Chromium) < 134.0.3124.83 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 134.0.3124.83. It is, therefore, affected by multiple vulnerabilities as referenced in the March 21, 2025 advisory.

- CVE-2025-2476 is a use after free in Lens. It was reported by SungKwon Lee of Enki Whitehat on 2025-03-05.

(CVE-2025-2476)

- Use after free in Lens in Google Chrome prior to 134.0.6998.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) (CVE-2025-2476)

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?ae8a73b6

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-2476

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29795

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29806

Solution

Upgrade to Microsoft Edge version 134.0.3124.83 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

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)

References

CVE	CVE-2025-2476
CVE	CVE-2025-29795

Plugin Information

Published: 2025/03/21, Modified: 2025/03/21

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 134.0.3124.83
```

144813 - Microsoft Teams < 1.3.0.13000 Remote Code Execution

Synopsis

The version of Microsoft Teams installed on the remote Windows host is affected by a remote code execution vulnerability.

Description

The version of Microsoft Teams installed on the remote Windows host is a version prior to 1.3.0.13000. It is, therefore, affected by remote code execution vulnerability.

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17091

Solution

Upgrade to Microsoft Teams 1.3.0.13000 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0123

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-17091
XREF	IAVA:2021-A-0002
XREF	CEA-ID:CEA-2020-0135

Plugin Information

Published: 2021/01/11, Modified: 2024/01/30

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe
Installed version : 1.0.0.0
Fixed version     : 1.3.0.13000
```

179635 - Microsoft Teams < 1.6.0.18681 RCE

Synopsis

The version of Microsoft Teams installed on the remote Windows host is affected by a Remote Code Execution vulnerability.

Description

The version of Microsoft Teams installed on the remote Windows host is version prior to 1.6.0.18681. It is, therefore, affected by a remote code execution vulnerability. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

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://learn.microsoft.com/en-us/officeupdates/teams-app-versioning

https://learn.microsoft.com/en-us/microsoftteams/teams-client-update

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29328

Solution

Upgrade to Microsoft Teams 1.6.0.18681 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.012

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-2023-29328
CVE	CVE-2023-29330
XREF	IAVA:2023-A-0417

Plugin Information

Published: 2023/08/10, Modified: 2023/08/14

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe
Installed version : 1.0.0.0
Fixed version     : 1.6.0.18681
```

193266 - Security Updates Outlook for Windows (April 2024)

Synopsis

The Microsoft Outlook application installed on the remote host is missing a security update.

Description

The Microsoft Outlook application installed on the remote host is missing a security update. It is, therefore, affected by a spoofing vulnerability. External attackers could send specially crafted emails that will cause a connection from the victim to an untrusted location of attackers' control. This will leak the Net-NTLMv2 hash of the victim to the untrusted network which an attacker can then relay to another service and authenticate as the victim.

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?02d9198f

Solution

Microsoft has released KB5002574 to address this issue.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.2

EPSS Score

0.1096

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-20670
MSKB	5002574
XREF	MSFT:MS24-5002574
XREF	IAVA:2024-A-0225-S

Plugin Information

Published: 2024/04/12, Modified: 2024/07/30

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.OutlookForWindows_1.0.0.0_neutral__8wekyb3d8bbwe
  Installed version : 1.0.0.0
  Fixed version     : 1.2023.0322.0100
```

214274 - Security Updates for Microsoft .NET Framework (January 2025)

Synopsis

The Microsoft .NET Framework installation on the remote host is missing a security update.

Description

The Microsoft .NET Framework installation on the remote host is missing a security update. It is, therefore, affected by multiple denial of service vulnerabilities, as follows:

- A remote code execution vulnerability. An attacker can exploit this issue to cause the affected component to execute unauthorized code. (CVE-2025-21176)

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

See Also

http://www.nessus.org/u?3ee48e6a

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21176

https://support.microsoft.com/en-us/help/5049614

https://support.microsoft.com/en-us/help/5049620

https://support.microsoft.com/en-us/help/5049622

https://support.microsoft.com/en-us/help/5049624

https://support.microsoft.com/en-us/help/5049993

https://support.microsoft.com/en-us/help/5050013

https://support.microsoft.com/en-us/help/5050180

https://support.microsoft.com/en-us/help/5050181

https://support.microsoft.com/en-us/help/5050182

https://support.microsoft.com/en-us/help/5050183

https://support.microsoft.com/en-us/help/5050184

https://support.microsoft.com/en-us/help/5050185

https://support.microsoft.com/en-us/help/5050186

https://support.microsoft.com/en-us/help/5050187

https://support.microsoft.com/en-us/help/5050188

https://support.microsoft.com/en-us/help/5050416

Solution

Microsoft has released security updates for Microsoft .NET Framework.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0327

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-21176
MSKB	5049614
MSKB	5049620
MSKB	5049622
MSKB	5049624
MSKB	5049993
MSKB	5050013
MSKB	5050180
MSKB	5050181
MSKB	5050182
MSKB	5050183
MSKB	5050184
MSKB	5050185
MSKB	5050186
MSKB	5050187
MSKB	5050188
MSKB	5050416

XREF MSFT:MS25-5049614
XREF MSFT:MS25-5049620
XREF MSFT:MS25-5049622
XREF MSFT:MS25-5049624
XREF MSFT:MS25-5049993
XREF MSFT:MS25-5050013
XREF MSFT:MS25-5050180
XREF MSFT:MS25-5050181
XREF MSFT:MS25-5050182
XREF MSFT:MS25-5050183
XREF MSFT:MS25-5050184
XREF MSFT:MS25-5050185
XREF MSFT:MS25-5050186
XREF MSFT:MS25-5050187
XREF MSFT:MS25-5050188
XREF MSFT:MS25-5050416
XREF IAVA:2025-A-0028-S
XREF CWE:126

Plugin Information

Published: 2025/01/16, Modified: 2025/03/13

Plugin Output

tcp/445/cifs

```
Microsoft .NET Framework 4.8.1
The remote host is missing one of the following rollup KBs :

Cumulative
  - 5049622

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll has not been patched.
    Remote version : 4.8.9266.0
    Should be      : 4.8.9290.0
```

tcp/445/cifs

```
Microsoft .NET Framework 4.8.1
The remote host is missing one of the following rollup KBs :

Cumulative
  - 5049622

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll has not been patched.
    Remote version : 4.8.9266.0
    Should be      : 4.8.9290.0
```

```
01_2025  - C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll has not been patched.
    Remote version : 4.8.9266.0
    Should be      : 4.8.9290.0
```

103569 - Windows Defender Antimalware/Antivirus Signature Definition Check

Synopsis

Windows Defender AntiMalware / AntiVirus Signatures are continuously not and should not be more than 1 day old

Description

Windows Defender has an AntiMalware/AntiVirus signature that gets updated continuously. The signature definition has not been updated in more than 1 day.

See Also

https://www.microsoft.com/en-us/wdsi/definitions

Solution

Trigger an update manually and/or enable auto-updates.

Risk Factor

High

Plugin Information

Published: 2017/10/02, Modified: 2024/08/06

Plugin Output

tcp/445/cifs

```
Malware Signature Timestamp : Mar. 25, 2025 at 11:19:30 GMT
Malware Signature Version   : 1.425.238.0
```

212105 - Microsoft Edge (Chromium) < 131.0.2903.86 (CVE-2024-49041)

Synopsis

The remote host has an web browser installed that is affected by a vulnerability.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 131.0.2903.86. It is, therefore, affected by a vulnerability as referenced in the December 5, 2024 advisory.

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2024-49041)

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?34e2bd22

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49041

Solution

Upgrade to Microsoft Edge version 131.0.2903.86 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

EPSS Score

0.0008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-49041
XREF	IAVA:2024-A-0805-S

Plugin Information

Published: 2024/12/06, Modified: 2025/01/24

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 131.0.2903.86
```

214664 - Microsoft Edge (Chromium) < 132.0.2957.127 (CVE-2025-21262)

Synopsis

The remote host has an web browser installed that is affected by a vulnerability.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 132.0.2957.127. It is, therefore, affected by a vulnerability as referenced in the January 24, 2025 advisory.

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2025-21262)

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?bfeed288

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21262

Solution

Upgrade to Microsoft Edge version 132.0.2957.127 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

2.5

EPSS Score

0.0008

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-21262
XREF	IAVA:2025-A-0072-S

Plugin Information

Published: 2025/01/27, Modified: 2025/02/14

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 132.0.2957.127
```

232301 - Microsoft Edge (Chromium) < 134.0.3124.51 Multiple Vulnerabilities

Synopsis

The remote host has an web browser installed that is affected by multiple vulnerabilities.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 134.0.3124.51. It is, therefore, affected by multiple vulnerabilities as referenced in the March 7, 2025 advisory.

- No cwe for this issue in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network. (CVE-2025-26643)

- Out of bounds read in V8 in Google Chrome prior to 134.0.6998.35 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2025-1914)

- Improper Limitation of a Pathname to a Restricted Directory in DevTools in Google Chrome on Windows prior to 134.0.6998.35 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted Chrome Extension. (Chromium security severity: Medium) (CVE-2025-1915)

- Use after free in Profiles in Google Chrome prior to 134.0.6998.35 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.

(Chromium security severity: Medium) (CVE-2025-1916)

- Inappropriate implementation in Browser UI in Google Chrome on Android prior to 134.0.6998.35 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium) (CVE-2025-1917)

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?8caad375

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1914

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1915

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1916

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1917

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1918

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1919

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1921

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1922

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-1923

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26643

Solution

Upgrade to Microsoft Edge version 134.0.3124.51 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0007

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-1914
CVE	CVE-2025-1915
CVE	CVE-2025-1916
CVE	CVE-2025-1917
CVE	CVE-2025-1918
CVE	CVE-2025-1919
CVE	CVE-2025-1921
CVE	CVE-2025-1922
CVE	CVE-2025-1923
CVE	CVE-2025-26643
XREF	IAVA:2025-A-0173

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 122.0.2365.106
Fixed version     : 134.0.3124.51
```

175408 - Microsoft Teams < 1.6.0.11166 Information Disclosure

Synopsis

The version of Microsoft Teams installed on the remote Windows host is affected by an information disclosure vulnerability.

Description

The version of Microsoft Teams installed on the remote Windows host is version prior to 1.6.0.11166. It is, therefore, affected by an information disclosure vulnerability. An unauthenticated, remote attacker can exploit this to disclose potentially sensitive information.

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://learn.microsoft.com/en-us/officeupdates/teams-app-versioning

https://learn.microsoft.com/en-us/microsoftteams/teams-client-update

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24881

Solution

Upgrade to Microsoft Teams 1.6.0.11166 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

EPSS Score

0.0242

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-2023-24881
XREF	IAVA:2023-A-0247-S

Plugin Information

Published: 2023/05/12, Modified: 2023/08/11

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe
Installed version : 1.0.0.0
Fixed version     : 1.6.0.11166
```

166555 - WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

Synopsis

The remote Windows host is potentially missing a mitigation for a remote code execution vulnerability.

Description

The remote system may be in a vulnerable state to CVE-2013-3900 due to a missing or misconfigured registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config \EnableCertPaddingCheck An unauthenticated, remote attacker could exploit this, by sending specially crafted requests, to execute arbitrary code on an affected host.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

http://www.nessus.org/u?9780b9d2

Solution

Add and enable registry value EnableCertPaddingCheck:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

Additionally, on 64 Bit OS systems, Add and enable registry value EnableCertPaddingCheck:

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config \EnableCertPaddingCheck

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.6

EPSS Score

0.7694

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.6 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2013-3900
XREF	CISA-KNOWN-EXPLOITED:2022/07/10
XREF	IAVA:2013-A-0227

Plugin Information

Published: 2022/10/26, Modified: 2025/01/06

Plugin Output

tcp/445/cifs

```
Nessus detected the following potentially insecure registry key configuration:
   - Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not present in the
registry.
   - Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not
present in the registry.
```

16193 - Antivirus Software Check

Synopsis

An antivirus application is installed on the remote host.

Description

An antivirus application is installed on the remote host, and its engine and virus definitions are up to date.

See Also

http://www.nessus.org/u?3ed73b52

https://www.tenable.com/blog/auditing-anti-virus-products-with-nessus

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/01/18, Modified: 2023/10/05

Plugin Output

tcp/445/cifs

```
Forefront_Endpoint_Protection :

A Microsoft anti-malware product is installed on the remote host :

  Product name                 : Windows Defender
  Path                         : C:\ProgramData\Microsoft\Windows Defender\Platform
\4.18.25010.11-0\
  Version                      : 4.18.25010.11
  Engine version               : 1.1.25020.1007
  Antivirus signature version  : 1.425.238.0
  Antispyware signature version : 1.425.238.0
```

92415 - Application Compatibility Cache

Synopsis

Nessus was able to gather application compatibility settings on the remote host.

Description

Nessus was able to generate a report on the application compatibility cache on the remote Windows host.

See Also

https://dl.mandiant.com/EE/library/Whitepaper_ShimCacheParser.pdf

http://www.nessus.org/u?4a076105

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/23

Plugin Output

tcp/0

```
Application compatibility cache report attached.
```

34097 - BIOS Info (SMB)

Synopsis

BIOS info could be read.

Description

It is possible to get information about the BIOS via the host's SMB interface.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2024/06/11

Plugin Output

tcp/0

```
Version      : VirtualBox
Release date : 20061201000000.000000+000
Secure boot  : enabled
```

34096 - BIOS Info (WMI)

Synopsis

The BIOS info could be read.

