Windows 10 VM Scan

Report generated by Nessus™ Sun, 03 Mar 2024 01:12:18 GMT Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

DESKTOP-96HJG8C

CRITICAL	HIGH	MEDIUM	LOW	INFO
41	111	18	1	172

Host Information

Netbios Name:	DESKTOP-96HJG8C
IP:	192.168.128.129
MAC Address:	00:0C:29:B7:F1:32
OS:	Microsoft Windows 10 Pro Build 19045

Vulnerabilities

60042 - Firefox 10.0.x < 10.0.6 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The installed version of Firefox 10.0.x is potentially affected by the following security issues :

- Several memory safety issues exist, some of which could potentially allow arbitrary code execution. (CVE-2012-1948)

- An error related to drag and drop can allow incorrect URLs to be displayed. (CVE-2012-1950)

- Several memory safety issues exist related to the Gecko layout engine. (CVE-2012-1951, CVE-2012-1952, CVE-2012-1953, CVE-2012-1954)

- An error related to JavaScript functions 'history.forward' and 'history.back' can allow incorrect URLs to be displayed. (CVE-2012-1955)

- Cross-site scripting attacks are possible due to an error related to the '<embed>' tag within an RSS '<description>' element. (CVE-2012-1957)

- A use-after-free error exists related to the method 'nsGlobalWindow::PageHidden'. (CVE-2012-1958)

- An error exists that can allow 'same-compartment security wrappers' (SCSW) to be bypassed. (CVE-2012-1959)

- The 'X-Frames-Options' header is ignored if it is duplicated. (CVE-2012-1961)

- A memory corruption error exists related to the method 'JSDependentString::undepend'. (CVE-2012-1962)

- An error related to the 'Content Security Policy' (CSP) implementation can allow the disclosure of OAuth 2.0 access tokens and OpenID credentials. (CVE-2012-1963)

- An error exists related to the certificate warning page that can allow 'clickjacking' thereby tricking a user into accepting unintended certificates. (CVE-2012-1964)

- An error exists related to the 'feed:' URL that can allow cross-site scripting attacks. (CVE-2012-1965)

- Cross-site scripting attacks are possible due to an error related to the 'data:' URL and context menus. (CVE-2012-1966)

- An error exists related to the 'javascript:' URL that can allow scripts to run at elevated privileges outside the sandbox. (CVE-2012-1967)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2012-42/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-43/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-44/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-45/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-46/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-47/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-48/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-49/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-51/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-52/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-53/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-54/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-55/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-56/

Solution

Upgrade to Firefox 10.0.6 or later.

Risk Factor

Critical

VPR Score

5.9

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

BID	54573
BID	54574
BID	54575
BID	54576
BID	54577
BID	54578
BID	54579
BID	54581
BID	54582
BID	54583
BID	54584
BID	54585
BID	54586
CVE	CVE-2012-1948
CVE	CVE-2012-1950
CVE	CVE-2012-1951
CVE	CVE-2012-1952
CVE	CVE-2012-1953
CVE	CVE-2012-1954
CVE	CVE-2012-1955
CVE	CVE-2012-1957
CVE	CVE-2012-1958
CVE	CVE-2012-1959
CVE	CVE-2012-1961
CVE	CVE-2012-1962
CVE	CVE-2012-1963
CVE	CVE-2012-1964
CVE	CVE-2012-1965
CVE	CVE-2012-1966
CVE	CVE-2012-1967
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722

XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2012/07/19, Modified: 2019/12/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 10.0.6 ESR
```

61714 - Firefox 10.0.x < 10.0.7 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The installed version of Firefox 10.0.x is potentially affected by the following security issues :

- Unspecified memory safety issues exist. (CVE-2012-1970)

- Multiple use-after-free errors exist. (CVE-2012-1972, CVE-2012-1973, CVE-2012-1974, CVE-2012-1975, CVE-2012-1976, CVE-2012-3956, CVE-2012-3957, CVE-2012-3958, CVE-2012-3959, CVE-2012-3960, CVE-2012-3961, CVE-2012-3962, CVE-2012-3963, CVE-2012-3964)

- An error exists related to bitmap (BMP) and icon (ICO) file decoding that can lead to memory corruption, causing application crashes and potentially arbitrary code execution. (CVE-2012-3966)

- A use-after-free error exists related to WebGL shaders.

(CVE-2012-3968)

- A buffer overflow exists related to SVG filters.

(CVE-2012-3969)

- A use-after-free error exists related to elements having 'requiredFeatures' attributes. (CVE-2012-3970)

- An XSLT out-of-bounds read error exists related to 'format-number'. (CVE-2012-3972)

- The installer can be tricked into running unauthorized executables. (CVE-2012-3974)

- Incorrect SSL certificate information can be displayed in the address bar when two 'onLocationChange' events fire out of order. (CVE-2012-3976)

- Security checks related to location objects can be bypassed if crafted calls are made to the browser chrome code. (CVE-2012-3978)

- Calling 'eval' in the web console can allow injected code to be executed with browser chrome privileges.

(CVE-2012-3980)

See Also

http://www.securityfocus.com/archive/1/524145/30/0/threaded

https://www.mozilla.org/en-US/security/advisories/mfsa2012-57/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-58/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-61/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-62/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-63/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-65/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-67/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-69/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-70/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-72/

Solution

Upgrade to Firefox 10.0.7 or later.

Risk Factor

Critical

VPR Score

6.7

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

BID	55249
BID	55257
BID	55266
BID	55274
BID	55276
BID	55278
BID	55292
BID	55306
BID	55310
BID	55312
BID	55313
BID	55314
BID	55316
BID	55317
BID	55318
BID	55319
BID	55320
BID	55321
BID	55322
BID	55323

BID	55324
BID	55325
BID	55340
BID	55341
BID	55342
CVE	CVE-2012-1970
CVE	CVE-2012-1972
CVE	CVE-2012-1973
CVE	CVE-2012-1974
CVE	CVE-2012-1975
CVE	CVE-2012-1976
CVE	CVE-2012-3956
CVE	CVE-2012-3957
CVE	CVE-2012-3958
CVE	CVE-2012-3959
CVE	CVE-2012-3960
CVE	CVE-2012-3961
CVE	CVE-2012-3962
CVE	CVE-2012-3963
CVE	CVE-2012-3964
CVE	CVE-2012-3966
CVE	CVE-2012-3968
CVE	CVE-2012-3969
CVE	CVE-2012-3970
CVE	CVE-2012-3972
CVE	CVE-2012-3974
CVE	CVE-2012-3976
CVE	CVE-2012-3978
CVE	CVE-2012-3980

Plugin Information

Published: 2012/08/29, Modified: 2019/12/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 10.0.7 ESR
```

62579 - Firefox 10.0.x < 10.0.8 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The installed version of Firefox 10.0.x is affected by the following vulnerabilities :

- Several memory safety bugs exist in the browser engine used in Mozilla-based products that could be exploited to execute arbitrary code. (CVE-2012-3983)

- Some methods of a feature used for testing (DOMWindowUtils) are not properly protected and may be called through script by web pages. (CVE-2012-3986)

- A potentially exploitable denial of service may be caused by a combination of invoking full-screen mode and navigating backwards in history. (CVE-2012-3988)

- When the 'GetProperty' function is invoked through JSAP, security checking can by bypassed when getting cross- origin properties, potentially allowing arbitrary code execution. (CVE-2012-3991)

- The 'location' property can be accessed by binary plugins through 'top.location' and 'top' can be shadowed by 'Object.defineProperty', potentially allowing cross- site scripting attacks through plugins. (CVE-2012-3994)

- The Chrome Object Wrapper (COW) has flaws that could allow access to privileged functions, allowing for cross- site scripting attacks or arbitrary code execution. (CVE-2012-3993, CVE-2012-4184)

- The 'location.hash' property is vulnerable to an attack that could allow an attacker to inject script or intercept post data. (CVE-2012-3992)

- The 'Address Sanitizer' tool is affected by multiple, potentially exploitable use-after-free flaws. (CVE-2012-3990, CVE-2012-3995, CVE-2012-4179, CVE-2012-4180, CVE-2012-4181, CVE-2012-4182, CVE-2012-4183)

- The 'Address Sanitizer' tool is affected by multiple, potentially exploitable heap memory corruption issues. (CVE-2012-4185, CVE-2012-4186, CVE-2012-4187, CVE-2012-4188)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2012-87/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-86/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-85/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-84/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-83/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-82/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-81/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-79/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-77/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-74/

Solution

Upgrade to Firefox 10.0.8 or later.

Risk Factor

Critical

VPR Score

8.9

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)

References

BID	55922
BID	55924
BID	55930
BID	55931
BID	56118
BID	56119
BID	56120
BID	56121
BID	56123
BID	56125
BID	56126
BID	56127
BID	56128
BID	56129
BID	56130
BID	56131
BID	56135
BID	56136
BID	56140
BID	56145
CVE	CVE-2012-3982
CVE	CVE-2012-3983

CVE	CVE-2012-3986
CVE	CVE-2012-3988
CVE	CVE-2012-3990
CVE	CVE-2012-3991
CVE	CVE-2012-3992
CVE	CVE-2012-3993
CVE	CVE-2012-3994
CVE	CVE-2012-3995
CVE	CVE-2012-4179
CVE	CVE-2012-4180
CVE	CVE-2012-4181
CVE	CVE-2012-4182
CVE	CVE-2012-4183
CVE	CVE-2012-4184
CVE	CVE-2012-4185
CVE	CVE-2012-4186
CVE	CVE-2012-4187
CVE	CVE-2012-4188
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Exploitable With

Metasploit (true)

Plugin Information

Published: 2012/10/17, Modified: 2019/12/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 10.0.8 ESR
```

62997 - Firefox 10.x < 10.0.11 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The installed version of Firefox 10.x is potentially affected by the following security issues :

- Several memory safety bugs exist in the browser engine used in Mozilla-based products that could be exploited to execute arbitrary code. (CVE-2012-5843)

- An error exists in the method 'image::RasterImage::DrawFrameTo' related to GIF images that could allow a heap-based buffer overflow, leading to arbitrary code execution. (CVE-2012-4202)

- An error exists related to the application installer and DLL loading. (CVE-2012-4206)

- Errors exist related to 'evalInSandbox', 'HZ-GB-2312'

charset, frames and the 'location' object, the 'Style Inspector', and 'cross-origin wrappers' that could allow cross-site scripting (XSS) attacks. (CVE-2012-4201, CVE-2012-4207, CVE-2012-4209, CVE-2012-4210, CVE-2012-5841)

- Various use-after-free, out-of-bounds read and buffer overflow errors exist that could potentially lead to arbitrary code execution. (CVE-2012-4214, CVE-2012-4215, CVE-2012-4216, CVE-2012-5829, CVE-2012-5830, CVE-2012-5833, CVE-2012-5835, CVE-2012-5839, CVE-2012-5840)

Please note the 10.x ESR branch will be unsupported as of 02/13/2013.

Only the 17.x ESR branch will receive security updates after that date.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2012-91/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-92/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-93/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-100/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-101/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-103/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-104/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-105/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-106/

Solution

Upgrade to Firefox 10.0.11 ESR or later.

Risk Factor

Critical

VPR Score

6.7

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

BID	56612
BID	56614
BID	56618
BID	56625
BID	56628
BID	56629
BID	56631
BID	56632
BID	56633
BID	56634
BID	56635
BID	56636
BID	56637
BID	56641
BID	56642
BID	56643
BID	56646
CVE	CVE-2012-4201
CVE	CVE-2012-4202
CVE	CVE-2012-4206
CVE	CVE-2012-4207
CVE	CVE-2012-4209
CVE	CVE-2012-4210
CVE	CVE-2012-4214
CVE	CVE-2012-4215
CVE	CVE-2012-4216
CVE	CVE-2012-5829

CVE	CVE-2012-5830
CVE	CVE-2012-5833
CVE	CVE-2012-5835
CVE	CVE-2012-5839
CVE	CVE-2012-5840
CVE	CVE-2012-5841
CVE	CVE-2012-5843
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2012/11/21, Modified: 2019/12/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 10.0.11 ESR
```

63548 - Firefox 10.x < 10.0.12 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The installed version of Firefox 10.x is potentially affected by the following security issues :

- Multiple, unspecified use-after-free, out-of-bounds read and buffer overflow errors exist. (CVE-2013-0761, CVE-2013-0762, CVE-2013-0763, CVE-2013-0766, CVE-2013-0767, CVE-2013-0771)

- Two intermediate certificates were improperly issued by TURKTRUST certificate authority. (CVE-2013-0743)

- A use-after-free error exists related to displaying HTML tables with many columns and column groups.
(CVE-2013-0744)

- An error exists related to the 'AutoWrapperChanger'
class that does not properly manage objects during garbage collection. (CVE-2012-0745)

- An error exists related to 'jsval', 'quickstubs', and compartmental mismatches that could lead to potentially exploitable crashes. (CVE-2013-0746)

- Errors exist related to events in the plugin handler that could allow same-origin policy bypass.
(CVE-2013-0747)

- An error related to the 'toString' method of XBL objects could lead to address information leakage.
(CVE-2013-0748)

- An unspecified memory corruption issue exists.
(CVE-2013-0749, CVE-2013-0769)

- A buffer overflow exists related to JavaScript string concatenation. (CVE-2013-0750)

- An error exists related to multiple XML bindings with SVG content, contained in XBL files. (CVE-2013-0752)

- A use-after-free error exists related to 'XMLSerializer' and 'serializeToStream'.
(CVE-2013-0753)

- A use-after-free error exists related to garbage collection and 'ListenManager'. (CVE-2013-0754)

- A use-after-free error exists related to the 'Vibrate'
library and 'domDoc'. (CVE-2013-0755)

- A use-after-free error exists related to JavaScript 'Proxy' objects. (CVE-2013-0756)

- 'Chrome Object Wrappers' (COW) can be bypassed by changing object prototypes, which could allow arbitrary code execution. (CVE-2013-0757)

- An error related to SVG elements and plugins could allow privilege escalation. (CVE-2013-0758)

- An error exists related to the address bar that could allow URL spoofing attacks. (CVE-2013-0759)

- An error exists related to SSL and threading that could result in potentially exploitable crashes.