Description

It is possible to get information about the BIOS via the host's WMI interface.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/05, Modified: 2025/03/11

Plugin Output

tcp/0

```
Vendor       : innotek GmbH
Version      : VirtualBox
Release date : 20061201000000.000000+000
UUID         : B77D91EF-602E-4EF3-B816-4269EE3AC34E
Secure boot  : enabled
```

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

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

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

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/03/13

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows_11:::x64-home -> Microsoft Windows 11

Following application CPE's matched on the remote system :

  cpe:/a:haxx:curl:8.8.0.0 -> Haxx Curl
  cpe:/a:microsoft:.net_framework:4.8.1 -> Microsoft .NET Framework
  cpe:/a:microsoft:edge:122.0.2365.106 -> Microsoft Edge
  cpe:/a:microsoft:ie:11.1.26100.0 -> Microsoft Internet Explorer
  cpe:/a:microsoft:internet_explorer:11.0.26100.1742 -> Microsoft Internet Explorer
  cpe:/a:microsoft:onedrive:25.46.310.5 -> Microsoft OneDrive
  cpe:/a:microsoft:remote_desktop_connection:10.0.26100.1000 -> Microsoft Remote Desktop Connection
  cpe:/a:microsoft:system_center_endpoint_protection:4.18.25010.11 -> Microsoft System Center
 Endpoint Protection
  cpe:/a:microsoft:teams:1.0.0.0 -> Microsoft Teams
  cpe:/a:microsoft:windows_defender:4.18.25010.11 -> Microsoft Windows Defender
```

24270 - Computer Manufacturer Information (WMI)

Synopsis

It is possible to obtain the name of the remote computer manufacturer.

Description

By making certain WMI queries, it is possible to obtain the model of the remote computer as well as the name of its manufacturer and its serial number.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/02/02, Modified: 2025/03/18

Plugin Output

tcp/0

```
Computer Manufacturer : innotek GmbH
Computer Model : VirtualBox
Computer SerialNumber : VirtualBox-b77d91ef-602e-4ef3-b816-4269ee3ac34e
Computer Type : Other

Computer Physical CPU's : 1
Computer Logical CPU's  : 3
  CPU0
    Architecture  : x64
    Physical Cores: 3
    Logical Cores : 3

Computer Memory : 15851 MB
```

171860 - Curl Installed (Windows)

Synopsis

Curl is installed on the remote Windows host.

Description

Curl, a command line tool for transferring data with URLs, was detected on the remote Windows host.

Please note, if the installation is located in either the Windows\System32 or Windows\SysWOW64 directory, it will be considered as managed by the OS. In this case, paranoid scanning is require to trigger downstream vulnerabilty checks. Paranoid scanning has no affect on this plugin itself.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/23, Modified: 2025/03/11

Plugin Output

tcp/0

```
Nessus detected 2 installs of Curl:

  Path          : c:\windows\system32\curl.exe
  Version       : 8.8.0.0
  Managed by OS : True

  Path          : c:\windows\syswow64\curl.exe
  Version       : 8.8.0.0
  Managed by OS : True
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/135/epmap

```
The following DCERPC services are available locally :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : SidKey Local End Point

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
```

```
Named pipe : lsasspirpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : lsapolicylookup

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : lsacap

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc  [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/445/cifs

```
The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Remote RPC service
Named pipe : \PIPE\ROUTER
Netbios name : \\WINDOWS11

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 338cd001-2244-31f1-aaaa-900038001003, version 1.0
Description : Remote Registry
Windows process : svchost.exe
Annotation : RemoteRegistry Interface
Type : Remote RPC service
Named pipe : \PIPE\winreg
Netbios name : \\WINDOWS11

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : da5a86c5-12c2-4943-ab30-7f74a813d853, version 1.0
Description : Unknown RPC service
Annotation : RemoteRegistry Perflib Interface
Type : Remote RPC service
Named pipe : \PIPE\winreg
Netbios name : \\WINDOWS11

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\WINDOWS11

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WINDOWS11

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WINDOWS11

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WINDOWS11

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49664/dce-rpc

```
The following DCERPC services are available on TCP port 49664 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.230.146

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.230.146

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.230.146

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
```

```
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.230.146
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49665/dce-rpc

```
The following DCERPC services are available on TCP port 49665 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.230.146
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49666/dce-rpc

```
The following DCERPC services are available on TCP port 49666 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.230.146

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.230.146
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49667/dce-rpc

```
The following DCERPC services are available on TCP port 49667 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.230.146
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49668/dce-rpc

```
The following DCERPC services are available on TCP port 49668 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.230.146

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.230.146

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.230.146

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
```

```
TCP Port : 49668
IP : 192.168.230.146

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.230.146
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49669/dce-rpc

```
The following DCERPC services are available on TCP port 49669 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49669
IP : 192.168.230.146
```

139785 - DISM Package List (Windows)

Synopsis

Use DISM to extract package info from the host.

Description

Using the Deployment Image Servicing Management tool, this plugin enumerates installed packages.

See Also

http://www.nessus.org/u?cbb428b2

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/08/25, Modified: 2025/03/11

Plugin Output

tcp/445/cifs

```
The following packages were enumerated using the Deployment Image Servicing and Management Tool:

Package      : Microsoft-OneCore-ApplicationModel-Sync-Desktop-FOD-
Package~31bf3856ad364e35~amd64~~10.0.26100.1742
State        : Installed
Release Type : OnDemand Pack
Install Time : 9/6/2024 4:10 AM

Package      : Microsoft-OneCore-DirectX-Database-FOD-
Package~31bf3856ad364e35~amd64~~10.0.26100.1742
State        : Installed
Release Type : OnDemand Pack
Install Time : 9/6/2024 4:10 AM

Package      : Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~en-
GB~10.0.26100.1742
State        : Installed
Release Type : Language Pack
Install Time : 9/6/2024 4:10 AM

Package      : Microsoft-Windows-Ethernet-Client-Intel-E1i68x64-FOD-
Package~31bf3856ad364e35~amd64~~10.0.26100.1742
State        : Installed
Release Type : OnDemand Pack
Install Time : 9/6/2024 4:10 AM
```

```
Package      : Microsoft-Windows-Ethernet-Client-Intel-E2f68-FOD-
Package~31bf3856ad364e35~amd64~~10.0.26100.1742
State        : Installed
Release Type : OnDemand Pack
Install Time : 9/6/2024 4:10 AM

Package      : Microsoft-Windows-Ethernet-Client-Realtek-Rtcx21x64-FOD-
Package~31bf3856ad364e35~amd64~~10.0.26100.1742
State        : Installed
Release Type : OnDemand Pack
Install Time : 9/6/2024 4:10 AM

Package      : Microsoft-Windows-Ethernet-Client-Vmware-Vmxnet3-FOD-
Package~31bf3856ad364e35~amd64~~10.0.26100.1742
State        : Installed
Release Type : OnDemand Pack
Install Time : 9/6/2024 4:10 AM

Package      : Microsoft-Windows-FodMetadata-Package~31bf3856ad364e35~amd64~~10.0.26100.1
State        : Installed
Release Type : Feature Pack
Install Time : 4/1/2024 4:12 PM

Package      : Microsoft-Windows-FodMetadataServicing-Desktop-CompDB-
Package~31bf3856ad364e35~amd64~~10.0.26100.1
State        : Installed
Release Type : Feature Pack
Install Time : 4/1/2024 4:12 PM

Package      : Microsoft-Windows-FodMetadataServicing-Desktop-Metadata-
Package~31bf3856ad364e35~amd64~~10.0.26100.1742
State        : Installed
Release Type : Feature Pack
Install [...]
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/03/11

Plugin Output

tcp/0

```
Hostname : WINDOWS11
  WINDOWS11 (WMI)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 101
```

71246 - Enumerate Local Group Memberships

Synopsis

Nessus was able to connect to a host via SMB to retrieve a list of local Groups and their Members.

Description

Nessus was able to connect to a host via SMB to retrieve a list of local Groups and their Members.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/12/06, Modified: 2025/03/11

Plugin Output

tcp/0

```
Group Name : Administrators
Host Name  : WINDOWS11
Group SID  : S-1-5-32-544
Members    :
  Name : Administrator
    Domain : WINDOWS11
    Class  : Win32_UserAccount
    SID    : S-1-5-21-933753971-2826297321-2361855607-500
  Name : kato
    Domain : WINDOWS11
    Class  : Win32_UserAccount
    SID    : S-1-5-21-933753971-2826297321-2361855607-1000

Group Name : Device Owners
Host Name  : WINDOWS11
Group SID  : S-1-5-32-583
Members    :

Group Name : Distributed COM Users
Host Name  : WINDOWS11
Group SID  : S-1-5-32-562
Members    :

Group Name : Event Log Readers
Host Name  : WINDOWS11
Group SID  : S-1-5-32-573
Members    :

Group Name : Guests
Host Name  : WINDOWS11
Group SID  : S-1-5-32-546
Members    :
```

```
  Name : Guest
    Domain : WINDOWS11
    Class  : Win32_UserAccount
    SID    : S-1-5-21-933753971-2826297321-2361855607-501

Group Name : Hyper-V Administrators
Host Name  : WINDOWS11
Group SID  : S-1-5-32-578
Members    :

Group Name : IIS_IUSRS
Host Name  : WINDOWS11
Group SID  : S-1-5-32-568
Members    :
  Name : IUSR
    Domain : WINDOWS11
    Class  : Win32_SystemAccount
    SID    : S-1-5-17

Group Name : OpenSSH Users
Host Name  : WINDOWS11
Group SID  : S-1-5-32-585
Members    :

Group Name : Performance Log Users
Host Name  : WINDOWS11
Group SID  : S-1-5-32-559
Members    :

Group Name : Performance Monitor Users
Host Name  : WINDOWS11
Group SID  : S-1-5-32-558
Members    :

Group Name : Remote Management Users
Host Name  : WINDOWS11
Group SID  : S-1-5-32-580
Members    :

Group Name : System Managed Accounts Group
Host Name  : WINDOWS11
Group SID  : S-1-5-32-581
Members    :
  Name : DefaultAccount
    Domain : WINDOWS11
    Class  : Win32_UserAccount
    SID    : S-1-5-21-933753971-2826297321-2361855607-503

Group Name : User Mode Hardware Operators
Host Name  : WINDOWS11
Group SID  : S-1-5-32-584
Members    :

Group Name : Users
Host Name  : WINDOWS11
Group SID  : S-1-5-32-545
Members    :
  Name : INTERACTIVE
    Domain : WINDOWS11
    Class  : Win32_SystemAccount
    SID    : S-1-5 [...]
```

72684 - Enumerate Users via WMI

Synopsis

Nessus was able to connect to a host via SMB to retrieve a list of users using WMI.

Description

Nessus was able to connect to a host via SMB to retrieve a list of users using WMI. Only identities that the authenticated SMB user has permissions to view will be retrieved by this plugin.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2014/02/25, Modified: 2025/03/11

Plugin Output

tcp/0

```
Name            : Administrator
SID             : S-1-5-21-933753971-2826297321-2361855607-500
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

Name            : DefaultAccount
SID             : S-1-5-21-933753971-2826297321-2361855607-503
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

Name            : Guest
SID             : S-1-5-21-933753971-2826297321-2361855607-501
Disabled        : True
Lockout         : False
Change password : False
Source          : Local

Name            : kato
SID             : S-1-5-21-933753971-2826297321-2361855607-1000
Disabled        : False
Lockout         : False
Change password : True
Source          : Local

Name            : WDAGUtilityAccount
```

```
SID             : S-1-5-21-933753971-2826297321-2361855607-504
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

No. Of Users : 5
```

168980 - Enumerate the PATH Variables

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

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

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/03/19

Plugin Output

tcp/0

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

C:\WINDOWS\system32
C:\WINDOWS
C:\WINDOWS\System32\Wbem
C:\WINDOWS\System32\WindowsPowerShell\v1.0\
C:\WINDOWS\System32\OpenSSH\
C:\Users\kato\AppData\Local\Microsoft\WindowsApps
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following card manufacturers were identified :

6C:A1:00:53:70:73 : Intel Corporate
08:00:27:11:82:D0 : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 6C:A1:00:53:70:73
  - 08:00:27:11:82:D0
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
192.168.230.146 resolves as windows11.
```

171410 - IP Assignment Method Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/03/19

Plugin Output

tcp/0

```
+ Loopback Pseudo-Interface 1
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ Ethernet
  + IPv4
    - Address       : 192.168.230.146
      Assign Method : dynamic
  + IPv6
    - Address       : fe80::d4ca:9a54:e938:a478%4
      Assign Method : dynamic
```

179947 - Intel CPUID detection

Synopsis

The processor CPUID was detected on the remote host.

Description

The CPUID of the Intel processor was detected on the remote host.

See Also

https://www.intel.com

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/18, Modified: 2025/03/11

Plugin Output

tcp/135/epmap

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

92421 - Internet Explorer Typed URLs

Synopsis

Nessus was able to enumerate URLs that were manually typed into the Internet Explorer address bar.

Description

Nessus was able to generate a list URLs that were manually typed into the Internet Explorer address bar.

See Also

https://forensafe.com/blogs/typedurls.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2024/05/08

Plugin Output

tcp/0

```
http://go.microsoft.com/fwlink/p/?LinkId=255141
http://go.microsoft.com/fwlink/p/?LinkId=255141
http://go.microsoft.com/fwlink/p/?LinkId=255141

Internet Explorer typed URL report attached.
```

160301 - Link-Local Multicast Name Resolution (LLMNR) Service Detection

Synopsis

Verify status of the LLMNR service on the remote host.

Description

The Link-Local Multicast Name Resolution (LLMNR) service allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link

See Also

http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2022/04/28, Modified: 2022/12/29

Plugin Output

tcp/445/cifs

```
LLMNR Key SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\EnableMulticast not found.
```

92424 - MUICache Program Execution History

Synopsis

Nessus was able to enumerate recently executed programs on the remote host.

Description

Nessus was able to query the MUIcache registry key to find evidence of program execution.

See Also

https://forensicartifacts.com/2010/08/registry-muicache/

http://windowsir.blogspot.com/2005/12/mystery-of-muicachesolved.html

http://www.nirsoft.net/utils/muicache_view.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/16

Plugin Output

tcp/0

```
c:\windows\system32\pcaui.exe.friendlyappname : Program Compatibility Assistant User Interface
c:\users\kato\downloads\firefox 1.0pr\firefox\firefox.exe.applicationcompany : Mozilla
c:\windows\system32\fsquirt.exe.applicationcompany : Microsoft Corporation
c:\windows\system32\shell32.dll.applicationcompany : Microsoft Corporation
c:\windows\system32\explorerframe.dll.friendlyappname : ExplorerFrame
c:\windows\system32\pcaui.exe.applicationcompany : Microsoft Corporation
c:\windows\system32\explorerframe.dll.applicationcompany : Microsoft Corporation
c:\windows\explorer.exe.applicationcompany : Microsoft Corporation
c:\windows\explorer.exe.friendlyappname : Windows Explorer
d:\vboxwindowsadditions-amd64.exe.friendlyappname : Oracle VirtualBox Guest Additions
c:\windows\system32\mmc.exe.friendlyappname : Microsoft Management Console
langid : .
c:\users\kato\downloads\firefox 1.0pr\firefox\firefox.exe.friendlyappname : Firefox
c:\windows\system32\shell32.dll.friendlyappname : Windows Shell Common Dll
d:\vboxwindowsadditions-amd64.exe.applicationcompany : Oracle and/or its affiliates
c:\windows\system32\fsquirt.exe.friendlyappname : fsquirt
c:\windows\system32\mmc.exe.applicationcompany : Microsoft Corporation
@%systemroot%\system32\drivers\wpdupfltr.sys,-100 : WPD Upper Class Filter Driver
@%systemroot%\system32\srvsvc.dll,-100 : Server
@tzres.dll,-352 : FLE Standard Time
```

```
@combase.dll,-5013 : The DCOMLAUNCH service launches COM and DCOM servers in response to object
 activation requests. If this service is stopped or disabled, programs using COM or DCOM will not
 function properly. It is strongly recommended that you have the DCOMLAUNCH service running.
@tzres.dll,-671 : AUS Eastern Summer Time
@tzres.dll,-2980 : (UTC+03:00) Moscow, St Petersburg
@%systemroot%\system32\axinstsv.dll,-103 : ActiveX Installer (AxInstSV)
@%systemroot%\system32\smphost.dll,-101 : Host service for the Microsoft Storage Spaces management
 provider. If this service is stopped or disabled, Storage Spaces cannot be managed.
@%systemroot%\system3 [...]
```

51351 - Microsoft .NET Framework Detection

Synopsis

A software framework is installed on the remote host.

Description

Microsoft .NET Framework, a software framework for Microsoft Windows operating systems, is installed on the remote host.

See Also

https://www.microsoft.com/net

http://www.nessus.org/u?15ae6806

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0655

Plugin Information

Published: 2010/12/20, Modified: 2022/10/18

Plugin Output

tcp/445/cifs

```
Nessus detected 2 installs of Microsoft .NET Framework:

  Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
  Version      : 4.8.1
  Full Version : 4.8.09032
  Install Type : Full
  Release      : 533320

  Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
  Version      : 4.8.1
  Full Version : 4.8.09032
  Install Type : Client
  Release      : 533320
```

176212 - Microsoft Edge Add-on Enumeration (Windows)

Synopsis

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

Description

Nessus was able to enumerate Microsoft Edge browser extensions installed on the remote host.

See Also

https://microsoftedge.microsoft.com/addons

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/05/22, Modified: 2025/03/11

Plugin Output

tcp/445/cifs

```
User : kato
|- Browser : Microsoft Edge
  |- Add-on information :

    Name    : unknown
    Version : 1.90.1
    Path    : C:\Users\kato\AppData\Local\Microsoft\Edge\User Data\Default\Extensions
\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.90.1_0

    Name        : Edge relevant text changes
    Description : Edge relevant text changes on select websites to improve user experience and
 precisely surfaces the action they want to take.
    Version     : 1.2.1
    Path        : C:\Users\kato\AppData\Local\Microsoft\Edge\User Data\Default\Extensions
\jmjflgjpcpepeafmmgdpfkogkghcpiha\1.2.1_0
```

136969 - Microsoft Edge Chromium Installed

Synopsis

Microsoft Edge (Chromium-based) is installed on the remote host.

Description

Microsoft Edge (Chromium-based), a Chromium-based web browser, is installed on the remote host.

See Also

https://www.microsoft.com/en-us/edge

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/05/29, Modified: 2025/03/11

Plugin Output

tcp/445/cifs

```
Path    : C:\Program Files (x86)\Microsoft\Edge\Application
Version : 122.0.2365.106
```

162560 - Microsoft Internet Explorer Installed

Synopsis

A web browser is installed on the remote Windows host.

Description

Microsoft Internet Explorer, a web browser bundled with Microsoft Windows, is installed on the remote Windows host.

See Also

https://support.microsoft.com/products/internet-explorer

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/06/28, Modified: 2025/03/11

Plugin Output

tcp/0

```
Path    : C:\WINDOWS\system32\mshtml.dll
Version : 11.0.26100.1742
```

72367 - Microsoft Internet Explorer Version Detection

Synopsis

Internet Explorer is installed on the remote host.

Description

The remote Windows host contains Internet Explorer, a web browser created by Microsoft.

See Also

https://support.microsoft.com/en-us/help/17621/internet-explorer-downloads

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0509

Plugin Information

Published: 2014/02/06, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Version  : 11.1.26100.0
```

138603 - Microsoft OneDrive Installed

Synopsis

A file hosting application is installed on the remote host.

Description

Microsoft OneDrive, a file hosting service, is installed on the remote host.

See Also

http://www.nessus.org/u?23c14184

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/07/17, Modified: 2025/03/11

Plugin Output

tcp/445/cifs

```
Path    : C:\Users\kato\AppData\Local\Microsoft\OneDrive\
Version : 25.46.310.5
```

57033 - Microsoft Patch Bulletin Feasibility Check

Synopsis

Nessus is able to check for Microsoft patch bulletins.

Description

Using credentials supplied in the scan policy, Nessus is able to collect information about the software and patches installed on the remote Windows host and will use that information to check for missing Microsoft security updates.

Note that this plugin is purely informational.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/06, Modified: 2021/07/12

Plugin Output

tcp/445/cifs

```
Nessus is able to test for missing patches using :
  Nessus
```

125835 - Microsoft Remote Desktop Connection Installed

Synopsis

A graphical interface connection utility is installed on the remote Windows host

Description

Microsoft Remote Desktop Connection (also known as Remote Desktop Protocol or Terminal Services Client) is installed on the remote Windows host.

See Also

http://www.nessus.org/u?1c33f0e7

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/06/12, Modified: 2022/10/10

Plugin Output

tcp/0

```
Path    : C:\WINDOWS\\System32\\mstsc.exe
Version : 10.0.26100.1000
```

93962 - Microsoft Security Rollup Enumeration

Synopsis

This plugin enumerates installed Microsoft security rollups.

Description

Nessus was able to enumerate the Microsoft security rollups installed on the remote Windows host.

See Also

http://www.nessus.org/u?b23205aa

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/10/11, Modified: 2024/11/21

Plugin Output

tcp/445/cifs

```
Cumulative Rollup : 09_2024 [KB5043080]
Cumulative Rollup : 08_2024

Latest effective update level : 09_2024
File checked                  : C:\WINDOWS\system32\ntoskrnl.exe
File version                  : 10.0.26100.1742
Associated KB                 : 5043080
```

144792 - Microsoft Teams Installed (Windows)

Synopsis

Microsoft Teams is installed on the remote Windows host.

Description

Microsoft Teams, a communication and collaboration tool, is installed on the remote Windows host.

Note that if the 'Show potential false alarms' setting is enabled, this plugin will attempt to detect the deployment file.

See Also

http://www.nessus.org/u?dbb8c851

https://docs.microsoft.com/en-us/microsoftteams/msi-deployment

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/01/07, Modified: 2025/03/11

Plugin Output

tcp/0

```
Path    : C:\Program Files\WindowsApps\MSTeams_1.0.0.0_x64__8wekyb3d8bbwe
Version : 1.0.0.0
```

10902 - Microsoft Windows 'Administrators' Group User List

Synopsis

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

Description

Using the supplied credentials, it is possible to extract the member list of the 'Administrators' group. Members of this group have complete 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: 2002/03/15, Modified: 2018/05/16

Plugin Output

tcp/445/cifs

```
The following users are members of the 'Administrators' group :

  - WINDOWS11\Administrator (User)
  - WINDOWS11\kato (User)
```

48763 - Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting

Synopsis

CWDIllegalInDllSearch Settings: Improper settings could allow code execution attacks.

Description

Windows Hosts can be hardened against DLL hijacking attacks by setting the The 'CWDIllegalInDllSearch' registry entry in to one of the following settings:

- 0xFFFFFFFF (Removes the current working directory from the default DLL search order)

- 1 (Blocks a DLL Load from the current working directory if the current working directory is set to a WebDAV folder)

- 2 (Blocks a DLL Load from the current working directory if the current working directory is set to a remote folder)

See Also

http://www.nessus.org/u?0c574c56

http://www.nessus.org/u?5234ef0c

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/08/26, Modified: 2019/12/20

Plugin Output

tcp/445/cifs

```
Name  : SYSTEM\CurrentControlSet\Control\Session Manager\CWDIllegalInDllSearch
Value : Registry Key Empty or Missing
```

10913 - Microsoft Windows - Local Users Information : Disabled Accounts

Synopsis

At least one local user account has been disabled.

Description

Using the supplied credentials, Nessus was able to list local user accounts that have been disabled.

Solution

Delete accounts that are no longer needed.

Risk Factor

None

Plugin Information

Published: 2002/03/17, Modified: 2018/08/13

Plugin Output

tcp/0

```
The following local user accounts have been disabled :

  - Administrator
  - Guest


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate
local users' setting, and then re-run the scan.
```

10914 - Microsoft Windows - Local Users Information : Never Changed Passwords

Synopsis

At least one local user has never changed his or her password.

Description

Using the supplied credentials, Nessus was able to list local users who have never changed their passwords.

Solution

Allow or require users to change their passwords regularly.

Risk Factor

None

Plugin Information

Published: 2002/03/17, Modified: 2019/07/08

Plugin Output

tcp/0

```
The following local user has never changed his/her password :\n
  - Guest


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate
local users' setting, and then re-run the scan.
```

10915 - Microsoft Windows - Local Users Information : User Has Never Logged In

Synopsis

At least one local user has never logged into his or her account.

Description

Using the supplied credentials, Nessus was able to list local users who have never logged into their accounts.

Solution

Delete accounts that are not needed.

Risk Factor

None

Plugin Information

Published: 2002/03/17, Modified: 2018/08/13

Plugin Output

tcp/0

```
The following local users have never logged in :

  - Administrator
  - Guest


Note that, in addition to the Administrator and Guest accounts, Nessus
has only checked for local users with UIDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for 'SMB use host SID to enumerate
local users' setting, and then re-run the scan.
```

92370 - Microsoft Windows ARP Table

Synopsis

Nessus was able to collect and report ARP table information from the remote host.

Description

Nessus was able to collect ARP table information from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2025/03/11

Plugin Output

tcp/0

```
192.168.230.67 : 6c-a1-00-53-70-73
192.168.230.152 : da-f4-f1-e4-70-4a
192.168.230.255 : ff-ff-ff-ff-ff-ff
224.0.0.22 : 01-00-5e-00-00-16
224.0.0.251 : 01-00-5e-00-00-fb
224.0.0.252 : 01-00-5e-00-00-fc
239.255.255.250 : 01-00-5e-7f-ff-fa
255.255.255.255 : ff-ff-ff-ff-ff-ff

Extended ARP table information attached.
```

92371 - Microsoft Windows DNS Cache

Synopsis

Nessus was able to collect and report DNS cache information from the remote host.

Description

Nessus was able to collect details of the DNS cache from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2025/03/11

Plugin Output

tcp/0

```
1D.tlu.dl.delivery.mp.microsoft.com
assets.msn.com
au.download.windowsupdate.com
cacerts.digicert.com
config.edge.skype.com
cp501.prod.do.dsp.mp.microsoft.com
ctldl.windowsupdate.com
displaycatalog.mp.microsoft.com
dl.delivery.mp.microsoft.com
download.windowsupdate.com
ecs.office.com
fe2cr.update.microsoft.com
fe3cr.delivery.mp.microsoft.com
geover.prod.do.dsp.mp.microsoft.com
kv501.prod.do.dsp.mp.microsoft.com
login.live.com
msedge.api.cdp.microsoft.com
msedge.b.tlu.dl.delivery.mp.microsoft.com
pti.store.microsoft.com
settings-win.data.microsoft.com
slscr.update.microsoft.com
slscr.update.microsoft.com
storeedgefd.dsx.mp.microsoft.com
v10.events.data.microsoft.com
v20.events.data.microsoft.com
windows.msn.com
www.bing.com
www.msftconnecttest.com
www.msn.com
```

```
DNS cache information attached.
```

92364 - Microsoft Windows Environment Variables

Synopsis

Nessus was able to collect and report environment variables from the remote host.

Description

Nessus was able to collect system and active account environment variables on the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0757

Plugin Information

Published: 2016/07/19, Modified: 2022/06/24

Plugin Output

tcp/0

```
Global Environment Variables :
  processor_level : 6
  comspec : %SystemRoot%\system32\cmd.exe
  number_of_processors : 3
  username : SYSTEM
  os : Windows_NT
  temp : %SystemRoot%\TEMP
  processor_revision : 8c01
  path : %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%
\System32\WindowsPowerShell\v1.0\;%SYSTEMROOT%\System32\OpenSSH\
  tmp : %SystemRoot%\TEMP
  processor_identifier : Intel64 Family 6 Model 140 Stepping 1, GenuineIntel
  driverdata : C:\Windows\System32\Drivers\DriverData
  pathext : .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
  processor_architecture : AMD64
  psmodulepath : %ProgramFiles%\WindowsPowerShell\Modules;%SystemRoot%\system32\WindowsPowerShell
\v1.0\Modules
  windir : %SystemRoot%

Active User Environment Variables
  - S-1-5-21-933753971-2826297321-2361855607-1000
    onedrive : C:\Users\kato\OneDrive
    temp : %USERPROFILE%\AppData\Local\Temp
    path : %USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
```

```
    tmp : %USERPROFILE%\AppData\Local\Temp
```

92365 - Microsoft Windows Hosts File

Synopsis

Nessus was able to collect the hosts file from the remote host.

Description

Nessus was able to collect the hosts file from the remote Windows host and report it as attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2020/01/27

Plugin Output

tcp/0

```
Windows hosts file attached.

MD5: 3688374325b992def12793500307566d
SHA-1: 4bed0823746a2a8577ab08ac8711b79770e48274
SHA-256: 2d6bdfb341be3a6234b24742377f93aa7c7cfb0d9fd64efa9282c87852e57085
```

187318 - Microsoft Windows Installed

Synopsis

The remote host is running Microsoft Windows.

Description

The remote host is running Microsoft Windows.

See Also

https://www.microsoft.com/en-us/windows

https://www.microsoft.com/en-us/windows-server

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/12/27, Modified: 2025/02/12

Plugin Output

tcp/0

```
OS Name      : Microsoft Windows 11 24H2
Vendor       : Microsoft
Product      : Windows
Release      : 11 24H2
Edition      : Home
Version      : 10.0.26100.1742
Role         : client
Kernel       : Windows NT 10.0
Architecture : x64
CPE v2.2     : cpe:/o:microsoft:windows_11_24h2:10.0.26100.1742:-
CPE v2.3     : cpe:2.3:o:microsoft:windows_11_24h2:10.0.26100.1742:-:*:*:home:*:x64:*
Type         : local
Method       : SMB
Confidence   : 100
```

20811 - Microsoft Windows Installed Software Enumeration (credentialed check)

Synopsis

It is possible to enumerate installed software.