(CVE-2013-0764)

- An error exists related to 'Canvas' and bad height or width values passed to it from HTML.
(CVE-2013-0768)

Please note the 10.x ESR branch will no longer be supported as of 02/13/2013. Only the 17.x ESR branch will receive security updates after that date.

See Also

http://www.zerodayinitiative.com/advisories/ZDI-13-003/

http://www.zerodayinitiative.com/advisories/ZDI-13-006/

http://www.zerodayinitiative.com/advisories/ZDI-13-037/

http://www.zerodayinitiative.com/advisories/ZDI-13-038/

http://www.zerodayinitiative.com/advisories/ZDI-13-039/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-01/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-02/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-03/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-04/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-05/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-07/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-08/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-09/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-10/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-11/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-12/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-13/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-14/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-15/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-16/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-17/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-18/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-19/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-20/

Solution

Upgrade to Firefox 10.0.12 ESR or later.

Risk Factor

Critical

VPR Score

9.5

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)

References

BID	57193
BID	57194
BID	57195
BID	57196
BID	57197
BID	57198
BID	57203
BID	57204
BID	57205
BID	57209
BID	57211
BID	57213
BID	57215
BID	57217
BID	57218
BID	57228
BID	57232
BID	57234
BID	57235
BID	57236
BID	57238
BID	57240
BID	57241
BID	57244
BID	57258
CVE	CVE-2013-0744
CVE	CVE-2013-0745
CVE	CVE-2013-0746
CVE	CVE-2013-0747
CVE	CVE-2013-0748
CVE	CVE-2013-0749

CVE	CVE-2013-0750
CVE	CVE-2013-0752
CVE	CVE-2013-0753
CVE	CVE-2013-0754
CVE	CVE-2013-0755
CVE	CVE-2013-0756
CVE	CVE-2013-0757
CVE	CVE-2013-0758
CVE	CVE-2013-0759
CVE	CVE-2013-0761
CVE	CVE-2013-0762
CVE	CVE-2013-0763
CVE	CVE-2013-0764
CVE	CVE-2013-0766
CVE	CVE-2013-0767
CVE	CVE-2013-0768
CVE	CVE-2013-0769
CVE	CVE-2013-0771
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2013/01/15, Modified: 2019/12/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 10.0.12 ESR
```

70714 - Firefox ESR < 17.0.10 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is potentially affected by multiple vulnerabilities.

Description

The installed version of Firefox ESR is earlier than 17.0.10, and is, therefore, potentially affected by the following vulnerabilities :

- The implementation of Network Security Services (NSS) does not ensure that data structures are initialized, which could result in a denial of service or disclosure of sensitive information. (2013-1739)

- Memory issues exist in the browser engine that could result in a denial of service or arbitrary code execution. (CVE-2013-5590, CVE-2013-5591, CVE-2013-5592)

- Memory issues exist in the JavaScript engine that could result in a denial of service or arbitrary code execution. (CVE-2013-5595, CVE-2013-5602)

- Multiple use-after-free vulnerabilities exist that could result in a denial of service or arbitrary code execution. (CVE-2013-5597, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601)

- A stack-based buffer overflow in txXPathNodeUtils::getBaseURI is possible due to uninitialized data during XSLT processing.

(CVE-2013-5604)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2013-93/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-95/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-96/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-98/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-100/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-101/

Solution

Upgrade to Firefox ESR 17.0.10 or later.

Risk Factor

Critical

VPR Score

5.9

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

BID	62966
BID	63405
BID	63415
BID	63417
BID	63418
BID	63421
BID	63422
BID	63423
BID	63424
BID	63427
BID	63428
BID	63430
CVE	CVE-2013-1739
CVE	CVE-2013-5590
CVE	CVE-2013-5591
CVE	CVE-2013-5592
CVE	CVE-2013-5595
CVE	CVE-2013-5597
CVE	CVE-2013-5599
CVE	CVE-2013-5600
CVE	CVE-2013-5601
CVE	CVE-2013-5602
CVE	CVE-2013-5604

Plugin Information

Published: 2013/10/31, Modified: 2019/11/27

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 17.0.10 ESR
```

85385 - Firefox ESR < 38.2 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The version of Firefox ESR installed on the remote Windows host is prior to 38.2. It is, therefore, affected by the following vulnerabilities :

- Multiple memory corruption issues exist that allow a remote attacker, via a specially crafted web page, to corrupt memory and potentially execute arbitrary code.

(CVE-2015-4473)

- An out-of-bounds read error exists in the PlayFromAudioQueue() function due to improper handling of mismatched sample formats. A remote attacker can exploit this, via a specially crafted MP3 file, to disclose memory contents or execute arbitrary code.

(CVE-2015-4475)

- A same-origin policy bypass vulnerability exists due to non-configurable properties being redefined in violation of the ECMAScript 6 standard during JSON parsing. A remote attacker can exploit this, by editing these properties to arbitrary values, to bypass the same-origin policy. (CVE-2015-4478)

- Multiple integer overflow conditions exist due to improper validation of user-supplied input when handling 'saio' chunks in MPEG4 video. A remote attacker can exploit this, via a specially crafted MPEG4 file, to execute arbitrary code. (CVE-2015-4479)

- An integer overflow condition exists in the bundled libstagefright component when handling H.264 media content. A remote attacker can exploit this, via a specially crafted MPEG4 file, to execute arbitrary code.

(CVE-2015-4480)

- An arbitrary file overwrite vulnerability exists in the Mozilla Maintenance Service due to a race condition. An attacker can exploit this, via the use of a hard link, to overwrite arbitrary files with log output.

(CVE-2015-4481)

- An out-of-bounds write error exists due to an array indexing flaw in the mar_consume_index() function when handling index names in MAR files. An attacker can exploit this to execute arbitrary code. (CVE-2015-4482)

- A denial of service vulnerability exists when handling JavaScript using shared memory without properly gating access to Atomics and SharedArrayBuffer views. An attacker can exploit this to crash the program, resulting in a denial of service condition.

(CVE-2015-4484)

- A heap-based buffer overflow condition exists in the resize_context_buffers() function due to improper validation of user-supplied input. A remote attacker can exploit this, via specially crafted WebM content, to cause a heap-based buffer overflow, resulting in the execution of arbitrary code. (CVE-2015-4485)

- A heap-based buffer overflow condition exists in the decrease_ref_count() function due to improper validation of user-supplied input. A remote attacker can exploit this, via specially crafted WebM content, to cause a heap-based buffer overflow, resulting in the execution of arbitrary code. (CVE-2015-4486)

- A buffer overflow condition exists in the ReplacePrep() function. A remote attacker can exploit this to cause a buffer overflow, resulting in the execution of arbitrary code. (CVE-2015-4487)

- A use-after-free error exists in the operator=() function. An attacker can exploit this to dereference already freed memory, resulting in the execution of arbitrary code. (CVE-2015-4488)

- A memory corruption issue exists in the nsTArray_Impl() function due to improper validation of user-supplied input during self-assignment. An attacker can exploit this to corrupt memory, resulting in the execution of arbitrary code. (CVE-2015-4489)

- A use-after-free error exists in the XMLHttpRequest::Open() function due to improper handling of recursive calls. An attacker can exploit this to dereference already freed memory, resulting in the execution of arbitrary code. (CVE-2015-4492)

- An integer underflow condition exists in the bundled libstagefright library. An attacker can exploit this to crash the application, resulting in a denial of service condition. (CVE-2015-4493)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-79/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-80/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-82/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-83/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-84/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-85/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-87/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-89/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-90/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-92/

Solution

Upgrade to Firefox ESR 38.2 or later.

Risk Factor

Critical

VPR Score

5.9

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

BID	76294
BID	76297
CVE	CVE-2015-4473
CVE	CVE-2015-4475
CVE	CVE-2015-4478
CVE	CVE-2015-4479
CVE	CVE-2015-4480
CVE	CVE-2015-4481
CVE	CVE-2015-4482
CVE	CVE-2015-4484
CVE	CVE-2015-4485
CVE	CVE-2015-4486
CVE	CVE-2015-4487
CVE	CVE-2015-4488
CVE	CVE-2015-4489
CVE	CVE-2015-4492
CVE	CVE-2015-4493

Plugin Information

Published: 2015/08/13, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 38.2 ESR
```

85688 - Firefox ESR < 38.2.1 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The version of Mozilla Firefox ESR installed on the remote Windows host is prior to 38.2.1. It is, therefore, affected by the following vulnerabilities :

- A use-after-free error exists when handling restyling operations during the resizing of canvas elements due to the canvas references being recreated, thus destroying the original references. A remote, unauthenticated attacker can exploit this to deference already freed memory, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2015-4497)

- A security feature bypass vulnerability exists due to a flaw that allows the manipulation of the 'data:' URL on a loaded web page without install permission prompts being displayed to the user. A remote, unauthenticated attacker can exploit this to install add-ons from a malicious source. (CVE-2015-4498)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-94/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-95/

Solution

Upgrade to Firefox ESR 38.2.1 or later.

Risk Factor

Critical

VPR Score

5.9

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-2015-4497
CVE	CVE-2015-4498

Plugin Information

Published: 2015/08/28, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 38.2.1 ESR
```

87475 - Firefox ESR < 38.5 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The version of Firefox ESR installed on the remote Windows host is prior to 38.5. It is, therefore, affected by the following vulnerabilities :

- Multiple unspecified memory corruption issues exist due to improper validation of user-supplied input. A remote attacker can exploit these issues by convincing a user to visit a specially crafted web page, resulting in the execution of arbitrary code. (CVE-2015-7201)

- A flaw exists in the RtpHeaderParser::Parse() function due to improper handling of RTP headers. An unauthenticated, remote attacker can exploit this, via specially crafted RTP headers, to execute arbitrary code. (CVE-2015-7205)

- A use-after-free error exists due to improper prevention of datachannel operations on closed PeerConnections. An attacker can exploit this to dereference already freed memory, resulting in the execution of arbitrary code.

(CVE-2015-7210)

- An overflow condition exists in the AllocateForSurface() function due to improper validation of user-supplied input when handling texture allocation in graphics operations. An attacker can exploit this to execute arbitrary code. (CVE-2015-7212)

- An integer overflow condition exists in the readMetaData() function due to improper validation of user-supplied input when handling a specially crafted MP4 file. An attacker can exploit this to execute arbitrary code. (CVE-2015-7213)

- A same-origin bypass vulnerability exists due to improper handling of 'data:' and 'view-source:' URIs. An attacker can exploit this to read data from cross-site URLs and local files. (CVE-2015-7214)

- An integer underflow condition exists in the bundled version of libstagefright in the parseChunk() function that is triggered when handling 'covr' chunks. An unauthenticated, remote attacker can exploit this, via specially crafted media content, to crash the application or execute arbitrary code. (CVE-2015-7222)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-138/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-139/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-145/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-146/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-147/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-149/

Solution

Upgrade to Firefox ESR 38.5 or later.