Description

This plugin lists software potentially installed on the remote host by crawling the registry entries in :

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall HKLM\SOFTWARE\Microsoft\Updates

Note that these entries do not necessarily mean the applications are actually installed on the remote host - they may have been left behind by uninstallers, or the associated files may have been manually removed.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0501

Plugin Information

Published: 2006/01/26, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
The following software are installed on the remote host :

Microsoft Edge  [version 122.0.2365.106]  [installed on 2025/03/22]
Microsoft Edge Update  [version 1.3.195.45]
Microsoft Edge WebView2 Runtime  [version 122.0.2365.106]
Oracle VirtualBox Guest Additions 7.1.6  [version 7.1.6.167084]
```

178102 - Microsoft Windows Installed Software Version Enumeration

Synopsis

Enumerates installed software versions.

Description

This plugin enumerates the installed software version by interrogating information obtained from various registry entries and files on disk. This plugin provides a best guess at the software version and a confidence level for that version.

Note that the versions detected here do not necessarily indicate the actual installed version nor do they necessarily mean that the application is actually installed on the remote host. In some cases there may be artifacts left behind by uninstallers on the system.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2023/07/10, Modified: 2024/07/15

Plugin Output

tcp/445/cifs

```
The following software information is available on the remote host :

 - Oracle VirtualBox Guest Additions 7.1.6
     Best Confidence Version  : 7.1.6.36012
     Version Confidence Level : 3
     All Possible Versions    :  7.1.6.36012, 7.1.6.167084
     Other Version Data
       [DisplayName] :
           Raw Value           : Oracle VirtualBox Guest Additions 7.1.6
       [UninstallString] :
           Raw Value           : C:\Program Files\Oracle\VirtualBox Guest Additions\uninst.exe
           Parsed File Path    : C:\Program Files\Oracle\VirtualBox Guest Additions\uninst.exe
           Parsed File Version : 7.1.6.36012
       [DisplayVersion] :
           Raw Value           : 7.1.6.167084
       [Publisher] :
           Raw Value           : Oracle and/or its affiliates

 - Microsoft Edge WebView2 Runtime
     Best Confidence Version  : 122.0.2365.106
     Version Confidence Level : 2
     All Possible Versions    :  122.0.2365.106
```

```
     Other Version Data
       [Version] :
           Raw Value           : 122.0.2365.106
       [DisplayName] :
           Raw Value           : Microsoft Edge WebView2 Runtime
       [DisplayVersion] :
           Raw Value           : 122.0.2365.106

 - Microsoft Edge
     Best Confidence Version  : 122.0.2365.106
     Version Confidence Level : 3
     All Possible Versions    :  122.0.2365.106
     Other Version Data
       [InstallDate] :
           Raw Value           : 2025/03/22
       [DisplayIcon] :
           Raw Value           : C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe,0
           Parsed File Path    : C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
           Parsed File Version : 122.0.2365.106
       [InstallLocation] :
           Raw Value           : C:\Program Files (x86)\Microsoft\Edge\Application
       [UninstallString] :
           Raw Value           : "C:\Program Files (x86)\Microsoft\Edge\Application
\122.0.2365.106\Installer\setup.exe" --uninstall --msedge --system-level --verbose-logging
           Parsed Fil [...]
```

92366 - Microsoft Windows Last Boot Time

Synopsis

Nessus was able to collect the remote host's last boot time in a human readable format.

Description

Nessus was able to collect and report the remote host's last boot time as an ISO 8601 timestamp.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/07/09

Plugin Output

tcp/0

```
Last reboot : 2025-03-31T14:38:57+01:00 (20250331143857.500000+060)
```

161502 - Microsoft Windows Logged On Users

Synopsis

Nessus was able to determine the logged on users from the registry

Description

Using the HKU registry, Nessus was able to enuemrate the SIDs of logged on users

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/05/25, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

```
Logged on users :
  - S-1-5-21-933753971-2826297321-2361855607-1000
    Domain   : WINDOWS11
    Username : kato
```

63080 - Microsoft Windows Mounted Devices

Synopsis

It is possible to get a list of mounted devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates mounted devices that have been connected to the remote host in the past.

See Also

http://www.nessus.org/u?99fcc329

Solution

Make sure that the mounted drives agree with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2012/11/28, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
  Name     : \dosdevices\e:
  Data     : \??\SCSI#CdRom&Ven_VBOX&Prod_CD-ROM#4&2617aeae&0&020000#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f00560042004f00580026005000720 06f006400 5

  Name     : \??\volume{f7732036-0725-11f0-8ee0-806e6f6e6963}
  Data     : \??\SCSI#CdRom&Ven_VBOX&Prod_CD-ROM#4&2617aeae&0&010000#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f00560042004f00580026005000720 06f006400 5

  Name     : \??\volume{f7732037-0725-11f0-8ee0-806e6f6e6963}
  Data     : \??\SCSI#CdRom&Ven_VBOX&Prod_CD-ROM#4&2617aeae&0&020000#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f00560042004f00580026005000720 06f006400 5

  Name     : \dosdevices\d:
  Data     : \??\SCSI#CdRom&Ven_VBOX&Prod_CD-ROM#4&2617aeae&0&010000#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
```

```
 Raw data :
5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f00560042004f005800260050007200 6f0064005
[...]
```

92372 - Microsoft Windows NetBIOS over TCP/IP Info

Synopsis

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

Description

Nessus was able to collect details for NetBIOS over TCP/IP from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2025/03/11

Plugin Output

tcp/0

```
NBT information attached.
First 10 lines of all CSVs:
nbtstat_local.csv:
Interface,Name,Suffix,Type,Status,MAC
192.168.230.146,WINDOWS11,<20>,UNIQUE,Registered,08:00:27:11:82:D0
192.168.230.146,WINDOWS11,<00>,UNIQUE,Registered,08:00:27:11:82:D0
192.168.230.146,WORKGROUP,<00>,GROUP,Registered,08:00:27:11:82:D0
```

103871 - Microsoft Windows Network Adapters

Synopsis

Identifies the network adapters installed on the remote host.

Description

Using the supplied credentials, this plugin enumerates and reports the installed network adapters on the remote Windows host.

Solution

Make sure that all of the installed network adapters agrees with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0758

Plugin Information

Published: 2017/10/17, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Network Adapter Driver Description : Intel(R) PRO/1000 MT Desktop Adapter
Network Adapter Driver Version     : 8.4.13.0
```

92367 - Microsoft Windows PowerShell Execution Policy

Synopsis

Nessus was able to collect and report the PowerShell execution policy for the remote host.

Description

Nessus was able to collect and report the PowerShell execution policy for the remote Windows host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2020/06/12

Plugin Output

tcp/0

```
HKLM\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell\ExecutionPolicy : Restricted
HKLM\SOFTWARE\Wow6432Node\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell\ExecutionPolicy :
 Restricted
```

151440 - Microsoft Windows Print Spooler Service Enabled

Synopsis

The Microsoft Windows Print Spooler service on the remote host is enabled.

Description

The Microsoft Windows Print Spooler service (spoolsv.exe) on the remote host is enabled.

See Also

http://www.nessus.org/u?8fc5df24

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/07, Modified: 2021/07/07

Plugin Output

tcp/445/cifs

```
The Microsoft Windows Print Spooler service on the remote host is enabled.
```

70329 - Microsoft Windows Process Information

Synopsis

Use WMI to obtain running process information.

Description

Report details on the running processes on the machine.

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: 2013/10/08, Modified: 2025/03/11

Plugin Output

tcp/0

```
Process Overview :
SID: Process (PID)
 0 : System Idle Process (0)
 0 : |- System (4)
 0 :    |- Memory Compression (2340)
 0 :    |- smss.exe (444)
 0 : Registry (116)
 1 : explorer.exe (4688)
 1 : |- SecurityHealthSystray.exe (4696)
 1 : |- msedge.exe (5408)
 1 :    |- msedge.exe (4652)
 1 :    |- msedge.exe (4672)
 1 :    |- msedge.exe (5940)
 1 :    |- msedge.exe (6396)
 1 :    |- msedge.exe (760)
 1 :    |- msedge.exe (8068)
 1 : |- VBoxTray.exe (8224)
 1 : |- cmd.exe (8984)
 1 :    |- conhost.exe (8992)
 0 : csrss.exe (652)
 0 : wininit.exe (724)
 0 : |- fontdrvhost.exe (532)
 0 : |- services.exe (844)
 0 :    |- svchost.exe (1000)
 1 :       |- backgroundTaskHost.exe (1220)
 0 :       |- TiWorker.exe (4100)
 1 :       |- SearchHost.exe (5596)
 1 :       |- StartMenuExperienceHost.exe (5624)
```

```
1 :       |- Widgets.exe (5792)
1 :       |- RuntimeBroker.exe (5832)
1 :       |- RuntimeBroker.exe (5976)
1 :       |- dllhost.exe (6228)
1 :       |- SystemSettings.exe (6452)
1 :       |- backgroundTaskHost.exe (6512)
1 :       |- backgroundTaskHost.exe (6660)
0 :       |- WmiPrvSE.exe (6992)
1 :       |- RuntimeBroker.exe (7224)
1 :       |- ApplicationFrameHost.exe (7776)
1 :       |- UserOOBEBroker.exe (7900)
0 :       |- WmiPrvSE.exe (8732)
0 :       |- WmiPrvSE.exe (8812)
1 :       |- smartscreen.exe (8924)
1 :       |- OpenConsole.exe (9036)
1 :       |- WindowsTerminal.exe (9080)
1 :       |- RuntimeBroker.exe (9168)
0 :    |- VBoxService.exe (1056)
0 :    |- svchost.exe (1116)
0 :    |- svchost.exe (1128)
0 :    |- svchost.exe (1212)
0 :    |- svchost.exe (1236)
0 :    |- svchost.exe (1304)
0 :    |- svchost.exe (1372)
0 :    |- svchost.exe (1468)
0 :    |- svchost.exe (1492)
0 :    |- svchost.exe (1544)
0 :    |- svchost.exe (1552)
0 :    |- svchost.exe (1584)
0 :    |- svchost.exe (1648)
1 :       |- taskhostw.exe (4388)
0 :    |- svchost.exe (1688)
0 :    |- svchost.exe (1764)
0 :    |- svchost.exe (1792)
1 :    [...]
```

70331 - Microsoft Windows Process Module Information

Synopsis

Use WMI to obtain running process module information.

Description

Report details on the running processes modules on the machine.

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/08, Modified: 2025/03/11

Plugin Output

tcp/0

```
Process_Modules_.csv : lists the loaded modules for each process.
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/135/epmap

```
The Win32 process 'svchost.exe' is listening on this port (pid 428).

This process 'svchost.exe' (pid 428) is hosting the following Windows services :
RpcEptMapper (@%windir%\system32\RpcEpMap.dll,-1001)
RpcSs (@combase.dll,-5010)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

udp/137/netbios-ns

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

udp/138

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/139/smb

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/445/cifs

```
The Win32 process 'System' is listening on this port (pid 4).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

udp/500

```
The Win32 process 'svchost.exe' is listening on this port (pid 3280).

This process 'svchost.exe' (pid 3280) is hosting the following Windows services :
IKEEXT (@%SystemRoot%\system32\ikeext.dll,-501)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

udp/1900

```
The Win32 process 'svchost.exe' is listening on this port (pid 1872).

This process 'svchost.exe' (pid 1872) is hosting the following Windows services :
SSDPSRV (@%systemroot%\system32\ssdpsrv.dll,-100)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

udp/4500

```
The Win32 process 'svchost.exe' is listening on this port (pid 3280).

This process 'svchost.exe' (pid 3280) is hosting the following Windows services :
IKEEXT (@%SystemRoot%\system32\ikeext.dll,-501)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/5040

```
The Win32 process 'svchost.exe' is listening on this port (pid 4776).

This process 'svchost.exe' (pid 4776) is hosting the following Windows services :
CDPSvc (@%SystemRoot%\system32\cdpsvc.dll,-100)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

udp/5050

```
The Win32 process 'svchost.exe' is listening on this port (pid 4776).

This process 'svchost.exe' (pid 4776) is hosting the following Windows services :
CDPSvc (@%SystemRoot%\system32\cdpsvc.dll,-100)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

udp/5353

```
The Win32 process 'svchost.exe' is listening on this port (pid 2044).

This process 'svchost.exe' (pid 2044) is hosting the following Windows services :
Dnscache (@%SystemRoot%\System32\dnsapi.dll,-101)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

udp/5355

```
The Win32 process 'svchost.exe' is listening on this port (pid 2044).

This process 'svchost.exe' (pid 2044) is hosting the following Windows services :
Dnscache (@%SystemRoot%\System32\dnsapi.dll,-101)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/7680

```
The Win32 process 'svchost.exe' is listening on this port (pid 7576).

This process 'svchost.exe' (pid 7576) is hosting the following Windows services :
DoSvc (@%systemroot%\system32\dosvc.dll,-100)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/49664/dce-rpc

```
The Win32 process 'lsass.exe' is listening on this port (pid 876).

This process 'lsass.exe' (pid 876) is hosting the following Windows services :
KeyIso (@keyiso.dll,-100)
SamSs (@%SystemRoot%\system32\samsrv.dll,-1)
VaultSvc (@%SystemRoot%\system32\vaultsvc.dll,-1003)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/49665/dce-rpc

```
The Win32 process 'wininit.exe' is listening on this port (pid 724).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/49666/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 1648).

This process 'svchost.exe' (pid 1648) is hosting the following Windows services :
Schedule (@%SystemRoot%\system32\schedsvc.dll,-100)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/49667/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 1552).

This process 'svchost.exe' (pid 1552) is hosting the following Windows services :
EventLog (@%SystemRoot%\system32\wevtsvc.dll,-200)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/49668/dce-rpc

```
The Win32 process 'spoolsv.exe' is listening on this port (pid 768).

This process 'spoolsv.exe' (pid 768) is hosting the following Windows services :
Spooler (@%systemroot%\system32\spoolsv.exe,-1)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/49669/dce-rpc

```
The Win32 process 'services.exe' is listening on this port (pid 844).
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

tcp/49772

```
The Win32 process 'svchost.exe' is listening on this port (pid 3452).

This process 'svchost.exe' (pid 3452) is hosting the following Windows services :
Winmgmt (@%Systemroot%\system32\wbem\wmisvc.dll,-205)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

udp/50600

```
The Win32 process 'svchost.exe' is listening on this port (pid 2044).

This process 'svchost.exe' (pid 2044) is hosting the following Windows services :
Dnscache (@%SystemRoot%\System32\dnsapi.dll,-101)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

udp/59236

```
The Win32 process 'svchost.exe' is listening on this port (pid 2044).

This process 'svchost.exe' (pid 2044) is hosting the following Windows services :
Dnscache (@%SystemRoot%\System32\dnsapi.dll,-101)
```

34252 - Microsoft Windows Remote Listeners Enumeration (WMI)

Synopsis

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

Description

This script uses WMI to list the processes running on the remote host and listening on TCP / UDP ports.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/23, Modified: 2025/03/11

Plugin Output

udp/59239

```
The Win32 process 'svchost.exe' is listening on this port (pid 1872).

This process 'svchost.exe' (pid 1872) is hosting the following Windows services :
SSDPSRV (@%systemroot%\system32\ssdpsrv.dll,-100)
```

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/03/30, Modified: 2015/01/12

Plugin Output

tcp/445/cifs

```
The following password policy is defined on the remote host:

Minimum password len: 0
Password history len: 0
Maximum password age (d): 42
Password must meet complexity requirements: Enabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 600
Time between failed logon (s): 600
Number of invalid logon before locked out (s): 10
```

38689 - Microsoft Windows SMB Last Logged On User Disclosure

Synopsis

Nessus was able to identify the last logged on user on the remote host.

Description

By connecting to the remote host with the supplied credentials, Nessus was able to identify the username associated with the last successful logon.

Microsoft documentation notes that interactive console logons change the DefaultUserName registry entry to be the last logged-on user.

See Also

http://www.nessus.org/u?a29751b5

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/05/05, Modified: 2019/09/02

Plugin Output

tcp/445/cifs

```
Last Successful logon : .\kato
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- Guest account
- Supplied credentials

See Also

http://www.nessus.org/u?5c2589f6

https://support.microsoft.com/en-us/help/246261

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2024/12/06

Plugin Output

tcp/445/cifs

```
- The SMB tests will be done as kato/******
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2024/01/31

Plugin Output

tcp/445/cifs

```
The remote host SID value is : S-1-5-21-933753971-2826297321-2361855607

The value of 'RestrictAnonymous' setting is : 0
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
Nessus was able to obtain the following information about the host, by
parsing the SMB2 Protocol's NTLM SSP message:

Target Name: WINDOWS11
NetBIOS Domain Name: WINDOWS11
NetBIOS Computer Name: WINDOWS11
DNS Domain Name: windows11
DNS Computer Name: windows11
DNS Tree Name: unknown
Product Version: 10.0.26100
```

48942 - Microsoft Windows SMB Registry : OS Version and Processor Architecture

Synopsis

It was possible to determine the processor architecture, build lab strings, and Windows OS version installed on the remote system.

Description

Nessus was able to determine the processor architecture, build lab strings, and the Windows OS version installed on the remote system by connecting to the remote registry with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/08/31, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Operating system version = 10.26100
Architecture = x64
Build lab extended = 26100.1.amd64fre.ge_release.240331-1435
```

11457 - Microsoft Windows SMB Registry : Winlogon Cached Password Weakness

Synopsis

User credentials are stored in memory.

Description

The registry key 'HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon\CachedLogonsCount' is not 0. Using a value greater than 0 for the CachedLogonsCount key indicates that the remote Windows host locally caches the passwords of the users when they login, in order to continue to allow the users to login in the case of the failure of the primary domain controller (PDC).

Cached logon credentials could be accessed by an attacker and subjected to brute force attacks.

See Also

http://www.nessus.org/u?184d3eab

http://www.nessus.org/u?fe16cea8

https://technet.microsoft.com/en-us/library/cc957390.aspx

Solution

Consult Microsoft documentation and best practices.

Risk Factor

None

Plugin Information

Published: 2003/03/24, Modified: 2018/06/05

Plugin Output

tcp/445/cifs

```
Max cached logons : 10
```

10400 - Microsoft Windows SMB Registry Remotely Accessible

Synopsis

Access the remote Windows Registry.

Description

It was possible to access the remote Windows Registry using the login / password combination used for the Windows local checks (SMB tests).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

44401 - Microsoft Windows SMB Service Config Enumeration

Synopsis

It was possible to enumerate configuration parameters of remote services.

Description

Nessus was able to obtain, via the SMB protocol, the launch parameters of each active service on the remote host (executable path, logon type, etc.).

Solution

Ensure that each service is configured properly.

Risk Factor

None

References

XREF IAVT:0001-T-0752

Plugin Information

Published: 2010/02/05, Modified: 2022/05/16

Plugin Output

tcp/445/cifs

```
The following services are set to start automatically :

  AudioEndpointBuilder startup parameters :
    Display name : Windows Audio Endpoint Builder
    Service name : AudioEndpointBuilder
    Log on as : LocalSystem
    Executable path : C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p

  Audiosrv startup parameters :
    Display name : Windows Audio
    Service name : Audiosrv
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p
    Dependencies : AudioEndpointBuilder/RpcSs/

  BFE startup parameters :
    Display name : Base Filtering Engine
    Service name : BFE
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
    Dependencies : RpcSs/

  BrokerInfrastructure startup parameters :
```

```
    Display name : Background Tasks Infrastructure Service
    Service name : BrokerInfrastructure
    Log on as : LocalSystem
    Executable path : C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
    Dependencies : RpcEptMapper/DcomLaunch/RpcSs/

  CDPSvc startup parameters :
    Display name : Connected Devices Platform Service
    Service name : CDPSvc
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\WINDOWS\system32\svchost.exe -k LocalService -p
    Dependencies : ncbservice/RpcSS/Tcpip/

  CDPUserSvc_33782 startup parameters :
    Display name : Connected Devices Platform User Service_33782
    Service name : CDPUserSvc_33782
    Executable path : C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup

  CoreMessagingRegistrar startup parameters :
    Display name : CoreMessaging
    Service name : CoreMessagingRegistrar
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetwork -p
    Dependencies : rpcss/

  CryptSvc startup parameters :
    Display name : Cryptographic Services
    Service name : CryptSvc
    Log on as : NT Authority\NetworkService
    Executable path  [...]
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

```
An SMB server is running on this port.
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

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

10456 - Microsoft Windows SMB Service Enumeration

Synopsis

It is possible to enumerate remote services.

Description

This plugin implements the SvcOpenSCManager() and SvcEnumServices() calls to obtain, using the SMB protocol, the list of active and inactive services of the remote host.

An attacker may use this feature to gain better knowledge of the remote host.

Solution

To prevent the listing of the services from being obtained, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter incoming traffic to this port.

Risk Factor

None

References

XREF IAVT:0001-T-0751

Plugin Information

Published: 2000/07/03, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Active Services :

Application Identity [ AppIDSvc ]
Application Information [ Appinfo ]
AppX Deployment Service (AppXSVC) [ AppXSvc ]
Windows Audio Endpoint Builder [ AudioEndpointBuilder ]
Windows Audio [ Audiosrv ]
BitLocker Drive Encryption Service [ BDESVC ]
Base Filtering Engine [ BFE ]
Background Intelligent Transfer Service [ BITS ]
Background Tasks Infrastructure Service [ BrokerInfrastructure ]
Capability Access Manager Service [ camsvc ]
Connected Devices Platform Service [ CDPSvc ]
Client Licence Service (ClipSVC) [ ClipSVC ]
CoreMessaging [ CoreMessagingRegistrar ]
Cryptographic Services [ CryptSvc ]
DCOM Server Process Launcher [ DcomLaunch ]
Device Install Service [ DeviceInstall ]
DHCP Client [ Dhcp ]
Connected User Experiences and Telemetry [ DiagTrack ]
```

```
Display Policy Service [ DispBrokerDesktopSvc ]
DNS Client [ Dnscache ]
Delivery Optimization [ DoSvc ]
Diagnostic Policy Service [ DPS ]
Data Usage [ DusmSvc ]
Windows Event Log [ EventLog ]
COM+ Event System [ EventSystem ]
Windows Font Cache Service [ FontCache ]
Group Policy Client [ gpsvc ]
IKE and AuthIP IPsec Keying Modules [ IKEEXT ]
IP Helper [ iphlpsvc ]
CNG Key Isolation [ KeyIso ]
Server [ LanmanServer ]
Workstation [ LanmanWorkstation ]
Geolocation Service [ lfsvc ]
Windows License Manager Service [ LicenseManager ]
TCP/IP NetBIOS Helper [ lmhosts ]
Local Session Manager [ LSM ]
Microsoft Defender Core Service [ MDCoreSvc ]
Windows Defender Firewall [ mpssvc ]
Network Connection Broker [ NcbService ]
Network List Service [ netprofm ]
Network Setup Service [ NetSetupSvc ]
Network Store Interface Service [ nsi ]
Program Compatibility Assistant Service [ PcaSvc ]
Plug and Play [ PlugPlay ]
IPsec Policy Agent [ PolicyAgent ]
Power [ Power ]
User Profile Service [ ProfSvc ]
Remote Access Connection Manager [ RasMan ]
Remote Registry [ RemoteRegistry ]
Radio Management Service [ RmSvc ]
RPC Endpoint Mapper [ RpcEptMapper ]
Remote Procedure Call (RPC) [ RpcSs ]
Security Accounts Manager [  [...]
```

92373 - Microsoft Windows SMB Sessions

Synopsis

Nessus was able to collect and report SMB session information from the remote host.

Description

Nessus was able to collect details of SMB sessions from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2025/03/11

Plugin Output

tcp/0

```
kato

Extended SMB session information attached.
```

23974 - Microsoft Windows SMB Share Hosting Office Files

Synopsis

The remote share contains Office-related files.

Description

This plugin connects to the remotely accessible SMB shares and attempts to find office related files (such as .doc, .ppt, .xls, .pdf etc).

Solution

Make sure that the files containing confidential information have proper access controls set on them.

Risk Factor

None

Plugin Information

Published: 2007/01/04, Modified: 2011/03/21

Plugin Output

tcp/445/cifs

```
Here is a list of office files which have been found on the remote SMB
shares :

  + C$ :

    - C:\Windows\System32\MSDRM\MsoIrmProtector.doc
    - C:\Windows\SysWOW64\MSDRM\MsoIrmProtector.doc
    - C:\Windows\WinSxS\amd64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.26100.1150_none_a9b280b0a5669e69\MsoIrmProtector.doc
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.26100.1_none_151382ec926a1266\MsoIrmProtector.doc
    - C:\Windows\System32\MSDRM\MsoIrmProtector.ppt
    - C:\Windows\SysWOW64\MSDRM\MsoIrmProtector.ppt
    - C:\Windows\WinSxS\amd64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.26100.1150_none_a9b280b0a5669e69\MsoIrmProtector.ppt
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.26100.1_none_151382ec926a1266\MsoIrmProtector.ppt
    - C:\Windows\System32\MSDRM\MsoIrmProtector.xls
    - C:\Windows\SysWOW64\MSDRM\MsoIrmProtector.xls
    - C:\Windows\WinSxS\amd64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.26100.1150_none_a9b280b0a5669e69\MsoIrmProtector.xls
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.26100.1_none_151382ec926a1266\MsoIrmProtector.xls
```

11777 - Microsoft Windows SMB Share Hosting Possibly Copyrighted Material

Synopsis

The remote host may contain material (movies/audio) infringing copyright.

Description

This plugin displays a list of media files (such as .mp3, .ogg, .mpg, .avi) which have been found on the remote SMB shares.

Some of these files may contain copyrighted materials, such as commercial movies or music files, that are being shared without the owner's permission.

If any of these files actually contain copyrighted material, and if they are freely swapped around, your organization might be held liable for copyright infringement by associations such as the RIAA or the MPAA.

Solution

Delete the files infringing copyright.

Risk Factor

None

Plugin Information

Published: 2003/06/26, Modified: 2012/11/29

Plugin Output

tcp/445/cifs

```
Here is a list of files which have been found on the remote SMB shares.
Some of these files may contain copyrighted materials, such as commercial
movies or music files.

 + C$ :

C:\Windows\ImmersiveControlPanel\SystemSettings\Assets\Aria.mp3
C:\Windows\WinSxS\amd64_microsoft-windows-
i..ntrolpanel.appxmain_31bf3856ad364e35_10.0.26100.1591_none_b67e058f470e99bc\Jenny.mp3
C:\Windows\WinSxS\amd64_microsoft-windows-
i..ntrolpanel.appxmain_31bf3856ad364e35_10.0.26100.1591_none_b67e058f470e99bc\Guy.mp3
C:\Windows\WinSxS\amd64_microsoft-windows-
i..ntrolpanel.appxmain_31bf3856ad364e35_10.0.26100.1591_none_b67e058f470e99bc\Aria.mp3
C:\Windows\ImmersiveControlPanel\SystemSettings\Assets\Jenny.mp3
C:\Windows\ImmersiveControlPanel\SystemSettings\Assets\Guy.mp3
```

10396 - Microsoft Windows SMB Shares Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials.

Depending on the share rights, it may allow an attacker to read / write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2021/10/04

Plugin Output

tcp/445/cifs

```
The following shares can be accessed as kato :

- ADMIN$  - (readable,writable)
  + Content of this share :
..
appcompat
apppatch
AppReadiness
assembly
bcastdvr
bfsvc.exe
Boot
bootstat.dat
Branding
BrowserCore
CbsTemp
Core.xml
Cursors
debug
diagnostics
DiagTrack
DigitalLocker
Downloaded Program Files
DtcInstall.log
ELAMBKUP
en-GB
```

```
en-US
explorer.exe
Fonts
GameBarPresenceWriter
Globalization
Help
HelpPane.exe
hh.exe
IdentityCRL
IME
ImmersiveControlPanel
InboxApps
INF
InputMethod
Installer
L2Schemas
LanguageOverlayCache
LiveKernelReports
Logs
lsasetup.log
Media
mib.bin
Microsoft.NET
Migration
ModemLogs
notepad.exe
OCR
Offline Web Pages
Panther
Performance
PLA
PolicyDefinitions
Prefetch
Provisioning
regedit.exe
Registration
rescache
Resources
SchCache
schemas
security
ServiceProfiles
ServiceState
servicing
Setup
setupact.log
setuperr.log
ShellComponents
ShellExperiences
SKB
SoftwareDistribution
Speech
Speech_OneCore
splwow64.exe
System
system.ini
System32
SystemApps
SystemResources
SystemTemp
SysWOW64
TAPI
Tasks
Temp
tracing
twain_32
twain_32.dll
UUS
Vss
WaaS
```

```
Web
win.ini
WindowsShell.Manifest
WindowsUpdate.log

- C$  - (readable,writable)
  + Content of this share :
Documents and Settings
DumpStack.log.tmp
pagefile.sys
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
swapfile.sys
System Volume Information
Users
vboxpostinstall.log
Windows
```

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Here are the SMB shares available on the remote host when logged in as kato:

  - ADMIN$
  - C$
  - IPC$
```

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
  SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
3.0        Windows 8
3.0.2      Windows 8.1
3.1.1      Windows 10

The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.1        Windows 10
```

92368 - Microsoft Windows Scripting Host Settings

Synopsis

Nessus was able to collect and report the Windows scripting host settings from the remote host.