Risk Factor

Critical

VPR Score

5.9

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

BID	79279
BID	79283
CVE	CVE-2015-7201
CVE	CVE-2015-7205
CVE	CVE-2015-7210
CVE	CVE-2015-7212
CVE	CVE-2015-7213
CVE	CVE-2015-7214
CVE	CVE-2015-7222

Plugin Information

Published: 2015/12/17, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 38.5 ESR
```

88460 - Firefox ESR < 38.6 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The version of Firefox ESR installed on the remote Windows host is prior to 38.6. It is, therefore, affected by the following vulnerabilities :

- Multiple unspecified memory corruption issues exist that allow a remote attacker to execute arbitrary code.

(CVE-2016-1930)

- A buffer overflow condition exists in WebGL that is triggered when handling cache out-of-memory error conditions. A remote attacker can exploit this to execute arbitrary code. (CVE-2016-1935)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2016-01/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-03/

Solution

Upgrade to Firefox ESR version 38.6 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.9

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-2016-1930
CVE	CVE-2016-1935
XREF	MFSA:2016-01
XREF	MFSA:2016-03

Plugin Information

Published: 2016/01/28, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 38.6 ESR
```

89874 - Firefox ESR < 38.7 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The version of Mozilla Firefox ESR installed on the remote Windows host is prior to 38.7. It is, therefore, affected by multiple vulnerabilities, the majority of which are remote code execution vulnerabilities. An unauthenticated, remote attacker can exploit these issues by convincing a user to visit a specially crafted website, resulting in the execution of arbitrary code in the context of the current user.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2016-16/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-17/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-20/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-21/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-23/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-24/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-25/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-27/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-28/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-31/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-34/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-35/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-37/

Solution

Upgrade to Mozilla Firefox ESR version 38.7 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.0

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)

References

CVE	CVE-2016-1950
CVE	CVE-2016-1952
CVE	CVE-2016-1954
CVE	CVE-2016-1957
CVE	CVE-2016-1958
CVE	CVE-2016-1960
CVE	CVE-2016-1961
CVE	CVE-2016-1962
CVE	CVE-2016-1964
CVE	CVE-2016-1965
CVE	CVE-2016-1966
CVE	CVE-2016-1974
CVE	CVE-2016-1977
CVE	CVE-2016-2790
CVE	CVE-2016-2791
CVE	CVE-2016-2792
CVE	CVE-2016-2793
CVE	CVE-2016-2794
CVE	CVE-2016-2795
CVE	CVE-2016-2796
CVE	CVE-2016-2797
CVE	CVE-2016-2798
CVE	CVE-2016-2799
CVE	CVE-2016-2800
CVE	CVE-2016-2801
CVE	CVE-2016-2802
XREF	MFSA:2016-16
XREF	MFSA:2016-17
XREF	MFSA:2016-20
XREF	MFSA:2016-21
XREF	MFSA:2016-23

XREF MFSA:2016-24
XREF MFSA:2016-25
XREF MFSA:2016-27
XREF MFSA:2016-28
XREF MFSA:2016-31
XREF MFSA:2016-34
XREF MFSA:2016-35
XREF MFSA:2016-37

Plugin Information

Published: 2016/03/11, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 38.7 ESR
```

178436 - Microsoft 365 (Office) App Code Execution (December 2021)

Synopsis

The Windows app installed on the remote host is affected by a code execution vulnerability.

Description

The Windows 'Microsoft 365 (Office)' app installed on the remote host is affected by a code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

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-2021-43905

Solution

Upgrade to app version 18.2110.13110.0, or later via the Microsoft Store.

Risk Factor

Medium

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

8.1

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-2021-43905
XREF	IAVA:2021-A-0584-S

Plugin Information

Published: 2023/07/18, Modified: 2023/07/19

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.MicrosoftOfficeHub_18.1903.1152.0_x64__8wekyb3d8bbwe
  Installed version : 18.1903.1152.0
  Fixed version     : 18.2110.13110.0
```

159816 - Microsoft Edge (Chromium) < 100.0.1185.44 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 100.0.1185.44. It is, therefore, affected by multiple vulnerabilities as referenced in the April 15, 2022 advisory.

- Use after free in tab groups in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1313)

- Use after free in storage in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1305)

- Inappropriate implementation in compositing in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (CVE-2022-1306)

- Inappropriate implementation in full screen in Google Chrome on Android prior to 100.0.4896.88 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (CVE-2022-1307)

- Use after free in BFCache in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1308)

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?84a20f12

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1305

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1306

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1307

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1308

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1309

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1310

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1312

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1313

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1314

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1364

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29144

Solution

Upgrade to Microsoft Edge version 100.0.1185.44 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

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-2022-1305
CVE	CVE-2022-1306
CVE	CVE-2022-1307
CVE	CVE-2022-1308
CVE	CVE-2022-1309
CVE	CVE-2022-1310
CVE	CVE-2022-1312
CVE	CVE-2022-1313
CVE	CVE-2022-1314
CVE	CVE-2022-1364
CVE	CVE-2022-29144
XREF	CISA-KNOWN-EXPLOITED:2022/05/06
XREF	IAVA:2022-A-0156-S

Plugin Information

Published: 2022/04/18, Modified: 2023/11/01

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 100.0.1185.44
```

161717 - Microsoft Edge (Chromium) < 102.0.1245.30 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 102.0.1245.30. It is, therefore, affected by multiple vulnerabilities as referenced in the May 31, 2022 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30127. (CVE-2022-30128)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30128. (CVE-2022-30127)

- Use after free in Indexed DB in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (CVE-2022-1853)

- Use after free in ANGLE in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1854)

- Use after free in Messaging in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1855)

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?ae294315

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1853

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1854

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1855

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1856

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1857

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1858

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1859

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1862

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1863

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1864

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1865

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1867

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1868

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1869

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1870

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1871
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1872
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1873
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1874
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1875
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1876
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26905
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30127
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30128

Solution

Upgrade to Microsoft Edge version 102.0.1245.30 or later.

Risk Factor

Medium

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-1853
CVE	CVE-2022-1854
CVE	CVE-2022-1855
CVE	CVE-2022-1856
CVE	CVE-2022-1857
CVE	CVE-2022-1858

CVE	CVE-2022-1859
CVE	CVE-2022-1862
CVE	CVE-2022-1863
CVE	CVE-2022-1864
CVE	CVE-2022-1865
CVE	CVE-2022-1867
CVE	CVE-2022-1868
CVE	CVE-2022-1869
CVE	CVE-2022-1870
CVE	CVE-2022-1871
CVE	CVE-2022-1872
CVE	CVE-2022-1873
CVE	CVE-2022-1874
CVE	CVE-2022-1875
CVE	CVE-2022-1876
CVE	CVE-2022-26905
CVE	CVE-2022-30127
CVE	CVE-2022-30128

Plugin Information

Published: 2022/05/31, Modified: 2023/10/26

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 102.0.1245.30
```

162168 - Microsoft Edge (Chromium) < 102.0.1245.41 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 102.0.1245.41. It is, therefore, affected by multiple vulnerabilities as referenced in the June 13, 2022 advisory.

- Use after free in ANGLE in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-2011)

- Use after free in WebGPU in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-2007)

- Double free in WebGL in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-2008)

- Out of bounds read in compositing in Google Chrome prior to 102.0.5005.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

(CVE-2022-2010)

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?c00d2c8a

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2007

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2008

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2010

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2011

Solution

Upgrade to Microsoft Edge version 102.0.1245.41 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.1

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-2022-2007
CVE	CVE-2022-2008
CVE	CVE-2022-2010
CVE	CVE-2022-2011
XREF	IAVA:2022-A-0231-S

Plugin Information

Published: 2022/06/13, Modified: 2023/03/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 102.0.1245.41
```

163893 - Microsoft Edge (Chromium) < 104.0.1293.47 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 104.0.1293.47. It is, therefore, affected by multiple vulnerabilities as referenced in the August 5, 2022 advisory.

- Use after free in Omnibox. (CVE-2022-2603)

- Use after free in Safe Browsing. (CVE-2022-2604)

- Out of bounds read in Dawn. (CVE-2022-2605)

- Use after free in Managed devices API. (CVE-2022-2606)

- Insufficient policy enforcement in Background Fetch. (CVE-2022-2610)

- Inappropriate implementation in Fullscreen API. (CVE-2022-2611)

- Side-channel information leakage in Keyboard input. (CVE-2022-2612)

- Use after free in Sign-In Flow. (CVE-2022-2614)

- Insufficient policy enforcement in Cookies. (CVE-2022-2615)

- Inappropriate implementation in Extensions API. (CVE-2022-2616)

- Use after free in Extensions API. (CVE-2022-2617)

- Insufficient validation of untrusted input in Internals. (CVE-2022-2618)

- Insufficient validation of untrusted input in Settings. (CVE-2022-2619)

- Use after free in Extensions. (CVE-2022-2621)

- Insufficient validation of untrusted input in Safe Browsing. (CVE-2022-2622)

- Use after free in Offline. (CVE-2022-2623)

- Heap buffer overflow in PDF. (CVE-2022-2624)

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?d822b1dc

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2603

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2604

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2605

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2606
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2610
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2611
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2612
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2614
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2615
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2616
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2617
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2618
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2619
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2621
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2622
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2623
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2624
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-33636
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-33649
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35796

Solution

Upgrade to Microsoft Edge version 104.0.1293.47 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

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-2022-2603
CVE	CVE-2022-2604
CVE	CVE-2022-2605
CVE	CVE-2022-2606
CVE	CVE-2022-2610
CVE	CVE-2022-2611
CVE	CVE-2022-2612
CVE	CVE-2022-2614
CVE	CVE-2022-2615
CVE	CVE-2022-2616
CVE	CVE-2022-2617
CVE	CVE-2022-2618
CVE	CVE-2022-2619
CVE	CVE-2022-2621
CVE	CVE-2022-2622
CVE	CVE-2022-2623
CVE	CVE-2022-2624
CVE	CVE-2022-33636
CVE	CVE-2022-33649
CVE	CVE-2022-35796

Plugin Information

Published: 2022/08/06, Modified: 2024/02/05

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 104.0.1293.47
```

164658 - Microsoft Edge (Chromium) < 105.0.1343.27 Vulnerability

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 105.0.1343.27. It is, therefore, affected by a vulnerability as referenced in the September 2, 2022 advisory.

- Insufficient data validation in Mojo. (CVE-2022-3075)

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?7aa022b9

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3075

Solution

Upgrade to Microsoft Edge version 105.0.1343.27 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

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

VPR Score

8.1

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-2022-3075
XREF	CISA-KNOWN-EXPLOITED:2022/09/29
XREF	IAVA:2022-A-0351-S
XREF	IAVA:2022-A-0361-S

Plugin Information

Published: 2022/09/02, Modified: 2023/10/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 105.0.1343.27
```

167274 - Microsoft Edge (Chromium) < 107.0.1418.42 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 107.0.1418.42. It is, therefore, affected by multiple vulnerabilities as referenced in the November 10, 2022 advisory.

- Use after free in V8 in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-3885)

- Use after free in Speech Recognition in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-3886)

- Use after free in Web Workers in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-3887)

- Use after free in WebCodecs in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-3888)

- Type confusion in V8 in Google Chrome prior to 107.0.5304.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-3889)

- Heap buffer overflow in Crashpad in Google Chrome on Android prior to 107.0.5304.106 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-2022-3890)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3885

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3886

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3887

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3888

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3889

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3890

Solution

Upgrade to Microsoft Edge version 107.0.1418.42 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

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

VPR Score

9.2

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-2022-3885
CVE	CVE-2022-3886
CVE	CVE-2022-3887
CVE	CVE-2022-3888
CVE	CVE-2022-3889
CVE	CVE-2022-3890
XREF	IAVA:2022-A-0493-S

Plugin Information

Published: 2022/11/10, Modified: 2023/10/25

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Microsoft\Edge\Application
  Installed version : 92.0.902.67
```

```
    Fixed version     : 107.0.1418.42
```

168239 - Microsoft Edge (Chromium) < 107.0.1418.62 Vulnerability

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 107.0.1418.62. It is, therefore, affected by a vulnerability as referenced in the November 28, 2022 advisory.