Description

Nessus was able to collect system and user level Windows scripting host settings from the remote Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/23

Plugin Output

tcp/0

```
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\displaylogo : 1
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\usewinsafer : 1
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\silentterminate : 0
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\activedebugging : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\displaylogo : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\usewinsafer : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\silentterminate : 0
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\activedebugging : 1

Windows scripting host configuration attached.
```

200493 - Microsoft Windows Start Menu Software Version Enumeration

Synopsis

Enumerates Start Menu software versions.

Description

This plugin enumerates the installed software version by interrogating information obtained from various registry entries and files on disk. This plugin provides a best guess at the software version and a confidence level for that version.

Note that the versions detected here do not necessarily indicate the actual installed version nor do they necessarily mean that the application is actually installed on the remote host. In some cases there may be artifacts left behind by uninstallers on the system.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2024/06/13, Modified: 2025/03/11

Plugin Output

tcp/445/cifs

```
The following software information is available on the remote host :

 - Microsoft Edge.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Microsoft Edge.lnk
     Target       : C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
     Version      : 122.0.2365.106

 - Remote Desktop Connection.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessories\Remote Desktop
 Connection.lnk
     Target       : C:\WINDOWS\system32\mstsc.exe
     Version      : 10.0.26100.1000

 - Steps Recorder.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessories\Steps
 Recorder.lnk
     Target       : C:\WINDOWS\system32\psr.exe
     Version      : 10.0.26100.1591

 - Windows Media Player Legacy.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessories\Windows Media
 Player Legacy.lnk
     Target       : C:\Program Files (x86)\Windows Media Player\wmplayer.exe
```

```
     Version      : 12.0.26100.1455

 - Character Map.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Accessories\System Tools
\Character Map.lnk
     Target       : C:\WINDOWS\system32\charmap.exe
     Version      : 5.2.3668.0

 - Component Services.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Administrative Tools
\Component Services.lnk
     Target       : C:\WINDOWS\system32\comexp.msc
     Version      : unknown

 - Computer Management.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Administrative Tools
\Computer Management.lnk
     Target       : C:\WINDOWS\system32\compmgmt.msc
     Version      : unknown

 - dfrgui.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Administrative Tools
\dfrgui.lnk
     Target       : C:\WINDOWS\system32\dfrgui.exe
     Version      : 10.0.26100.1

 - Disk Cleanup.lnk
     .lnk Path    : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\\Administrative Tools\Disk
 Cleanup.lnk
     Target       : C [...]
```

58452 - Microsoft Windows Startup Software Enumeration

Synopsis

It is possible to enumerate startup software.

Description

This plugin lists software that is configured to run on system startup by crawling the registry entries in :

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersi on\Run

Solution

Review the list of applications and remove any that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2012/03/23, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
The following startup item was found :

  SecurityHealth - %windir%\system32\SecurityHealthSystray.exe
  VBoxTray - %SystemRoot%\system32\VBoxTray.exe
```

38153 - Microsoft Windows Summary of Missing Patches

Synopsis

The remote host is missing several Microsoft security patches.

Description

This plugin summarizes updates for Microsoft Security Bulletins or Knowledge Base (KB) security updates that have not been installed on the remote Windows host based on the results of either a credentialed check using the supplied credentials or a check done using a supported third-party patch management tool.

Note the results of missing patches also include superseded patches.

Review the summary and apply any missing updates in order to be up to date.

Solution

Run Windows Update on the remote host or use a patch management solution.

Risk Factor

None

Plugin Information

Published: 2009/04/24, Modified: 2019/06/13

Plugin Output

tcp/445/cifs

```
The patches for the following bulletins or KBs are missing on the remote host :

 - KB5044284 ( https://support.microsoft.com/en-us/help/5044284 )
 - KB5046617 ( https://support.microsoft.com/en-us/help/5046617 )
 - KB5046696 ( https://support.microsoft.com/en-us/help/5046696 )
 - KB5048667 ( https://support.microsoft.com/en-us/help/5048667 )
 - KB5048794 ( https://support.microsoft.com/en-us/help/5048794 )
 - KB5049622 ( https://support.microsoft.com/en-us/help/5049622 )
 - KB5050009 ( https://support.microsoft.com/en-us/help/5050009 )
 - KB5051987 ( https://support.microsoft.com/en-us/help/5051987 )
 - KB5052105 ( https://support.microsoft.com/en-us/help/5052105 )
 - KB5053598 ( https://support.microsoft.com/en-us/help/5053598 )
```

92369 - Microsoft Windows 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 Windows host and generate a report as a CSV attachment.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2023/06/06

Plugin Output

tcp/0

```
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\TimeZoneKeyName : GMT Standard Time
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardName : @tzres.dll,-262
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightName : @tzres.dll,-261
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DynamicDaylightTimeDisabled : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardBias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightBias : 0xFFFFFFC4
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\Bias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\ActiveTimeBias : 0xFFFFFFC4
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightStart :
 00000300050001000000000000000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardStart :
 00000a0005000200000000000000000
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202503251052
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : cred
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.230.67
Port scanner(s) : wmi_netstat
Port range : default
Ping RTT : 2241.447 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : yes, as '192.168.230.146\kato' via SMB
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 : 2025/3/31 14:41 GMT Standard Time (UTC +01:00)
Scan duration : 1158 sec
Scan for malware : no
```

64582 - Netstat Connection Information

Synopsis

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

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/0

```
Nessus was able to find 23 open ports.
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/135/epmap

```
Port 135/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

udp/137/netbios-ns

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

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

udp/138

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

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

udp/500

```
Port 500/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

udp/1900

```
Port 1900/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

udp/4500

```
Port 4500/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/5040

```
Port 5040/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

udp/5050

```
Port 5050/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

udp/5353

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

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

udp/5355

```
Port 5355/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/7680

```
Port 7680/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/49664/dce-rpc

```
Port 49664/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/49665/dce-rpc

```
Port 49665/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/49666/dce-rpc

```
Port 49666/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/49667/dce-rpc

```
Port 49667/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/49668/dce-rpc

```
Port 49668/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/49669/dce-rpc

```
Port 49669/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

tcp/49772

```
Port 49772/tcp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

udp/50600

```
Port 50600/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

udp/59236

```
Port 59236/udp was found to be open
```

34220 - Netstat Portscanner (WMI)

Synopsis

Remote open ports can be enumerated via WMI.

Description

Using the WMI interface, Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/09/16, Modified: 2025/03/11

Plugin Output

udp/59239

```
Port 59239/udp was found to be open
```

24272 - Network Interfaces Enumeration (WMI)

Synopsis

Nessus was able to obtain the list of network interfaces on the remote host.

Description

Nessus was able, via WMI queries, to extract a list of network interfaces on the remote host and the IP addresses attached to them.

Note that this plugin only enumerates IPv6 addresses for systems running Windows Vista or later.

See Also

http://www.nessus.org/u?b362cab2

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/02/03, Modified: 2025/03/11

Plugin Output

tcp/0

```
+ Network Interface Information :

 - Network Interface = [00000000] Intel(R) PRO/1000 MT Desktop Adapter
 - MAC Address = 08:00:27:11:82:D0
 - IPAddress/IPSubnet = 192.168.230.146/255.255.255.0
 - IPAddress/IPSubnet = fe80::d4ca:9a54:e938:a478/64


+ Routing Information :

    Destination     Netmask         Gateway
    -----------     -------         -------
    0.0.0.0         0.0.0.0         192.168.230.152
    127.0.0.0       255.0.0.0       0.0.0.0
    127.0.0.1       255.255.255.255 0.0.0.0
    127.255.255.255 255.255.255.255 0.0.0.0
    192.168.230.0   255.255.255.0   0.0.0.0
    192.168.230.146 255.255.255.255 0.0.0.0
    192.168.230.255 255.255.255.255 0.0.0.0
    224.0.0.0       240.0.0.0       0.0.0.0
    224.0.0.0       240.0.0.0       0.0.0.0
    255.255.255.255 255.255.255.255 0.0.0.0
```

```
    255.255.255.255 255.255.255.255 0.0.0.0
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Microsoft Windows 11 Home Build 26100
Confidence level : 101
Method : Misc
Type : general-purpose
Fingerprint : unknown

Remote operating system : Microsoft Windows 10 Home Build 26100
Confidence level : 100
Method : SMB_OS
Type : general-purpose
Fingerprint : unknown
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows 11 Home Build 26100
Confidence level : 101
Method : Misc


The remote host is running Microsoft Windows 11 Home Build 26100
```

117887 - OS Security Patch Assessment Available

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0516

Plugin Information

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

Plugin Output

tcp/445/cifs

```
OS Security Patch Assessment is available.

Account  : 192.168.230.146\kato
Protocol : SMB
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/03/11

Plugin Output

tcp/0

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

+ Install the following Microsoft patches :
- KB5053598 (1 vulnerabilities)
- KB5049622
- KB5048794
- KB5046696

[ Microsoft Edge (Chromium) < 134.0.3124.83 Multiple Vulnerabilities (233201) ]

+ Action to take : Upgrade to Microsoft Edge version 134.0.3124.83 or later.

+Impact : Taking this action will resolve 271 different vulnerabilities (CVEs).


[ Microsoft Teams < 1.6.0.18681 RCE (179635) ]

+ Action to take : Upgrade to Microsoft Teams 1.6.0.18681 or later.

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


[ Security Updates for Microsoft .NET Framework (January 2025) (214274) ]
```

```
+ Action to take : Microsoft has released security updates for Microsoft .NET Framework.
```

92428 - Recent File History

Synopsis

Nessus was able to enumerate recently opened files on the remote host.

Description

Nessus was able to gather evidence of files opened by file type from the remote host.

See Also

https://www.4n6k.com/2014/02/forensics-quickie-pinpointing-recent.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/11/15

Plugin Output

tcp/0

```
C:\\Users\kato\AppData\Roaming\Microsoft\Windows\Recent\Network and Sharing Centre.lnk

Recent files found in registry and appdata attached.
```

92429 - Recycle Bin Files

Synopsis

Nessus was able to enumerate files in the recycle bin on the remote host.

Description

Nessus was able to generate a list of all files found in $Recycle.Bin subdirectories.

See Also

http://www.nessus.org/u?0c1a03df

http://www.nessus.org/u?61293b38

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/11/15

Plugin Output

tcp/0

```
C:\\$Recycle.Bin\\.
C:\\$Recycle.Bin\\..
C:\\$Recycle.Bin\\S-1-5-18
C:\\$Recycle.Bin\\S-1-5-21-933753971-2826297321-2361855607-1000
C:\\$Recycle.Bin\\S-1-5-18\.
C:\\$Recycle.Bin\\S-1-5-18\..
C:\\$Recycle.Bin\\S-1-5-18\desktop.ini
C:\\$Recycle.Bin\\S-1-5-21-933753971-2826297321-2361855607-1000\.
C:\\$Recycle.Bin\\S-1-5-21-933753971-2826297321-2361855607-1000\..
C:\\$Recycle.Bin\\S-1-5-21-933753971-2826297321-2361855607-1000\desktop.ini
```

92430 - Registry Editor Last Accessed

Synopsis

Nessus was able to find the last key accessed by the Registry Editor when it was closed on the remote host.

Description

Nessus was able to find evidence of the last key that was opened when the Registry Editor was closed for each user.

See Also

https://support.microsoft.com/en-us/help/244004

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/11/15

Plugin Output

tcp/0

```
kato
  - Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```

10860 - SMB Use Host SID to Enumerate Local Users

Synopsis

Nessus was able to enumerate local users.

Description

Using the host security identifier (SID), Nessus was able to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2023/02/28

Plugin Output

tcp/445/cifs

```
  - Administrator (id 500, Administrator account)
  - Guest (id 501, Guest account)
  - kato (id 1000)

Note that, in addition to the Administrator, Guest, and Kerberos
accounts, Nessus has enumerated local users with IDs between
1000 and 1200. To use a different range, edit the scan policy
and change the 'Enumerate Local Users: Start UID' and/or 'End UID'
preferences under 'Assessment->Windows' and re-run the scan. Only
UIDs between 1 and 2147483647 are allowed for this range.
```

160486 - Server Message Block (SMB) Protocol Version Detection

Synopsis

Verify the version of SMB on the remote host.

Description

The Server Message Block (SMB) Protocol provides shared access to files and printers across nodes on a network.

See Also

http://www.nessus.org/u?f463096b

http://www.nessus.org/u?1a4b3744

Solution

Disable SMB version 1 and block all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

Risk Factor

None

Plugin Information

Published: 2022/05/04, Modified: 2022/05/04

Plugin Output

tcp/445/cifs

```
- SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB2 : Key not found.
- SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB3 : Key not found.
- SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB1 : Key not found.
```

150799 - Target Access Problems by Authentication Protocol - Maximum Privilege Account Used in Scan

Synopsis

Nessus scanned the target host with the highest available privilege level. Yet Nessus encountered permissions issues while accessing one or more items during the scan.

Description

Nessus was able to log in to the remote host using the provided credentials. The provided credentials have the highest privilege possible on the remote host. Yet Nessus encountered permissions issues while accessing items during the scan.

It is likely that this condition is caused by one or more of the following:

1) A plugin tried to access a resource that requires a special privilege level such as NT_AUTHORITY on Windows. The resource may have had its permissions altered since the plugin was written.

2) Environmental issues may have caused an intermittent failure in authentication that caused Nessus to stop attempting privilege escalation.

3) A resource on the host that Nessus attempts to access multiple times may be configured with access limits. Related lockouts may look like permissions failures.

4) Nessus may have tried to access a resource that does not exist on a target that fails to properly report permissions issues.

For instance, on some legacy unix systems such as AIX or HP-UX there is no way to distinguish a missing resource from a permissions error.

If you believe that the plugin indicated attempted to access the wrong resource or a resource that has recently received special OS protection, please contact Tenable Support.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/06, Modified: 2021/07/06

Plugin Output

tcp/445/cifs

```
Nessus was able to log in to the remote host via the following
protocol as kato. This credential has the highest
privilege level possible for this host. Yet Nessus encountered
the following permissions issues while performing the planned checks:
```

```
  Protocol        : SMB
  Port            : 445

Problems:
Plugin 171956:  Permission was denied while opening 'WINDOWS\System32\Tasks\Microsoft\Windows
\Security\Pwdless\IntelligentPwdlessTask'.
```

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

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

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

Please note the following :

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Nessus was able to log in to the remote host via the following :

User:       '192.168.230.146\kato'
Port:       445
Proto:      SMB
Method:     password
```

161691 - The Microsoft Windows Support Diagnostic Tool (MSDT) RCE Workaround Detection (CVE-2022-30190)

Synopsis

Checks for the HKEY_CLASSES_ROOT\ms-msdt registry key.

Description

The remote host has the HKEY_CLASSES_ROOT\ms-msdt registry key. This is a known exposure for CVE-2022-30190.

Note that Nessus has not tested for CVE-2022-30190. It is only checking if the registry key exists. The recommendation is to apply the latest patch.

See Also

http://www.nessus.org/u?440e4ba1

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

http://www.nessus.org/u?b9345997

Solution

Apply the latest Cumulative Update.

Risk Factor

None

Plugin Information

Published: 2022/05/31, Modified: 2022/07/28

Plugin Output

tcp/445/cifs

```
The HKEY_CLASSES_ROOT\ms-msdt registry key exists on the target. This may indicate that the target
 is vulnerable to CVE-2022-30190, if the vendor patch is not applied.
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
20250331143857.500000+060
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.230.67 to 192.168.230.146 :
192.168.230.67

ttl was greater than 50 - Completing Traceroute.

?

Hop Count: 1

An error was detected along the way.
```

92434 - User Download Folder Files

Synopsis

Nessus was able to enumerate downloaded files on the remote host.

Description

Nessus was able to generate a report of all files listed in the default user download folder.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/16

Plugin Output

tcp/0

```
C:\\Users\kato\Downloads\desktop.ini
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\AccessibleMarshal.dll
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\browser.jar
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\chrome.rdf
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\chromelist.txt
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\classic.jar
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\comm.jar
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\embed-sample.jar
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\en-US.jar
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\help.jar
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\icons\default\winInspectorMain.ico
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\inspector.jar
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\installed-chrome.txt
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\modern.jar
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\overlayinfo\browser\content\overlays.rdf
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\overlayinfo\communicator\content\overlays.rdf
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\overlayinfo\inspector\content\overlays.rdf
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\overlayinfo\messenger\content\overlays.rdf
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\overlayinfo\navigator\content\overlays.rdf
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\pipnss.jar
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\pippki.jar
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\chrome\toolkit.jar
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\components\accessibility-msaa.xpt
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\components\accessibility.xpt
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\components\alerts.xpt
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\components\appshell.xpt
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\components\autocomplete.xpt
C:\\Users\kato\Downloads\Firefox 1.0PR\firefox\components\autocon [...]
```

92431 - User Shell Folders Settings

Synopsis

Nessus was able to find the folder paths for user folders on the remote host.

Description

Nessus was able to gather a list of settings from the target system that store common user folder locations. A few of the more common locations are listed below :

- Administrative Tools
- AppData
- Cache
- CD Burning
- Cookies
- Desktop
- Favorites
- Fonts
- History
- Local AppData
- My Music
- My Pictures
- My Video
- NetHood
- Personal
- PrintHood
- Programs
- Recent
- SendTo
- Start Menu
- Startup
- Templates

See Also

https://technet.microsoft.com/en-us/library/cc962613.aspx

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/16

Plugin Output

tcp/0

```
kato
  - {7d1d3a04-debb-4115-95cf-2f29da2920da} : C:\Users\kato\Searches
  - {1b3ea5dc-b587-4786-b4ef-bd1dc332aeae} : C:\Users\kato\AppData\Roaming\Microsoft\Windows
\Libraries
  - {374de290-123f-4565-9164-39c4925e467b} : C:\Users\kato\Downloads
  - recent : C:\Users\kato\AppData\Roaming\Microsoft\Windows\Recent
  - my video : C:\Users\kato\Videos
  - my music : C:\Users\kato\Music
  - {56784854-c6cb-462b-8169-88e350acb882} : C:\Users\kato\Contacts
  - {bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968} : C:\Users\kato\Links
  - {a520a1a4-1780-4ff6-bd18-167343c5af16} : C:\Users\kato\AppData\LocalLow
  - sendto : C:\Users\kato\AppData\Roaming\Microsoft\Windows\SendTo
  - start menu : C:\Users\kato\AppData\Roaming\Microsoft\Windows\Start Menu
  - cookies : C:\Users\kato\AppData\Local\Microsoft\Windows\INetCookies
  - personal : C:\Users\kato\Documents
  - administrative tools : C:\Users\kato\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
\Administrative Tools
  - startup : C:\Users\kato\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
  - nethood : C:\Users\kato\AppData\Roaming\Microsoft\Windows\Network Shortcuts
  - history : C:\Users\kato\AppData\Local\Microsoft\Windows\History
  - {4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4} : C:\Users\kato\Saved Games
  - {00bcfc5a-ed94-4e48-96a1-3f6217f21990} : C:\Users\kato\AppData\Local\Microsoft\Windows
\RoamingTiles
  - !do not use this registry key : Use the SHGetFolderPath or SHGetKnownFolderPath function instead
  - local appdata : C:\Users\kato\AppData\Local
  - my pictures : C:\Users\kato\Pictures
  - templates : C:\Users\kato\AppData\Roaming\Microsoft\Windows\Templates
  - printhood : C:\Users\kato\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
  - cache : C:\Users\kato\AppData\Local\Microsoft\Windows\INetCache
  - desktop : C:\Users\kato\Desktop
  - programs : C:\Users\kato\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
  - fonts : C:\WINDOWS\Fonts
  - cd burning : C:\Users\kato\AppData\Local\Microsoft\Windows\Burn\Burn
  - favorites : C:\Users\kato\Favorit [...]
```

92435 - UserAssist Execution History

Synopsis

Nessus was able to enumerate program execution history on the remote host.

Description

Nessus was able to gather evidence from the UserAssist registry key that has a list of programs that have been executed.

See Also

https://www.nirsoft.net/utils/userassist_view.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2019/11/12

Plugin Output

tcp/0

```
windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel
microsoft.windows.controlpanel
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\pcaui.exe
microsoft.windowscalculator_8wekyb3d8bbwe!app
microsoft.windowsterminal_8wekyb3d8bbwe!app
microsoft.windowsfeedbackhub_8wekyb3d8bbwe!app
d:\vboxwindowsadditions-amd64.exe
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\services.msc
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\file explorer.lnk
microsoft.paint_8wekyb3d8bbwe!app
microsoft.windows.startmenuexperiencehost_cw5n1h2txyewy!app
microsoft.windowsnotepad_8wekyb3d8bbwe!app
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\administrative tools\services.lnk
d:\vboxwindowsadditions.exe
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\wf.msc
microsoft.microsoftstickynotes_8wekyb3d8bbwe!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\useraccountcontrolsettings.exe
microsoft.xboxgamingoverlay_8wekyb3d8bbwe!app
ueme_ctlcuacount:ctor
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\microsoft edge.lnk
c:\users\kato\downloads\firefox 1.0pr\firefox\firefox.exe
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\cmd.exe
{f38bf404-1d43-42f2-9305-67de0b28fc23}\regedit.exe
msedge
```

```
microsoft.gethelp_8wekyb3d8bbwe!app
microsoft.windows.explorer
{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\system tools\command prompt.lnk
{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\system tools\control panel.lnk
ueme_ctlsession
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\administrative tools\registry editor.lnk
microsoft.windows.shellexperiencehost_cw5n1h2txyewy!app
microsoftwindows.client.cbs_cw5n1h2txyewy!cortanaui

Extended userassist report attached.
```

24269 - WMI Available

Synopsis

WMI queries can be made against the remote host.

Description

The supplied credentials can be used to make WMI (Windows Management Instrumentation) requests against the remote host over DCOM.

These requests can be used to gather information about the remote host, such as its current state, network interface configuration, etc.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/02/03, Modified: 2025/03/11

Plugin Output

tcp/445/cifs

```
The remote host returned the following caption from Win32_OperatingSystem:

Microsoft Windows 11 Home
```

51187 - WMI Encryptable Volume Enumeration

Synopsis

The remote Windows host has encryptable volumes available.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates encryptable volume information available on the remote host via WMI.

See Also

http://www.nessus.org/u?8aa7973e

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/12/15, Modified: 2025/03/11

Plugin Output

tcp/0

```
Here is a list of encryptable volumes available on the remote system :

+ DriveLetter C:

  - BitLocker Version : 2.0
  - Conversion Status : Used Space Only Encrypted
  - DeviceID : \\?\Volume{e16434cf-b74b-4575-8970-4b6fa8fcab21}\
  - Encryption Method : XTS-AES 128
  - Identification Field : Unknown
  - Key Protectors : None Found
  - Lock Status : Unlocked
  - Percentage Encrypted : 100.0%
  - PersistentVolumeID : {045B323F-E892-436B-9E7A-DB91007B758D}
  - Protection Status : Protection Off
  - Size : 78.85 GB
```

52001 - WMI QuickFixEngineering (QFE) Enumeration

Synopsis

The remote Windows host has quick-fix engineering updates installed.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via WMI.

See Also

http://www.nessus.org/u?0c4ec249

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/16, Modified: 2025/03/11

Plugin Output

tcp/0

```
Here is a list of quick-fix engineering updates installed on the
remote system :

+ KB5042098
  - Description : Update
  - InstalledOn : 9/6/2024

+ KB5043080
  - Description : Security Update
  - InstalledOn : 9/6/2024

+ KB5043113
  - Description : Security Update
  - InstalledOn : 9/6/2024

Note that for detailed information on installed QFE's such as InstalledBy, Caption,
and so on, please run the scan with 'Report Verbosity' set to 'verbose'.
```

51186 - WMI Trusted Platform Module Enumeration

Synopsis

The remote Windows host has a Trusted Platform Module available.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates information about the Trusted Platform Module installed on the remote host via WMI.

See Also

http://www.nessus.org/u?69aba7c6

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/12/14, Modified: 2025/03/11

Plugin Output

tcp/0

```
Here is the info about the Trusted Platform Modules installed on
the remote system :

+ ManufacturerId : IBM/1229081856

  - IsActivated_InitialValue : 1
  - IsEnabled_InitialValue : 1
  - IsOwned_InitialValue : 1
  - ManufacturerVersion : 8217.4131.22.13878
  - PhysicalPresenceVersionInfo : 1.3
  - SpecVersion : 2.0, 0, 1.64
```

44871 - WMI Windows Feature Enumeration

Synopsis

It is possible to enumerate Windows features using WMI.

Description

Nessus was able to enumerate the server features of the remote host by querying the 'Win32_ServerFeature' class of the '\Root\cimv2' WMI namespace for Windows Server versions or the 'Win32_OptionalFeature' class of the '\Root\cimv2' WMI namespace for Windows Desktop versions.

Note that Features can only be enumerated for Windows 7 and later for desktop versions.

See Also

https://msdn.microsoft.com/en-us/library/cc280268

https://docs.microsoft.com/en-us/windows/desktop/WmiSdk/querying-the-status-of-optional-features

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0754

Plugin Information

Published: 2010/02/24, Modified: 2025/03/11

Plugin Output

tcp/0

```
Nessus enumerated the following Windows features :

  - MSRDC-Infrastructure
  - MediaPlayback
  - MicrosoftWindowsPowerShellV2
  - MicrosoftWindowsPowerShellV2Root
  - NetFx4-AdvSrvs
  - Printing-Foundation-Features
  - Printing-Foundation-InternetPrinting-Client
  - Printing-PrintToPDFServices-Features
  - SearchEngine-Client-Package
  - WCF-Services45
```

```
    - WCF-TCP-PortSharing45
    - WindowsMediaPlayer
    - WorkFolders-Client
```

162174 - Windows Always Installed Elevated Status

Synopsis

Windows AlwaysInstallElevated policy status was found on the remote Windows host

Description

Windows AlwaysInstallElevated policy status was found on the remote Windows host.

You can use the AlwaysInstallElevated policy to install a Windows Installer package with elevated (system) privileges This option is equivalent to granting full administrative rights, which can pose a massive security risk. Microsoft strongly discourages the use of this setting.

Solution

If enabled, disable AlwaysInstallElevated policy per your corporate security guidelines.

Risk Factor

None

Plugin Information

Published: 2022/06/14, Modified: 2022/06/14

Plugin Output

tcp/445/cifs

```
AlwaysInstallElevated policy is not enabled under HKEY_LOCAL_MACHINE.
AlwaysInstallElevated policy is not enabled under HKEY_USERS
 user:S-1-5-21-933753971-2826297321-2361855607-1000
```

48337 - Windows ComputerSystemProduct Enumeration (WMI)

Synopsis

It is possible to obtain product information from the remote host using WMI.

Description

By querying the WMI class 'Win32_ComputerSystemProduct', it is possible to extract product information about the computer system such as UUID, IdentifyingNumber, vendor, etc.

See Also

http://www.nessus.org/u?a21ce849

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/08/16, Modified: 2025/03/11

Plugin Output

tcp/0

```
+ Computer System Product
  - IdentifyingNumber : VirtualBox-b77d91ef-602e-4ef3-b816-4269ee3ac34e
  - Description       : Computer System Product
  - Vendor            : innotek GmbH
  - Name              : VirtualBox
  - UUID              : B77D91EF-602E-4EF3-B816-4269EE3AC34E
  - Version           : 1.2
```

159817 - Windows Credential Guard Status

Synopsis

Retrieves the status of Windows Credential Guard.

Description

Retrieves the status of Windows Credential Guard.

Credential Guard prevents attacks such as such as Pass-the-Hash or Pass-The-Ticket by protecting NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials.

See Also

http://www.nessus.org/u?fb8c8c37

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/04/18, Modified: 2023/08/25

Plugin Output

tcp/445/cifs

```
Windows Credential Guard is not fully enabled.
The following registry keys have not been set :
  - System\CurrentControlSet\Control\DeviceGuard\RequirePlatformSecurityFeatures : Key not found.
  - System\CurrentControlSet\Control\LSA\LsaCfgFlags : Key not found.
  - System\CurrentControlSet\Control\DeviceGuard\EnableVirtualizationBasedSecurity : Key not found.
```

58181 - Windows DNS Server Enumeration

Synopsis

Nessus enumerated the DNS servers being used by the remote Windows host.