- Heap buffer overflow in GPU in Google Chrome prior to 107.0.5304.121 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-2022-4135)

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?2fa4911e

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4135

Solution

Upgrade to Microsoft Edge version 107.0.1418.62 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

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

VPR Score

8.1

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-2022-4135
XREF	CISA-KNOWN-EXPLOITED:2022/12/19
XREF	IAVA:2022-A-0501-S
XREF	IAVA:2022-A-0502-S

Plugin Information

Published: 2022/11/29, Modified: 2023/09/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 107.0.1418.62
```

173711 - Microsoft Edge (Chromium) < 111.0.1661.54 / 110.0.1587.78 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 111.0.1661.54 / 110.0.1587.78. It is, therefore, affected by multiple vulnerabilities as referenced in the March 24, 2023 advisory.

- Use after free in Passwords in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1528)

- Out of bounds memory access in WebHID in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a malicious HID device. (Chromium security severity: High) (CVE-2023-1529)

- Use after free in PDF in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1530)

- Use after free in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1531)

- Out of bounds read in GPU Video in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1532)

- Use after free in WebProtect in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1533)

- Out of bounds read in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1534)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1528

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1529

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1530

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1531

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1532

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1533

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1534
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28261
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28286

Solution

Upgrade to Microsoft Edge version 111.0.1661.54 / 110.0.1587.78 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-1528
CVE	CVE-2023-1529
CVE	CVE-2023-1530
CVE	CVE-2023-1531
CVE	CVE-2023-1532
CVE	CVE-2023-1533
CVE	CVE-2023-1534
CVE	CVE-2023-28261
CVE	CVE-2023-28286

XREF IAVA:2023-A-0161-S

Plugin Information

Published: 2023/03/30, Modified: 2023/05/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 111.0.1661.54
```

181483 - Microsoft Edge (Chromium) < 117.0.2045.31 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 117.0.2045.31. It is, therefore, affected by multiple vulnerabilities as referenced in the September 15, 2023 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability (CVE-2023-36562, CVE-2023-36735)

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2023-36727)

- Heap buffer overflow in WebP in Google Chrome prior to 116.0.5845.187 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical) (CVE-2023-4863)

- Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 117.0.5938.62 allowed a remote attacker to obfuscate a permission prompt via a crafted HTML page. (Chromium security severity:

Medium) (CVE-2023-4900)

- Inappropriate implementation in Prompts in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to potentially spoof security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4901)

- Inappropriate implementation in Input in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4902)

- Inappropriate implementation in Custom Mobile Tabs in Google Chrome on Android prior to 117.0.5938.62 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity:

Medium) (CVE-2023-4903)

- Insufficient policy enforcement in Downloads in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to bypass Enterprise policy restrictions via a crafted download. (Chromium security severity:

Medium) (CVE-2023-4904)

- Inappropriate implementation in Prompts in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4905)

- Insufficient policy enforcement in Autofill in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-4906)

- Inappropriate implementation in Intents in Google Chrome on Android prior to 117.0.5938.62 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-4907)

- Inappropriate implementation in Picture in Picture in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-4908)

- Inappropriate implementation in Interstitials in Google Chrome prior to 117.0.5938.62 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-4909)

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?db9a43f1

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36562

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36727

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36735

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4863

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4900

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4901

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4902

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4903

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4904

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4905

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4906

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4907

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4908

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4909

Solution

Upgrade to Microsoft Edge version 117.0.2045.31 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

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

VPR Score

9.8

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-2023-4863
CVE	CVE-2023-4900
CVE	CVE-2023-4901
CVE	CVE-2023-4902
CVE	CVE-2023-4903
CVE	CVE-2023-4904
CVE	CVE-2023-4905
CVE	CVE-2023-4906
CVE	CVE-2023-4907
CVE	CVE-2023-4908
CVE	CVE-2023-4909
CVE	CVE-2023-36562
CVE	CVE-2023-36727
CVE	CVE-2023-36735
XREF	CISA-KNOWN-EXPLOITED:2023/10/04

Plugin Information

Published: 2023/09/15, Modified: 2023/10/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 117.0.2045.31
```

186447 - Microsoft Edge (Chromium) < 118.0.2088.122 / 119.0.2151.97 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 118.0.2088.122 / 119.0.2151.97. It is, therefore, affected by multiple vulnerabilities as referenced in the November 29, 2023 advisory.

- Integer overflow in Skia in Google Chrome prior to 119.0.6045.199 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a malicious file. (Chromium security severity: High) (CVE-2023-6345)

- Use after free in WebAudio in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-6346)

- Use after free in Mojo in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-6347)

- Type Confusion in Spellcheck in Google Chrome prior to 119.0.6045.199 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-6348)

- Use after free in libavif in Google Chrome prior to 119.0.6045.199 allowed a remote attacker to potentially exploit heap corruption via a crafted avif file. (Chromium security severity: High) (CVE-2023-6350, CVE-2023-6351)

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?88d07bbe

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6345

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6346

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6347

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6348

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6350

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6351

Solution

Upgrade to Microsoft Edge version 118.0.2088.122 / 119.0.2151.97 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

9.9

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-2023-6345
CVE	CVE-2023-6346
CVE	CVE-2023-6347
CVE	CVE-2023-6348
CVE	CVE-2023-6350
CVE	CVE-2023-6351
XREF	CISA-KNOWN-EXPLOITED:2023/12/21

Plugin Information

Published: 2023/11/29, Modified: 2023/12/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 119.0.2151.97
```

186681 - Microsoft Edge (Chromium) < 120.0.2210.61 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 120.0.2210.61. It is, therefore, affected by multiple vulnerabilities as referenced in the December 7, 2023 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability (CVE-2023-35618)

- Microsoft Edge (Chromium-based) Information Disclosure Vulnerability (CVE-2023-36880, CVE-2023-38174)

- Use after free in Media Stream in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-6508)

- Use after free in Side Panel Search in Google Chrome prior to 120.0.6099.62 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: High) (CVE-2023-6509)

- Use after free in Media Capture in Google Chrome prior to 120.0.6099.62 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium) (CVE-2023-6510)

- Inappropriate implementation in Autofill in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-6511)

- Inappropriate implementation in Web Browser UI in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to potentially spoof the contents of an iframe dialog context menu via a crafted HTML page.

(Chromium security severity: Low) (CVE-2023-6512)

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?7f2952a2

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35618

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36880

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38174

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6508

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6509

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6510

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6511

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6512

Solution

Upgrade to Microsoft Edge version 120.0.2210.61 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

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

VPR Score

7.4

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-2023-6508
CVE	CVE-2023-6509
CVE	CVE-2023-6510
CVE	CVE-2023-6511
CVE	CVE-2023-6512
CVE	CVE-2023-35618
CVE	CVE-2023-36880
CVE	CVE-2023-38174
XREF	IAVA:2023-A-0677-S

Plugin Information

Published: 2023/12/07, Modified: 2023/12/22

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 120.0.2210.61
```

153450 - Microsoft Edge (Chromium) < 93.0.961.52 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 93.0.961.52. It is, therefore, affected by multiple vulnerabilities as referenced in the September 16, 2021 advisory.

- Use after free in Indexed DB API in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (CVE-2021-30633)

- Use after free in Selection API in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who convinced the user the visit a malicious website to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-30625)

- Out of bounds memory access in ANGLE in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-30626)

- Type confusion in Blink layout in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-30627)

- Stack buffer overflow in ANGLE in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. (CVE-2021-30628)

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?603235a5

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30625

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30626

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30627

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30628

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30629

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30630

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30633

Solution

Upgrade to Microsoft Edge version 93.0.961.52 or later.

Risk Factor

Medium

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

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-2021-30625
CVE	CVE-2021-30626
CVE	CVE-2021-30627
CVE	CVE-2021-30628
CVE	CVE-2021-30629
CVE	CVE-2021-30630
CVE	CVE-2021-30633
XREF	CISA-KNOWN-EXPLOITED:2021/11/17

Plugin Information

Published: 2021/09/17, Modified: 2024/01/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 93.0.961.52
```

153666 - Microsoft Edge (Chromium) < 94.0.992.31 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 94.0.992.31. It is, therefore, affected by multiple vulnerabilities as referenced in the September 24, 2021 advisory.

- Use after free in Portals in Google Chrome prior to 94.0.4606.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

(CVE-2021-37973)

- Use after free in Offline use in Google Chrome on Android prior to 94.0.4606.54 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.

(CVE-2021-37956)

- Use after free in WebGPU in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-37957)

- Inappropriate implementation in Navigation in Google Chrome on Windows prior to 94.0.4606.54 allowed a remote attacker to inject scripts or HTML into a privileged page via a crafted HTML page. (CVE-2021-37958)

- Use after free in Task Manager in Google Chrome prior to 94.0.4606.54 allowed an attacker who convinced a user to enage in a series of user gestures to potentially exploit heap corruption via a crafted HTML page.

(CVE-2021-37959)

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?6dbcb9b7

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37956

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37957

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37958

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37959

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37961

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37962

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37963

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37964

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37965

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37966

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37967
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37968
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37969
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37970
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37971
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37972
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37973

Solution

Upgrade to Microsoft Edge version 94.0.992.31 or later.

Risk Factor

Medium

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

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)

STIG Severity

I

References

CVE	CVE-2021-37956
CVE	CVE-2021-37957
CVE	CVE-2021-37958
CVE	CVE-2021-37959
CVE	CVE-2021-37961

CVE	CVE-2021-37962
CVE	CVE-2021-37963
CVE	CVE-2021-37964
CVE	CVE-2021-37965
CVE	CVE-2021-37966
CVE	CVE-2021-37967
CVE	CVE-2021-37968
CVE	CVE-2021-37969
CVE	CVE-2021-37970
CVE	CVE-2021-37971
CVE	CVE-2021-37972
CVE	CVE-2021-37973
XREF	IAVA:2021-A-0448-S
XREF	CISA-KNOWN-EXPLOITED:2021/11/17

Plugin Information

Published: 2021/09/24, Modified: 2024/01/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 94.0.992.31
```

154327 - Microsoft Edge (Chromium) < 95.0.1020.30 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 95.0.1020.30. It is, therefore, affected by multiple vulnerabilities as referenced in the October 21, 2021 advisory.

- Use after free in PDF Accessibility in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-37993)

- Heap buffer overflow in Skia in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (CVE-2021-37981)

- Use after free in Incognito in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-37982)

- Use after free in Dev Tools in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-37983)

- Heap buffer overflow in PDFium in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-37984)

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?6d633bfe

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37981

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37982

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37983

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37984

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37985

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37986

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37987

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37988

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37989

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37990

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37991

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37992

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37993

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37994

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37995
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37996
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42307

Solution

Upgrade to Microsoft Edge version 95.0.1020.30 or later.

Risk Factor

Medium

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

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-2021-37981
CVE	CVE-2021-37982
CVE	CVE-2021-37983
CVE	CVE-2021-37984
CVE	CVE-2021-37985
CVE	CVE-2021-37986
CVE	CVE-2021-37987
CVE	CVE-2021-37988
CVE	CVE-2021-37989

CVE	CVE-2021-37990
CVE	CVE-2021-37991
CVE	CVE-2021-37992
CVE	CVE-2021-37993
CVE	CVE-2021-37994
CVE	CVE-2021-37995
CVE	CVE-2021-37996
CVE	CVE-2021-42307
XREF	IAVA:2021-A-0491-S
XREF	IAVA:2021-A-0544-S

Plugin Information

Published: 2021/10/21, Modified: 2023/10/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 95.0.1020.30
```

154738 - Microsoft Edge (Chromium) < 95.0.1020.40 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 95.0.1020.40. It is, therefore, affected by multiple vulnerabilities as referenced in the October 29, 2021 advisory.

- Inappropriate implementation in V8 in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-38003)

- Use after free in Sign-In in Google Chrome prior to 95.0.4638.69 allowed a remote attacker who convinced a user to sign into Chrome to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-37997)

- Use after free in Garbage Collection in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-37998)

- Insufficient data validation in New Tab Page in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to inject arbitrary scripts or HTML in a new browser tab via a crafted HTML page.

(CVE-2021-37999)

- Insufficient validation of untrusted input in Intents in Google Chrome on Android prior to 95.0.4638.69 allowed a remote attacker to arbitrarily browser to a malicious URL via a crafted HTML page.

(CVE-2021-38000)

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?dd5c7f7f

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37997

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37998

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37999

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38000

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38001

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38002

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38003

Solution

Upgrade to Microsoft Edge version 95.0.1020.40 or later.