Description

Nessus was able to enumerate the DNS servers configured on the remote Windows host by looking in the registry.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/03/01, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Nessus enumerated DNS servers for the following interfaces :

Interface: {2a65c772-29c7-4aad-8c3f-1e016b1998c4}
Network Connection : Ethernet
DhcpNameServer: 192.168.230.152

Interface: Default
DhcpNameServer: 192.168.230.152
```

131023 - Windows Defender Installed

Synopsis

Windows Defender is installed on the remote Windows host.

Description

Windows Defender, an antivirus component of Microsoft Windows is installed on the remote Windows host.

See Also

https://www.microsoft.com/en-us/windows/comprehensive-security

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/11/15, Modified: 2025/03/18

Plugin Output

tcp/0

```
Path                          : C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25010.11-0\
Version                       : 4.18.25010.11
Engine Version                : 1.1.25020.1007
Malware Signature Timestamp : Mar. 25, 2025 at 11:19:30 GMT
Malware Signature Version   : 1.425.238.0
Signatures Last Updated     : Mar. 25, 2025 at 19:55:44 GMT
```

164690 - Windows Disabled Command Prompt Enumeration

Synopsis

This plugin determines if the DisableCMD policy is enabled or disabled on the remote host for each local user.

Description

The remote host may employ the DisableCMD policy on a per user basis. Enumerated local users may have the following registry key:

'HKLM\Software\Policies\Microsoft\Windows\System\DisableCMD'

- Unset or 0: The command prompt is enabled normally.

- 1: The command promt is disabled.

- 2: The command prompt is disabled however windows batch processing is allowed.

See Also

http://www.nessus.org/u?b40698bc

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/09/06, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

```
Username: kato
  SID: S-1-5-21-933753971-2826297321-2361855607-1000
  DisableCMD: Unset

Username: DefaultAccount
  SID: S-1-5-21-933753971-2826297321-2361855607-503
  DisableCMD: Unset

Username: Administrator
  SID: S-1-5-21-933753971-2826297321-2361855607-500
  DisableCMD: Unset

Username: WDAGUtilityAccount
  SID: S-1-5-21-933753971-2826297321-2361855607-504
```

```
    DisableCMD: Unset

  Username: Guest
    SID: S-1-5-21-933753971-2826297321-2361855607-501
    DisableCMD: Unset
```

72482 - Windows Display Driver Enumeration

Synopsis

Nessus was able to enumerate one or more of the display drivers on the remote host.

Description

Nessus was able to enumerate one or more of the display drivers on the remote host via WMI.

See Also

http://www.nessus.org/u?b6e87533

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0756

Plugin Information

Published: 2014/02/06, Modified: 2025/03/11

Plugin Output

tcp/0

```
Device Name         : VirtualBox Graphics Adapter (WDDM)
Driver File Version : 7.1.6.17084
Driver Date         : 01/21/2025
```

171956 - Windows Enumerate Accounts

Synopsis

Enumerate Windows accounts.

Description

Enumerate Windows accounts.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/28, Modified: 2025/03/11

Plugin Output

tcp/0

```
Windows accounts enumerated. Results output to DB.
User data gathered in scan starting at : 2025/3/31 14:41 GMT Standard Time
```

159929 - Windows LSA Protection Status

Synopsis

Windows LSA Protection is disabled on the remote Windows host.

Description

The LSA Protection validates users for local and remote sign-ins and enforces local security policies to prevent reading memory and code injection by non-protected processes. This provides added security for the credentials that the LSA stores and manages. This protects against Pass-the-Hash or Mimikatz-style attacks.

Solution

Enable LSA Protection per your corporate security guidelines.

Risk Factor

None

Plugin Information

Published: 2022/04/20, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

148541 - Windows Language Settings Detection

Synopsis

This plugin enumerates language files on a windows host.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates language IDs listed on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/04/14, Modified: 2022/02/01

Plugin Output

tcp/0

```
Default Install Language Code: 2057

Default Active Language Code: 1033

Other common microsoft Language packs may be scanned as well.
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

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

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

udp/137/netbios-ns

```
The following 3 NetBIOS names have been gathered :

 WINDOWS11        = File Server Service
 WINDOWS11        = Computer name
 WORKGROUP        = Workgroup / Domain name

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

   08:00:27:11:82:d0
```

77668 - Windows Prefetch Folder

Synopsis

Nessus was able to retrieve the Windows prefetch folder file list.

Description

Nessus was able to retrieve and display the contents of the Windows prefetch folder (%systemroot% \prefetch*). This information shows programs that have run with the prefetch and superfetch mechanisms enabled.

See Also

http://www.nessus.org/u?8242d04f

http://www.nessus.org/u?d6b15983

http://www.forensicswiki.org/wiki/Prefetch

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2014/09/12, Modified: 2018/11/15

Plugin Output

tcp/0

```
+ HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
rootdirpath :
enableprefetcher : 3

+ Prefetch file list :
  - \WINDOWS\prefetch\AM_BASE.EXE-FE51F0AA.pf
  - \WINDOWS\prefetch\AM_DELTA.EXE-3A6EE7FD.pf
  - \WINDOWS\prefetch\AM_ENGINE.EXE-79E5B6A9.pf
  - \WINDOWS\prefetch\APPLICATIONFRAMEHOST.EXE-4CE44C83.pf
  - \WINDOWS\prefetch\AUDIODG.EXE-9848A323.pf
  - \WINDOWS\prefetch\BACKGROUNDTASKHOST.EXE-54485D81.pf
  - \WINDOWS\prefetch\BACKGROUNDTASKHOST.EXE-97CC50AB.pf
  - \WINDOWS\prefetch\BACKGROUNDTASKHOST.EXE-CA639011.pf
  - \WINDOWS\prefetch\BACKGROUNDTRANSFERHOST.EXE-2046E6BC.pf
  - \WINDOWS\prefetch\BACKGROUNDTRANSFERHOST.EXE-FD394D32.pf
  - \WINDOWS\prefetch\CMD.EXE-CD245F9E.pf
  - \WINDOWS\prefetch\COMPATTELRUNNER.EXE-93B5AB09.pf
  - \WINDOWS\prefetch\CONHOST.EXE-F98A1078.pf
  - \WINDOWS\prefetch\CONSENT.EXE-2D674CE4.pf
```

```
- \WINDOWS\prefetch\COOKIE_EXPORTER.EXE-CF199192.pf
- \WINDOWS\prefetch\CREDENTIALENROLLMENTMANAGER.E-419C97B0.pf
- \WINDOWS\prefetch\CTFMON.EXE-5E6E7DF5.pf
- \WINDOWS\prefetch\DEFRAG.EXE-22AD8A37.pf
- \WINDOWS\prefetch\DIRECTXDATABASEUPDATER.EXE-B419FBAB.pf
- \WINDOWS\prefetch\DISMHOST.EXE-71696596.pf
- \WINDOWS\prefetch\DLLHOST.EXE-08D3C038.pf
- \WINDOWS\prefetch\DLLHOST.EXE-1B91EF29.pf
- \WINDOWS\prefetch\DLLHOST.EXE-34E3C159.pf
- \WINDOWS\prefetch\DLLHOST.EXE-5C8817D4.pf
- \WINDOWS\prefetch\DLLHOST.EXE-6153BB8F.pf
- \WINDOWS\prefetch\DLLHOST.EXE-6A829A47.pf
- \WINDOWS\prefetch\DLLHOST.EXE-891DC51D.pf
- \WINDOWS\prefetch\DLLHOST.EXE-B51A0D95.pf
- \WINDOWS\prefetch\DLLHOST.EXE-D7A86B5E.pf
- \WINDOWS\prefetch\DLLHOST.EXE-E4082A4F.pf
- \WINDOWS\prefetch\DLLHOST.EXE-E5221F10.pf
- \WINDOWS\prefetch\DLLHOST.EXE-F8F2B7B0.pf
- \WINDOWS\prefetch\DRVINST.EXE-26FFA444.pf
- \WINDOWS\prefetch\EXPLORER.EXE-03C49D11.pf
- \WINDOWS\prefetch\FILECOAUTH.EXE-0D492C8A.pf
- \WINDOWS\prefetch\FILECOAUTH.EXE-75070FC4.pf
- \WINDOWS\prefetch\FILECOAUTH.EXE-E3855B72.pf
- \WINDOWS\prefetch\FILESYNCCONFIG.EXE-1E4B2975.pf
- \WIN [...]
```

155963 - Windows Printer Driver Enumeration

Synopsis

Nessus was able to enumerate one or more of the printer drivers on the remote host.

Description

Nessus was able to enumerate one or more of the printer drivers on the remote host via WMI.

See Also

http://www.nessus.org/u?fab99415

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/12/09, Modified: 2025/03/11

Plugin Output

tcp/445/cifs

```
--- Microsoft Virtual Print Class Driver ---

  Path               : C:\WINDOWS\System32\DriverStore\FileRepository
\ntprint4.inf_amd64_c49de045256fee63\Amd64\msdwdrv.dll
  Version            : 10.0.26100.1591
  Supported Platform : Windows x64

--- Microsoft enhanced Point and Print compatibility driver ---

Nessus detected 2 installs of Microsoft enhanced Point and Print compatibility driver:

  Path               : C:\WINDOWS\system32\spool\DRIVERS\x64\3\mxdwdrv.dll
  Version            : 10.0.26100.1742
  Supported Platform : Windows x64

  Path               : C:\WINDOWS\system32\spool\DRIVERS\W32X86\3\mxdwdrv.dll
  Version            : 10.0.26100.1742
  Supported Platform : Windows NT x86

--- Microsoft IPP Class Driver ---

  Path               : C:\WINDOWS\System32\DriverStore\FileRepository
\ntprint.inf_amd64_5083be912240d5a2\Amd64\mxdwdrv.dll
  Version            : 10.0.26100.1
```

```
   Supported Platform : Windows x64

--- Universal Print Class Driver ---

   Path               : C:\WINDOWS\System32\DriverStore\FileRepository
\ntprint.inf_amd64_5083be912240d5a2\Amd64\mxdwdrv.dll
   Version            : 10.0.26100.1
   Supported Platform : Windows x64
```

63620 - Windows Product Key Retrieval

Synopsis

This plugin retrieves the Windows Product key of the remote Windows host.

Description

Using the supplied credentials, Nessus was able to obtain the retrieve the Windows host's partial product key'.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/01/18, Modified: 2013/01/18

Plugin Output

tcp/445/cifs

```
  Product key : XXXXX-XXXXX-XXXXX-XXXXX-8HVX7

Note that all but the final portion of the key has been obfuscated.
```

160576 - Windows Services Registry ACL

Synopsis

Checks Windows Registry for Service ACLs

Description

Checks Windows Registry for Service ACLs.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2022/05/05, Modified: 2024/01/15

Plugin Output

tcp/445/cifs

```
Verbosity must be set to 'Report as much information as possible' for this plugin to produce output.
```

85736 - Windows Store Application Enumeration

Synopsis

It is possible to obtain the list of applications installed from the Windows Store.

Description

This plugin connects to the remote Windows host with the supplied credentials and uses WMI and Powershell to enumerate applications installed on the host from the Windows Store.

See Also

https://www.microsoft.com/en-us/store/apps

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/09/02, Modified: 2025/03/11

Plugin Output

tcp/0

```
  -1527c705-839a-4832-9118-54d4Bd6a0c89
      Version : 10.0.19640.1000
      InstallLocation : C:\Windows\SystemApps\Microsoft.Windows.FilePicker_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -c5e2524a-ea46-4f67-841f-6a9465d9d515
      Version : 10.0.26100.1
      InstallLocation : C:\Windows\SystemApps\Microsoft.Windows.FileExplorer_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -E2A4F912-2574-4A75-9BB0-0D023378592B
      Version : 10.0.19640.1000
      InstallLocation : C:\Windows\SystemApps\Microsoft.Windows.AppResolverUX_cw5n1h2txyewy
      Architecture : Neutral
      Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

  -F46D4000-FD22-4DB4-AC8E-4E1DDDE828FE
      Version : 10.0.26100.1
      InstallLocation : C:\Windows\SystemApps
\Microsoft.Windows.AddSuggestedFoldersToLibraryDialog_cw5n1h2txyewy
      Architecture : Neutral
```

```
    Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.AAD.BrokerPlugin
    Version : 1000.19580.1000.0
    InstallLocation : C:\Windows\SystemApps\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy
    Architecture : Neutral
    Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.AccountsControl
    Version : 10.0.26100.1
    InstallLocation : C:\Windows\SystemApps\Microsoft.AccountsControl_cw5n1h2txyewy
    Architecture : Neutral
    Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.AsyncTextService
    Version : 10.0.26100.1
    InstallLocation : C:\Windows\SystemApps\Microsoft.AsyncTextService_8wekyb3d8bbwe
    Architecture : Neutral
    Publisher : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US

-Microsoft.BioEnrollment
    Version : 10.0.19587.1000
 [...]
```

204960 - Windows System Driver Enumeration (Windows)

Synopsis

One or more kernel or file system drivers were enumerated on the remote Windows host.

Description

One or more kernel or file system drivers were enumerated on the remote Windows host.

See Also

http://www.nessus.org/u?43f8ab81

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/08/01, Modified: 2025/03/11

Plugin Output

tcp/0

```
Total : 383

  Name          : 1394ohci
  Path          : C:\WINDOWS\system32\drivers\1394ohci.sys
  Service Type  : Kernel Driver
  Description   : 1394 OHCI Compliant Host Controller
  State         : Stopped

  Name          : 3ware
  Path          : C:\WINDOWS\system32\drivers\3ware.sys
  Service Type  : Kernel Driver
  Description   : 3ware
  State         : Stopped

  Name          : ACPI
  Path          : C:\WINDOWS\system32\drivers\ACPI.sys
  Service Type  : Kernel Driver
  Description   : Microsoft ACPI Driver
  State         : Running

  Name          : AcpiDev
  Path          : C:\WINDOWS\system32\drivers\AcpiDev.sys
  Service Type  : Kernel Driver
  Description   : ACPI Devices driver
```

```
  State        : Stopped

  Name         : acpiex
  Path         : C:\WINDOWS\system32\Drivers\acpiex.sys
  Service Type : Kernel Driver
  Description  : Microsoft ACPIEx Driver
  State        : Running

  Name         : acpipagr
  Path         : C:\WINDOWS\system32\DriverStore\FileRepository\acpipagr.inf_amd64_d1093347a27ff89c
\acpipagr.sys
  Service Type : Kernel Driver
  Description  : ACPI Processor Aggregator Driver
  State        : Stopped

  Name         : AcpiPmi
  Path         : C:\WINDOWS\system32\DriverStore\FileRepository
\acpipmi.inf_amd64_3ced06eb61dcc792\acpipmi.sys
  Service Type : Kernel Driver
  Description  : ACPI Power Meter Driver
  State        : Stopped

  Name         : acpitime
  Path         : C:\WINDOWS\system32\drivers\acpitime.sys
  Service Type : Kernel Driver
  Description  : ACPI Wake Alarm Driver
  State        : Stopped

  Name         : Acx01000
  Path         : C:\WINDOWS\system32\drivers\Acx01000.sys
  Service Type : Kernel Driver
  Description  : Acx01000
  State        : Stopped

  Name         : ADP80XX
  Path         : C:\WINDOWS\system32\drivers\ADP80XX.SYS
  Service Type : Kernel Driver
  Description  : ADP80XX
  State        : Stopped

  Name         : AFD
  Path         : C:\WINDOWS\system32\drivers\afd.sys
  Service Type : Kernel Driver
  Description  : Ancillary Function Driver for Winsock
  Sta [...]
```