Risk Factor

Medium

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

7.4

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

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

STIG Severity

I

References

CVE	CVE-2021-37997
CVE	CVE-2021-37998
CVE	CVE-2021-37999
CVE	CVE-2021-38000
CVE	CVE-2021-38001
CVE	CVE-2021-38002
CVE	CVE-2021-38003
XREF	IAVA:2021-A-0522-S
XREF	CISA-KNOWN-EXPLOITED:2021/11/17

Plugin Information

Published: 2021/10/29, Modified: 2023/04/25

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Microsoft\Edge\Application
  Installed version : 92.0.902.67
```

```
    Fixed version     : 95.0.1020.40
```

155653 - Microsoft Edge (Chromium) < 96.0.1052.29 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 96.0.1052.29. It is, therefore, affected by multiple vulnerabilities as referenced in the November 19, 2021 advisory.

- Insufficient policy enforcement in iframe sandbox in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (CVE-2021-38017)

- Use after free in loader in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-38005)

- Use after free in storage foundation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-38006, CVE-2021-38011)

- Type confusion in V8 in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-38007, CVE-2021-38012)

- Use after free in media in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-38008)

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?95dce263

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38005

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38006

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38007

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38008

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38009

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38010

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38011

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38012

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38013

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38014

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38015

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38016

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38017

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38018

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38019

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38020
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38021
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38022
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42308
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43221

Solution

Upgrade to Microsoft Edge version 96.0.1052.29 or later.

Risk Factor

Medium

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

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

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

STIG Severity

I

References

CVE	CVE-2021-38005
CVE	CVE-2021-38006
CVE	CVE-2021-38007
CVE	CVE-2021-38008
CVE	CVE-2021-38009
CVE	CVE-2021-38010
CVE	CVE-2021-38011

CVE	CVE-2021-38012
CVE	CVE-2021-38013
CVE	CVE-2021-38014
CVE	CVE-2021-38015
CVE	CVE-2021-38016
CVE	CVE-2021-38017
CVE	CVE-2021-38018
CVE	CVE-2021-38019
CVE	CVE-2021-38020
CVE	CVE-2021-38021
CVE	CVE-2021-38022
CVE	CVE-2021-43221
XREF	IAVA:2021-A-0544-S

Plugin Information

Published: 2021/11/20, Modified: 2023/10/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 96.0.1052.29
```

171335 - Microsoft Edge (Chromium) < 96.0.1054.29 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 96.0.1054.29. It is, therefore, affected by multiple vulnerabilities as referenced in the November 19, 2021 advisory.

- Use after free in loader in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-38005)

- Use after free in storage foundation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-38006, CVE-2021-38011)

- Type confusion in V8 in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-38007, CVE-2021-38012)

- Use after free in media in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-38008)

- Inappropriate implementation in cache in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (CVE-2021-38009)

- Inappropriate implementation in service workers in Google Chrome prior to 96.0.4664.45 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.

(CVE-2021-38010)

- Heap buffer overflow in fingerprint recognition in Google Chrome on ChromeOS prior to 96.0.4664.45 allowed a remote attacker who had compromised a WebUI renderer process to potentially perform a sandbox escape via a crafted HTML page. (CVE-2021-38013)

- Out of bounds write in Swiftshader in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-38014)

- Inappropriate implementation in input in Google Chrome prior to 96.0.4664.45 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (CVE-2021-38015)

- Insufficient policy enforcement in background fetch in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (CVE-2021-38016)

- Insufficient policy enforcement in iframe sandbox in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (CVE-2021-38017)

- Inappropriate implementation in navigation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (CVE-2021-38018)

- Insufficient policy enforcement in CORS in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (CVE-2021-38019)

- Insufficient policy enforcement in contacts picker in Google Chrome on Android prior to 96.0.4664.45 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.

(CVE-2021-38020)

- Inappropriate implementation in referrer in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (CVE-2021-38021)

- Inappropriate implementation in WebAuthentication in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (CVE-2021-38022)

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2021-42308)

- Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability (CVE-2021-43221)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38005

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38006

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38007

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38008

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38009

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38010

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38011

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38012

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38013

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38014

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38015

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38016

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38017

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38018

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38019

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38020

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38021

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38022

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42308

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43221

Solution

Upgrade to Microsoft Edge version 96.0.1054.29 or later.

Risk Factor

Medium

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

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

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

STIG Severity

I

References

CVE	CVE-2021-38005
CVE	CVE-2021-38006
CVE	CVE-2021-38007
CVE	CVE-2021-38008
CVE	CVE-2021-38009
CVE	CVE-2021-38010
CVE	CVE-2021-38011
CVE	CVE-2021-38012
CVE	CVE-2021-38013
CVE	CVE-2021-38014
CVE	CVE-2021-38015
CVE	CVE-2021-38016
CVE	CVE-2021-38017
CVE	CVE-2021-38018
CVE	CVE-2021-38019
CVE	CVE-2021-38020
CVE	CVE-2021-38021
CVE	CVE-2021-38022
CVE	CVE-2021-42308
CVE	CVE-2021-43221

XREF IAVA:2021-A-0544-S

Plugin Information

Published: 2023/02/10, Modified: 2023/10/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 96.0.1054.29
```

156545 - Microsoft Edge (Chromium) < 97.0.1072.55 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 97.0.1072.55. It is, therefore, affected by multiple vulnerabilities as referenced in the January 6, 2022 advisory.

- Use after free in File Manager API in Google Chrome on Chrome OS prior to 97.0.4692.71 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-0107)

- Use after free in Storage in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-0096)

- Inappropriate implementation in DevTools in Google Chrome prior to 97.0.4692.71 allowed an attacker who convinced a user to install a malicious extension to to potentially allow extension to escape the sandbox via a crafted HTML page. (CVE-2022-0097)

- Use after free in Screen Capture in Google Chrome on Chrome OS prior to 97.0.4692.71 allowed an attacker who convinced a user to perform specific user gestures to potentially exploit heap corruption via specific user gestures. (CVE-2022-0098)

- Use after free in Sign-in in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who convinced a user to perform specific user gestures to potentially exploit heap corruption via specific user gesture.

(CVE-2022-0099)

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?10ad4694

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0096

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0097

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0098

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0099

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0100

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0101

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0102

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0103

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0104

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0105

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0106

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0107

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0108
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0109
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0110
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0111
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0112
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0113
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0114
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0115
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0116
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0117
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0118
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0120
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21929
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21930
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21931
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21954
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21970

Solution

Upgrade to Microsoft Edge version 97.0.1072.55 or later.

Risk Factor

High

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-0096
CVE	CVE-2022-0097
CVE	CVE-2022-0098
CVE	CVE-2022-0099
CVE	CVE-2022-0100
CVE	CVE-2022-0101
CVE	CVE-2022-0102
CVE	CVE-2022-0103
CVE	CVE-2022-0104
CVE	CVE-2022-0105
CVE	CVE-2022-0106
CVE	CVE-2022-0107
CVE	CVE-2022-0108
CVE	CVE-2022-0109
CVE	CVE-2022-0110
CVE	CVE-2022-0111
CVE	CVE-2022-0112
CVE	CVE-2022-0113
CVE	CVE-2022-0114
CVE	CVE-2022-0115
CVE	CVE-2022-0116
CVE	CVE-2022-0117
CVE	CVE-2022-0118
CVE	CVE-2022-0120
CVE	CVE-2022-21929
CVE	CVE-2022-21930
CVE	CVE-2022-21931
CVE	CVE-2022-21954
CVE	CVE-2022-21970

Plugin Information

Published: 2022/01/06, Modified: 2022/05/06

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Microsoft\Edge\Application
  Installed version : 92.0.902.67
```

```
    Fixed version     : 97.0.1072.55
```

158583 - Microsoft Edge (Chromium) < 99.0.1150.30 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 99.0.1150.30. It is, therefore, affected by multiple vulnerabilities as referenced in the March 3, 2022 advisory.

- Use after free in Chrome OS Shell in Google Chrome on Chrome OS prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in a series of user interaction to potentially exploit heap corruption via user interactions. (CVE-2022-0808)

- Heap buffer overflow in ANGLE in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-0789)

- Use after free in Cast UI in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially perform a sandbox escape via a crafted HTML page. (CVE-2022-0790)

- Use after free in Omnibox in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via user interactions.

(CVE-2022-0791)

- Out of bounds read in ANGLE in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-0792)

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?764ee88a

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0789

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0790

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0791

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0792

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0793

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0794

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0795

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0796

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0797

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0798

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0799

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0800

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0801
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0802
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0803
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0804
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0805
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0806
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0807
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0808
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0809

Solution

Upgrade to Microsoft Edge version 99.0.1150.30 or later.

Risk Factor

Medium

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

7.4

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

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

STIG Severity

I

References

CVE	CVE-2022-0789
CVE	CVE-2022-0790

CVE	CVE-2022-0791
CVE	CVE-2022-0792
CVE	CVE-2022-0793
CVE	CVE-2022-0794
CVE	CVE-2022-0795
CVE	CVE-2022-0796
CVE	CVE-2022-0797
CVE	CVE-2022-0798
CVE	CVE-2022-0799
CVE	CVE-2022-0800
CVE	CVE-2022-0801
CVE	CVE-2022-0802
CVE	CVE-2022-0803
CVE	CVE-2022-0804
CVE	CVE-2022-0805
CVE	CVE-2022-0806
CVE	CVE-2022-0807
CVE	CVE-2022-0808
CVE	CVE-2022-0809
XREF	IAVA:2022-A-0096-S

Plugin Information

Published: 2022/03/03, Modified: 2023/01/10

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 99.0.1150.30
```

159037 - Microsoft Edge (Chromium) < 99.0.1150.46 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 99.0.1150.46. It is, therefore, affected by multiple vulnerabilities as referenced in the March 17, 2022 advisory.

- Use after free in New Tab Page in Google Chrome prior to 99.0.4844.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific user interactions. (CVE-2022-0980)

- Use after free in Blink Layout in Google Chrome on Android prior to 99.0.4844.74 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.

(CVE-2022-0971)

- Use after free in Extensions in Google Chrome prior to 99.0.4844.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.

(CVE-2022-0972)

- Use after free in Safe Browsing in Google Chrome prior to 99.0.4844.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-0973)

- Use after free in Splitscreen in Google Chrome on Chrome OS prior to 99.0.4844.74 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-0974)

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?0cc84aae

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0971

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0972

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0973

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0974

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0975

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0976

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0977

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0978

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0979

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0980

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26899

Solution

Upgrade to Microsoft Edge version 99.0.1150.46 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

9.2

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-2022-0971
CVE	CVE-2022-0972
CVE	CVE-2022-0973
CVE	CVE-2022-0974
CVE	CVE-2022-0975
CVE	CVE-2022-0976
CVE	CVE-2022-0977
CVE	CVE-2022-0978
CVE	CVE-2022-0979
CVE	CVE-2022-0980
CVE	CVE-2022-26899
XREF	IAVA:2022-A-0120-S
XREF	IAVA:2021-A-0544-S

Plugin Information

Published: 2022/03/17, Modified: 2023/11/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 99.0.1150.46
```

52544 - Microsoft Forefront Endpoint Protection / System Center Endpoint Protection / Anti-malware Client Detection and Status

Synopsis

An antivirus or antimalware application is installed on the remote host, but it is not working properly.

Description

Microsoft Forefront Endpoint Protection, or another antimalware product from Microsoft, is installed on the remote host. However, there is a problem with the installation; either its services are not running or its engine and/or virus definitions are out of date.

See Also

http://www.nessus.org/u?a56c4934

Solution

Make sure that updates are working and the associated services are running.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2011/03/04, Modified: 2022/10/10

Plugin Output

tcp/445/cifs

```
A Microsoft anti-malware product is installed on the remote host :

  Product name                 : Windows Defender
  Path                         : C:\Program Files\Windows Defender\
  Version                      : 4.18.1909.6
  Engine version               : 1.1.16400.2
  Antivirus signature version  : 1.303.25.0
  Antispyware signature version : 1.303.25.0
```

```
The antivirus signatures are out of date. The last known updated
version from the vendor is : 1.305.1053.0
The antispyware signatures are out of date. The last known updated
version from the vendor is : 1.305.1053.0

As a result, the remote host might be infected by viruses received by
email or other means.
```

22024 - Microsoft Internet Explorer Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of Internet Explorer.

Description

According to its self-reported version number, the installation of Microsoft Internet Explorer on the remote Windows host is no longer supported.

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

See Also

http://www.nessus.org/u?828ddfe1

http://www.nessus.org/u?e0d2ff5a

https://docs.microsoft.com/en-us/deployedge/edge-ie-disable-ie11

Solution

Either Upgrade to a version of Internet Explorer that is currently supported or disable Internet Explorer on the target device.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0557

Plugin Information

Published: 2006/07/11, Modified: 2023/07/04

Plugin Output

tcp/445/cifs

```
The remote host has Internet Explorer version 11.3636.19041.0 installed, which is no longer
 supported.

Internet Explorer is being detected as enabled on this device.
This is due to the fact that the Registry key is missing or not set:

'\HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\NotifyDisableIEOptions'

The InternetExplorerIntegrationReloadInIEModeAllowed policy is not configured
which means users can render content in IE Mode.
```

96775 - Mozilla Firefox ESR < 45.7 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The version of Mozilla Firefox ESR installed on the remote Windows host is prior to 45.7. It is, therefore, affected by multiple vulnerabilities :

- Mozilla developers and community members Christian Holler, Gary Kwong, Andre Bargull, Jan de Mooij, Tom Schuster, and Oriol reported memory safety bugs present in Firefox 50.1 and Firefox ESR 45.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code.

(CVE-2017-5373)

- JIT code allocation can allow for a bypass of ASLR and DEP protections leading to potential memory corruption attacks. (CVE-2017-5375)

- Use-after-free while manipulating XSL in XSLT documents (CVE-2017-5376)

- Hashed codes of JavaScript objects are shared between pages. This allows for pointer leaks because an object's address can be discovered through hash codes, and also allows for data leakage of an object's content using these hash codes. (CVE-2017-5378)

- A potential use-after-free found through fuzzing during DOM manipulation of SVG content. (CVE-2017-5380)

- URLs containing certain unicode glyphs for alternative hyphens and quotes do not properly trigger punycode display, allowing for domain name spoofing attacks in the location bar. (CVE-2017-5383)

- WebExtension scripts can use the 'data:' protocol to affect pages loaded by other web extensions using this protocol, leading to potential data disclosure or privilege escalation in affected extensions.

(CVE-2017-5386)

- The JSON viewer in the Developer Tools uses insecure methods to create a communication channel for copying and viewing JSON or HTTP headers data, allowing for potential privilege escalation. (CVE-2017-5390)

- A use-after-free vulnerability in the Media Decoder when working with media files when some events are fired after the media elements are freed from memory.

(CVE-2017-5396)

Note that Tenable Network Security has extracted the preceding description block directly from the Mozilla security advisories.

Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2017-02/

https://bugzilla.mozilla.org/show_bug.cgi?id=1285833

https://bugzilla.mozilla.org/show_bug.cgi?id=1285960
https://bugzilla.mozilla.org/show_bug.cgi?id=1297361
https://bugzilla.mozilla.org/show_bug.cgi?id=1311687
https://bugzilla.mozilla.org/show_bug.cgi?id=1312001
https://bugzilla.mozilla.org/show_bug.cgi?id=1319070
https://bugzilla.mozilla.org/show_bug.cgi?id=1322107
https://bugzilla.mozilla.org/show_bug.cgi?id=1322315
https://bugzilla.mozilla.org/show_bug.cgi?id=1322420
https://bugzilla.mozilla.org/show_bug.cgi?id=1323338
https://bugzilla.mozilla.org/show_bug.cgi?id=1324716
https://bugzilla.mozilla.org/show_bug.cgi?id=1325200
https://bugzilla.mozilla.org/show_bug.cgi?id=1325877
https://bugzilla.mozilla.org/show_bug.cgi?id=1325938
https://bugzilla.mozilla.org/show_bug.cgi?id=1328251
https://bugzilla.mozilla.org/show_bug.cgi?id=1328834
https://bugzilla.mozilla.org/show_bug.cgi?id=1329403
https://bugzilla.mozilla.org/show_bug.cgi?id=1330769
https://bugzilla.mozilla.org/show_bug.cgi?id=1331058

Solution

Upgrade to Mozilla Firefox ESR version 45.7 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	95757
BID	95758
BID	95762
BID	95769
CVE	CVE-2017-5373
CVE	CVE-2017-5375
CVE	CVE-2017-5376
CVE	CVE-2017-5378
CVE	CVE-2017-5380
CVE	CVE-2017-5383
CVE	CVE-2017-5386
CVE	CVE-2017-5390
CVE	CVE-2017-5396
XREF	MFSA:2017-02

Plugin Information

Published: 2017/01/25, Modified: 2019/11/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 45.7 ESR
```

97638 - Mozilla Firefox ESR < 45.8 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The version of Mozilla Firefox ESR installed on the remote Windows host is prior to 45.8. It is, therefore, affected by multiple vulnerabilities :

- Mozilla developers and community members Boris Zbarsky, Christian Holler, Honza Bambas, Jon Coppeard, Randell Jesup, Andre Bargull, Kan-Ru Chen, and Nathan Froyd reported memory safety bugs present in Firefox 51 and Firefox ESR 45.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. (CVE-2017-5398)

- JIT-spray targeting asm.js combined with a heap spray allows for a bypass of ASLR and DEP protections leading to potential memory corruption attacks. (CVE-2017-5400)

- A crash triggerable by web content in which an ErrorResult references unassigned memory due to a logic error. The resulting crash may be exploitable.

(CVE-2017-5401)

- A use-after-free can occur when events are fired for a FontFace object after the object has been already been destroyed while working with fonts. This results in a potentially exploitable crash. (CVE-2017-5402)

- A use-after-free error can occur when manipulating ranges in selections with one node inside a native anonymous tree and one node outside of it. This results in a potentially exploitable crash. (CVE-2017-5404)

- Certain response codes in FTP connections can result in the use of uninitialized values for ports in FTP operations. (CVE-2017-5405)

- Using SVG filters that don't use the fixed point math implementation on a target iframe, a malicious page can extract pixel values from a targeted user. This can be used to extract history information and read text values across domains. This violates same-origin policy and leads to information disclosure. (CVE-2017-5407)

- Video files loaded video captions cross-origin without checking for the presence of CORS headers permitting such cross-origin use, leading to potential information disclosure for video captions. (CVE-2017-5408)

- The Mozilla Windows updater can be called by a non-privileged user to delete an arbitrary local file by passing a special path to the callback parameter through the Mozilla Maintenance Service, which has privileged access. Note: This attack requires local system access and only affects Windows. Other operating systems are not affected. (CVE-2017-5409)

- Memory corruption resulting in a potentially exploitable crash during garbage collection of JavaScript due errors in how incremental sweeping is managed for memory cleanup. (CVE-2017-5410)

Note that Tenable Network Security has extracted the preceding description block directly from the Mozilla security advisories.

Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2017-06/

Solution

Upgrade to Mozilla Firefox ESR version 45.8 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

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

BID	96651
BID	96654
BID	96664
BID	96677
BID	96693
BID	96696
CVE	CVE-2017-5398
CVE	CVE-2017-5400
CVE	CVE-2017-5401
CVE	CVE-2017-5402
CVE	CVE-2017-5404
CVE	CVE-2017-5405
CVE	CVE-2017-5407

CVE	CVE-2017-5408
CVE	CVE-2017-5409
CVE	CVE-2017-5410
XREF	MFSA:2017-06

Plugin Information

Published: 2017/03/09, Modified: 2019/11/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 45.8 ESR
```

119606 - Mozilla Firefox ESR < 60.4 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox ESR installed on the remote Windows host is prior to 60.4. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2018-30 advisory.

- Mozilla developers and community members Christian Holler, Diego Calleja, Andrew McCreight, Jon Coppeard, Jed Davis, Natalia Csoregi, Nicolas B. Pierron, and Tyson Smith reported memory safety bugs present in Firefox 63 and Firefox ESR 60.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. (CVE-2018-12405)

- A buffer overflow and out-of-bounds read can occur in TextureStorage11 within the ANGLE graphics library, used for WebGL content. This results in a potentially exploitable crash. (CVE-2018-17466)

- A use-after-free vulnerability can occur after deleting a selection element due to a weak reference to the select element in the options collection. This results in a potentially exploitable crash. (CVE-2018-18492)

- A buffer overflow can occur in the Skia library during buffer offset calculations with hardware accelerated canvas 2D actions due to the use of 32-bit calculations instead of 64-bit. This results in a potentially exploitable crash. (CVE-2018-18493)

- A same-origin policy violation allowing the theft of cross-origin URL entries when using the Javascript location property to cause a redirection to another site using performance.getEntries(). This is a same-origin policy violation and could allow for data theft.

(CVE-2018-18494)

- A potential vulnerability leading to an integer overflow can occur during buffer size calculations for images when a raw value is used instead of the checked value.

This leads to a possible out-of-bounds write.

(CVE-2018-18498)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2018-30/

https://bugzilla.mozilla.org/show_bug.cgi?id=1488295

https://bugzilla.mozilla.org/show_bug.cgi?id=1499861

https://bugzilla.mozilla.org/show_bug.cgi?id=1504452

https://bugzilla.mozilla.org/show_bug.cgi?id=1487964

https://bugzilla.mozilla.org/show_bug.cgi?id=1500011

https://bugzilla.mozilla.org/show_bug.cgi?id=1494752

https://bugzilla.mozilla.org/show_bug.cgi?id=1498765

https://bugzilla.mozilla.org/show_bug.cgi?id=1503326
https://bugzilla.mozilla.org/show_bug.cgi?id=1505181
https://bugzilla.mozilla.org/show_bug.cgi?id=1500759
https://bugzilla.mozilla.org/show_bug.cgi?id=1504365
https://bugzilla.mozilla.org/show_bug.cgi?id=1506640
https://bugzilla.mozilla.org/show_bug.cgi?id=1503082
https://bugzilla.mozilla.org/show_bug.cgi?id=1502013
https://bugzilla.mozilla.org/show_bug.cgi?id=1510471

Solution

Upgrade to Mozilla Firefox ESR version 60.4 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-12405
CVE	CVE-2018-17466
CVE	CVE-2018-18492
CVE	CVE-2018-18493
CVE	CVE-2018-18494
CVE	CVE-2018-18498
XREF	MFSA:2018-30

Plugin Information

Published: 2018/12/12, Modified: 2019/11/01

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 60.4 ESR
```

121477 - Mozilla Firefox ESR < 60.5

Synopsis

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

Description

The version of Firefox ESR installed on the remote Windows host is prior to 60.5. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2019-02 advisory.

- A use-after-free vulnerability can occur while parsing an HTML5 stream in concert with custom HTML elements.

This results in the stream parser object being freed while still in use, leading to a potentially exploitable crash. (CVE-2018-18500)

- An earlier fix for an Inter-process Communication (IPC) vulnerability, CVE-2011-3079, added authentication to communication between IPC endpoints and server parents during IPC process creation. This authentication is insufficient for channels created after the IPC process is started, leading to the authentication not being correctly applied to later channels. This could allow for a sandbox escape through IPC channels due to lack of message validation in the listener process.

(CVE-2018-18505)

- Mozilla developers and community members Alex Gaynor, Christoph Diehl, Steven Crane, Jason Kratzer, Gary Kwong, and Christian Holler reported memory safety bugs present in Firefox 64 and Firefox ESR 60.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. (CVE-2018-18501)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2019-02/

https://bugzilla.mozilla.org/show_bug.cgi?id=1510114

https://bugzilla.mozilla.org/show_bug.cgi?id=1497749

https://bugzilla.mozilla.org/show_bug.cgi?id=1087565

https://bugzilla.mozilla.org/show_bug.cgi?id=1512450

https://bugzilla.mozilla.org/show_bug.cgi?id=1517542

https://bugzilla.mozilla.org/show_bug.cgi?id=1513201

https://bugzilla.mozilla.org/show_bug.cgi?id=1460619

https://bugzilla.mozilla.org/show_bug.cgi?id=1502871

https://bugzilla.mozilla.org/show_bug.cgi?id=1516738

https://bugzilla.mozilla.org/show_bug.cgi?id=1516514

Solution

Upgrade to Mozilla Firefox ESR version 60.5 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-18500
CVE	CVE-2018-18501
CVE	CVE-2018-18505
XREF	MFSA:2019-02

Plugin Information

Published: 2019/01/30, Modified: 2021/02/09

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 60.5 ESR
```

134407 - Mozilla Firefox ESR < 68.6 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox ESR installed on the remote Windows host is prior to 68.6. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-09 advisory. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2020-09/

Solution

Upgrade to Mozilla Firefox ESR version 68.6 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-20503
CVE	CVE-2020-6805

CVE	CVE-2020-6806
CVE	CVE-2020-6807
CVE	CVE-2020-6811
CVE	CVE-2020-6812
CVE	CVE-2020-6814
XREF	MFSA:2020-09

Plugin Information

Published: 2020/03/11, Modified: 2020/05/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 68.6 ESR
```

40362 - Mozilla Foundation Unsupported Application Detection

Synopsis

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

Description

According to its version, there is at least one unsupported Mozilla application (Firefox, Thunderbird, and/or SeaMonkey) installed on the remote host. This version of the software is no longer actively maintained.

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

See Also

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

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

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

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

https://www.seamonkey-project.org/releases/

Solution

Upgrade to a version that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	IAVA:0001-A-0565

Plugin Information

Published: 2009/07/24, Modified: 2022/11/04

Plugin Output

tcp/445/cifs

```
Product           : Mozilla Firefox ESR
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1
Latest version    : 115.6.0
EOL URL           : https://www.mozilla.org/en-US/firefox/releases/
```

187901 - Security Updates for Microsoft .NET Framework (January 2024)

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 vulnerabilities, as follows:

- Denial of service vulnerability in Microsoft .NET Framework. (CVE-2023-36042, CVE-2024-21312)

- Security feature bypass in System.Data.SqlClient SQL data provider. An attacker can perform a man-in-the-middle attack on the connection between the client and server in order to read and modify the TLS traffic. (CVE-2024-0056)

- Security feature bypass in applications that use the X.509 chain building APIs. When processing an untrusted certificate with malformed signatures, the framework returns an incorrect reason code.

Applications which make use of this reason code may treat this scenario as a successful chain build, potentially bypassing the application's typical authentication logic. (CVE-2024-0057)

See Also

http://www.nessus.org/u?a8f77e6e

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36042

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0056

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0057

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21312

https://support.microsoft.com/en-us/help/5033898

https://support.microsoft.com/en-us/help/5033899

https://support.microsoft.com/en-us/help/5033904

https://support.microsoft.com/en-us/help/5033907

https://support.microsoft.com/en-us/help/5033909

https://support.microsoft.com/en-us/help/5033910

https://support.microsoft.com/en-us/help/5033911

https://support.microsoft.com/en-us/help/5033912

https://support.microsoft.com/en-us/help/5033914

https://support.microsoft.com/en-us/help/5033916

https://support.microsoft.com/en-us/help/5033917

https://support.microsoft.com/en-us/help/5033918

https://support.microsoft.com/en-us/help/5033919

https://support.microsoft.com/en-us/help/5033920

https://support.microsoft.com/en-us/help/5033922

https://support.microsoft.com/en-us/help/5033945
https://support.microsoft.com/en-us/help/5033946
https://support.microsoft.com/en-us/help/5033947
https://support.microsoft.com/en-us/help/5033948

Solution

Microsoft has released security updates for Microsoft .NET Framework.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.1

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-2023-36042
CVE	CVE-2024-0056
CVE	CVE-2024-0057
CVE	CVE-2024-21312
MSKB	5033898
MSKB	5033899
MSKB	5033904
MSKB	5033907

MSKB	5033909
MSKB	5033910
MSKB	5033911
MSKB	5033912
MSKB	5033914
MSKB	5033916
MSKB	5033917
MSKB	5033918
MSKB	5033919
MSKB	5033920
MSKB	5033922
MSKB	5033945
MSKB	5033946
MSKB	5033947
MSKB	5033948
XREF	MSFT:MS24-5033898
XREF	MSFT:MS24-5033899
XREF	MSFT:MS24-5033904
XREF	MSFT:MS24-5033907
XREF	MSFT:MS24-5033909
XREF	MSFT:MS24-5033910
XREF	MSFT:MS24-5033911
XREF	MSFT:MS24-5033912
XREF	MSFT:MS24-5033914
XREF	MSFT:MS24-5033916
XREF	MSFT:MS24-5033917
XREF	MSFT:MS24-5033918
XREF	MSFT:MS24-5033919
XREF	MSFT:MS24-5033920
XREF	MSFT:MS24-5033922
XREF	MSFT:MS24-5033945
XREF	MSFT:MS24-5033946
XREF	MSFT:MS24-5033947
XREF	MSFT:MS24-5033948
XREF	IAVA:2024-A-0011

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Microsoft .NET Framework 4.8
The remote host is missing one of the following rollup KBs :

Cumulative
  - 5033909

C:\Windows\Microsoft.NET\Framework\v4.0.30319\system.web.dll has not been patched.
    Remote version : 4.8.4682.0
    Should be      : 4.8.4690.0
```

58348 - Firefox 10.0.x < 10.0.3 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The installed version of Firefox 10.0.x is potentially affected by the following security issues :

- Multiple memory corruption issues. By tricking a user into visiting a specially crafted page, these issues may allow an attacker to execute arbitrary code in the context of the affected application. (CVE-2012-0454, CVE-2012-0457, CVE-2012-0459, CVE-2012-0461, CVE-2012-0462, CVE-2012-0463, CVE-2012-0464)

- An HTTP Header security bypass vulnerability exists that can be leveraged by attackers to bypass certain security restrictions and conduct cross-site scripting attacks. (CVE-2012-0451).

- A security bypass vulnerability exists that can be exploited by an attacker if the victim can be tricked into setting a new home page by dragging a specially crafted link to the 'home' button URL, which will set the user's home page to a 'javascript:' URL. (CVE-2012-0458)

- An information disclosure vulnerability exists due to an out-of-bounds read in SVG filters. (CVE-2012-0456)

- A cross-site scripting vulnerability exists that can be triggered by dragging and dropping 'javascript:' links onto a frame. (CVE-2012-0455)

- 'window.fullScreen' is writeable by untrusted content, allowing attackers to perform UI spoofing attacks. (CVE-2012-0460)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2012-12/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-13/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-14/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-15/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-16/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-17/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-18/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-19/

Solution

Upgrade to Firefox 10.0.3 ESR or later.

Risk Factor

High

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	52455
BID	52456
BID	52457
BID	52458
BID	52459
BID	52460
BID	52461
BID	52463
BID	52464
BID	52465
BID	52466
BID	52467
CVE	CVE-2012-0451
CVE	CVE-2012-0454
CVE	CVE-2012-0455
CVE	CVE-2012-0456
CVE	CVE-2012-0457
CVE	CVE-2012-0458
CVE	CVE-2012-0459
CVE	CVE-2012-0460
CVE	CVE-2012-0461
CVE	CVE-2012-0462
CVE	CVE-2012-0463
CVE	CVE-2012-0464
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725

XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2012/03/15, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 10.0.3 ESR
```

58897 - Firefox 10.0.x < 10.0.4 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The installed version of Firefox 10.0.x is potentially affected by the following security issues :

- An off-by-one error exists in the 'OpenType Sanitizer'

which can lead to out-bounds-reads and possible code execution. (CVE-2011-3062)

- Memory safety issues exist that could lead to arbitrary code execution. (CVE-2012-0467)

- A use-after-free error exists related to 'IDBKeyRange'

of 'indexedDB'. (CVE-2012-0469)

- Heap-corruption errors exist related to 'gfxImageSurface' that could lead to possible code execution. (CVE-2012-0470)

- A multi-octet encoding issue exists that could allow cross-site scripting attacks as certain octets in multibyte character sets can destroy following octets.

(CVE-2012-0471)

- An error exists related to font rendering with 'cairo- dwrite' that can cause memory corruption leading to crashes and potentially code execution. (CVE-2012-0472)

- An error exists in 'WebGLBuffer' that could lead to the reading of illegal video memory. (CVE-2012-0473)

- An unspecified error could allow URL bar spoofing.

(CVE-2012-0474)

- A decoding issue exists related to 'ISO-2022-KR' and 'ISO-2022-CN' character sets that could lead to cross-site scripting attacks. (CVE-2012-0477)

- An error exists related to 'WebGL' and 'texImage2D'

that could allow application crashes and possibly code execution when 'JSVAL_TO_OBJECT' is used on ordinary objects. (CVE-2012-0478)

- Address bar spoofing is possible when 'Atom XML' or 'RSS' data is loaded over HTTPS leading to phishing attacks. (CVE-2012-0479)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2012-20/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-22/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-23/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-24/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-25/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-26/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-27/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-29/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-30/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-31/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-33/

Solution

Upgrade to Firefox 10.0.4 ESR or later.

Risk Factor

High

VPR Score

8.8

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	53218
BID	53219
BID	53220
BID	53222
BID	53223
BID	53224
BID	53225
BID	53227
BID	53228
BID	53229
BID	53231
CVE	CVE-2011-3062
CVE	CVE-2012-0467
CVE	CVE-2012-0469
CVE	CVE-2012-0470
CVE	CVE-2012-0471
CVE	CVE-2012-0472

CVE	CVE-2012-0473
CVE	CVE-2012-0474
CVE	CVE-2012-0477
CVE	CVE-2012-0478
CVE	CVE-2012-0479
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2012/04/27, Modified: 2018/07/17

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 10.0.4 ESR
```

59408 - Firefox 10.0.x < 10.0.5 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The installed version of Firefox 10.0.x is potentially affected by the following security issues :

- An error exists in the ASN.1 decoder when handling zero length items that can lead to application crashes.
(CVE-2012-0441)

- Multiple memory corruption errors exist. (CVE-2012-1937, CVE-2012-1939)

- Two heap-based buffer overflows and one heap-based use- after-free error exist and are potentially exploitable.
(CVE-2012-1940, CVE-2012-1941, CVE-2012-1947)

- The inline-script blocking feature of the 'Content Security Policy' (CSP) does not properly block inline event handlers. This error allows remote attackers to more easily carry out cross-site scripting attacks.
(CVE-2012-1944)

- A use-after-free error exists related to replacing or inserting a node into a web document.
(CVE-2012-1946)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2012-34/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-36/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-38/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-39/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-40/

Solution

Upgrade to Firefox 10.0.5 ESR or later.

Risk Factor

High

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	53791
BID	53792
BID	53793
BID	53794
BID	53797
BID	53798
BID	53800
BID	53801
CVE	CVE-2012-0441
CVE	CVE-2012-1937
CVE	CVE-2012-1939
CVE	CVE-2012-1940
CVE	CVE-2012-1941
CVE	CVE-2012-1944
CVE	CVE-2012-1946
CVE	CVE-2012-1947
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2012/06/07, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 10.0.5 ESR
```

58005 - Firefox 10.x < 10.0.2 'png_decompress_chunk' Integer Overflow

Synopsis

The remote Windows host contains a web browser that is potentially affected by an integer overflow vulnerability.

Description

The installed version of Firefox 10.x is earlier than 10.0.2 and is, therefore, potentially affected by an integer overflow vulnerability.

An integer overflow error exists in 'libpng', a library used by this application. When decompressing certain PNG image files, this error can allow a heap-based buffer overflow which can crash the application or potentially allow code execution.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2012-11/

http://www.nessus.org/u?6846f277

Solution

Upgrade to Firefox 10.0.2 or later.

Risk Factor

High

VPR Score

6.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	52049
CVE	CVE-2011-3026

Plugin Information

Published: 2012/02/17, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 10.0.2 ESR
```

62588 - Firefox 10.x < 10.0.9 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The installed version of Firefox 10.x is potentially affected by the following security issues :

- An unspecified error exists that can allow attackers to bypass the 'Same Origin Policy' and access the 'Location' object. (CVE-2012-4192)

- An error exists related to 'security wrappers' and the function 'defaultValue()' that can allow cross-site scripting attacks. (CVE-2012-4193)

See Also

http://www.nessus.org/u?8993e6b4

http://www.nessus.org/u?dc43f3c3

https://www.mozilla.org/en-US/security/advisories/mfsa2012-89/

Solution

Upgrade to Firefox 10.0.9 ESR or later.

Risk Factor

High

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	56154
BID	56155
CVE	CVE-2012-4192
CVE	CVE-2012-4193

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2012/10/17, Modified: 2019/12/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 10.0.9 ESR
```

70947 - Firefox ESR < 17.0.11 Null_Cipher Code Execution

Synopsis

The remote Windows host contains a web browser that is potentially affected by a code execution vulnerability.

Description

The installed version of Firefox ESR is a version prior to 17.0.11, and is, therefore, potentially affected by a code execution vulnerability related to the function 'Null_Cipher' in the file 'ssl/ssl3con.c' and handling handshake packets.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2013-103/

http://www.nessus.org/u?cbfe91d6

https://developer.mozilla.org/en-US/docs/NSS/NSS_3.14.5_release_notes

Solution

Upgrade to Firefox ESR 17.0.11 or later.

Risk Factor

High

VPR Score

5.8

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	63737
CVE	CVE-2013-5605

Plugin Information

Published: 2013/11/18, Modified: 2019/11/27

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 17.0.11 ESR
```

86070 - Firefox ESR < 38.3 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The version of Firefox ESR installed on the remote Windows host is prior to 38.3. It is, therefore, affected by the following vulnerabilities :

- Multiple unspecified memory corruption issues exist due to improper validation of user-supplied input. A remote attacker can exploit these issues to corrupt memory and execute arbitrary code. (CVE-2015-4500)

- Multiple unspecified memory corruption issues exist due to improper validation of user-supplied input. A remote attacker can exploit these issues to corrupt memory and execute arbitrary code. (CVE-2015-4501)

- A flaw exists in the Mozilla updater that allows a local attacker to replace arbitrary files on the system, resulting in the execution of arbitrary code.

(CVE-2015-4505)

- A buffer overflow condition exists in the libvpx component when parsing vp9 format video. A remote attacker can exploit this, via a specially crafted vp9 format video, to execute arbitrary code. (CVE-2015-4506)

- A user-after-free error exists when manipulating HTML media elements on a page during script manipulation of the URI table of these elements. An attacker can exploit this to cause a denial of service condition.

(CVE-2015-4509)

- A buffer overflow condition exists in the nestegg library when decoding a WebM format video with maliciously formatted headers. An attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2015-4511)

- A memory corruption issue exists in NetworkUtils.cpp. An attacker can potentially exploit this issue to cause a denial of service condition or to execute arbitrary code. (CVE-2015-4517)

- An information disclosure vulnerability exists due to a flaw that occurs when a previously loaded image on a page is dropped into content after a redirect, resulting in the redirected URL being available to scripts.

(CVE-2015-4519)

- Multiple security bypass vulnerabilities exist due to errors in the handling of CORS preflight request headers. (CVE-2015-4520)

- A memory corruption issue exists in the ConvertDialogOptions() function. An attacker can potentially exploit this issue to cause a denial of service condition or to execute arbitrary code.

(CVE-2015-4521)

- An overflow condition exists in the GetMaxLength() function. An attacker can potentially exploit this to cause a denial of service condition or to execute arbitrary code. (CVE-2015-4522)

- An overflow condition exists in the GrowBy() function.

An attacker can potentially exploit this to cause a denial of service condition or to execute arbitrary code. (CVE-2015-7174)

- An overflow condition exists in the AddText() function.

An attacker can potentially exploit this to cause a denial of service condition or to execute arbitrary code. (CVE-2015-7175)

- A stack overflow condition exists in the AnimationThread() function due to a bad sscanf argument. An attacker can potentially exploit this to cause a denial of service condition or to execute arbitrary code. (CVE-2015-7176)

- A memory corruption issue exists in the InitTextures() function. An attacker can potentially exploit this issue to cause a denial of service condition or to execute arbitrary code. (CVE-2015-7177)

- An out-of-bounds memory error exists in the linkAttributes() function when manipulating shaders. An attacker can potentially exploit this issue to cause a denial of service condition or to execute arbitrary code. (CVE-2015-7178)

- An overflow condition exists in the reserveVertexSpace() function due to an insufficient allocation of memory for a shader attribute array. An attacker can potentially exploit this issue to cause a denial of service condition or to execute arbitrary code. (CVE-2015-7179)

- A memory corruption issue exists in ReadbackResultWriterD3D11::Run due to mishandling of the return status. An attacker can potentially exploit this issue to cause a denial of service condition or to execute arbitrary code. (CVE-2015-7180)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-96/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-100/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-101/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-105/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-106/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-110/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-111/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-112/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-113/

Solution

Upgrade to Firefox ESR 38.3 or later.

Risk Factor

High

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-4500
CVE	CVE-2015-4501
CVE	CVE-2015-4505
CVE	CVE-2015-4506
CVE	CVE-2015-4509
CVE	CVE-2015-4511
CVE	CVE-2015-4517
CVE	CVE-2015-4519
CVE	CVE-2015-4520
CVE	CVE-2015-4521
CVE	CVE-2015-4522
CVE	CVE-2015-7174
CVE	CVE-2015-7175
CVE	CVE-2015-7176
CVE	CVE-2015-7177
CVE	CVE-2015-7178
CVE	CVE-2015-7179
CVE	CVE-2015-7180

Plugin Information

Published: 2015/09/22, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 38.3 ESR
```

86763 - Firefox ESR < 38.4 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The version of Firefox ESR installed on the remote Windows host is prior to 38.4. It is, therefore, affected by the following vulnerabilities :

- Multiple memory corruption issues exist due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit these issues, via a specially crafted web page, to cause a denial of service condition or the execution of arbitrary code.

(CVE-2015-4513, CVE-2015-4514)

- An unspecified use-after-poison flaw exists in the sec_asn1d_parse_leaf() function in Mozilla Network Security Services (NSS) due to improper restriction of access to an unspecified data structure. A remote attacker can exploit this, via crafted OCTET STRING data, to cause a denial of service condition or the execution of arbitrary code. (CVE-2015-7181)

- A heap buffer overflow condition exists in the ASN.1 decoder in Mozilla Network Security Services (NSS) due to improper validation of user-supplied input. A remote attacker can exploit this, via crafted OCTET STRING data, to cause a denial of service condition or the execution of arbitrary code. (CVE-2015-7182)

- An integer overflow condition exists in the PL_ARENA_ALLOCATE macro in the Netscape Portable Runtime (NSPR) due to improper validation of user-supplied input. A remote attacker can exploit this to corrupt memory, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2015-7183)

- A same-origin bypass vulnerability exists due to improper handling of trailing whitespaces in the IP address hostname. A remote attacker can exploit this, by appending whitespace characters to an IP address string, to bypass the same-origin policy and conduct a cross-site scripting attack. (CVE-2015-7188)

- A race condition exists in the JPEGEncoder() function due to improper validation of user-supplied input when handling canvas elements. A remote attacker can exploit this to cause a heap-based buffer overflow, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2015-7189)

- A cross-origin resource sharing (CORS) request bypass vulnerability exists due to improper implementation of the CORS cross-origin request algorithm for the POST method in situations involving an unspecified Content-Type header manipulation. A remote attacker can exploit this to perform a simple request instead of a 'preflight' request. (CVE-2015-7193)

- A buffer underflow condition exists in libjar due to improper validation of user-supplied input when handling ZIP archives. A remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2015-7194)

- A memory corruption issue exists in the _releaseobject() function in dom/plugins/base/nsNPAPIPlugin.cpp due to improper deallocation of JavaScript wrappers. A remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code.

(CVE-2015-7196)

- A security bypass vulnerability exists due to improperly controlling the ability of a web worker to create a WebSocket object in the WebSocketImpl::Init() method.

A remote attacker can exploit this to bypass intended mixed-content restrictions. (CVE-2015-7197)

- A buffer overflow condition exists in TextureStorage11 in ANGLE due to improper validation of user-supplied input. A remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2015-7198)

- A flaw exists in the AddWeightedPathSegLists() function due to missing return value checks during SVG rendering.

A remote attacker can exploit this, via a crafted SVG document, to corrupt memory, resulting in a denial of service condition or the execution of arbitrary code.

(CVE-2015-7199)

- A flaw exists in the CryptoKey interface implementation due to missing status checks. A remote attacker can exploit this to make changes to cryptographic keys and execute arbitrary code. (CVE-2015-7200)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-116/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-122/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-123/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-127/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-128/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-130/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-131/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-132/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-133/

Solution

Upgrade to Firefox ESR 38.4 or later.

Risk Factor

High

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	77415
BID	77416
CVE	CVE-2015-4513
CVE	CVE-2015-4514
CVE	CVE-2015-7181
CVE	CVE-2015-7182
CVE	CVE-2015-7183
CVE	CVE-2015-7188
CVE	CVE-2015-7189
CVE	CVE-2015-7193
CVE	CVE-2015-7194
CVE	CVE-2015-7196
CVE	CVE-2015-7197
CVE	CVE-2015-7198
CVE	CVE-2015-7199
CVE	CVE-2015-7200

Plugin Information

Published: 2015/11/05, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 38.4 ESR
```

88753 - Firefox ESR < 38.6.1 Multiple Graphite 2 Library RCE

Synopsis

The remote Windows host contains a web browser that is affected by multiple remote code execution vulnerabilities.

Description

The version of Mozilla Firefox ESR installed on the remote Windows host is prior to 38.6.1. It is, therefore, affected by multiple remote code execution vulnerabilities in the Graphite 2 library :

- An overflow condition exists in the Context Item functionality due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via a crafted Graphite smart font, to cause a heap-based buffer overflow, resulting in a denial of service or the execution of arbitrary code.

(CVE-2016-1523)

- An out-of-bounds write error exists in the setAttr() function that is triggered when handling maliciously crafted fonts. An unauthenticated, remote attacker can exploit this to execute arbitrary code.
(CVE-2016-1969)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2016-14/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-38/

Solution

Upgrade to Mozilla Firefox ESR version 38.6.1 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

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

BID	82991
CVE	CVE-2016-1523
CVE	CVE-2016-1969
XREF	MFSA:2016-14
XREF	MFSA:2016-38

Plugin Information

Published: 2016/02/16, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 38.6.1 ESR
```

90791 - Firefox ESR < 38.8 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The version of Firefox ESR installed on the remote Windows host is prior to 38.8. It is, therefore, affected by multiple vulnerabilities :

- Multiple memory corruption issues exist that allow an attacker to corrupt memory, resulting in the execution of arbitrary code. (CVE-2016-2805, CVE-2016-2807)

- A flaw exists due to improper validation of user-supplied input when handling the 32-bit generation count of the underlying HashMap. A context-dependent attacker can exploit this to cause a buffer overflow condition, resulting in a denial of service or the execution of arbitrary code. (CVE-2016-2808)

- A heap buffer overflow condition exists in the Google Stagefright component due to improper validation of user-supplied input when handling CENC offsets and the sizes table. A context-dependent attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-2814)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2016-39/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-44/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-47/

Solution

Upgrade to Firefox ESR version 38.8 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

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

BID	88099
BID	88100
CVE	CVE-2016-2805
CVE	CVE-2016-2807
CVE	CVE-2016-2808
CVE	CVE-2016-2814
XREF	MFSA:2016-39
XREF	MFSA:2016-44
XREF	MFSA:2016-47

Plugin Information

Published: 2016/04/29, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 38.8 ESR
```

187795 - KB5034122: Windows 10 Version 21H2 / Windows 10 Version 22H2 Security Update (January 2024)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5034122. It is, therefore, affected by multiple vulnerabilities

- Microsoft ODBC Driver Remote Code Execution Vulnerability (CVE-2024-20654)

- BitLocker Security Feature Bypass Vulnerability (CVE-2024-20666)

- Windows Kerberos Security Feature Bypass Vulnerability (CVE-2024-20674)

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/5034122

Solution

Apply Security Update 5034122

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-35737
CVE	CVE-2024-20652
CVE	CVE-2024-20653
CVE	CVE-2024-20654
CVE	CVE-2024-20657
CVE	CVE-2024-20658
CVE	CVE-2024-20660
CVE	CVE-2024-20661
CVE	CVE-2024-20663
CVE	CVE-2024-20664
CVE	CVE-2024-20666
CVE	CVE-2024-20674
CVE	CVE-2024-20680
CVE	CVE-2024-20681
CVE	CVE-2024-20682
CVE	CVE-2024-20683
CVE	CVE-2024-20687
CVE	CVE-2024-20690
CVE	CVE-2024-20691
CVE	CVE-2024-20692
CVE	CVE-2024-20694
CVE	CVE-2024-20696
CVE	CVE-2024-20698
CVE	CVE-2024-20699
CVE	CVE-2024-20700
CVE	CVE-2024-21305
CVE	CVE-2024-21306
CVE	CVE-2024-21307
CVE	CVE-2024-21310
CVE	CVE-2024-21311
CVE	CVE-2024-21313
CVE	CVE-2024-21314
CVE	CVE-2024-21316
CVE	CVE-2024-21320

MSKB	5034122
XREF	MSFT:MS24-5034122
XREF	IAVA:2024-A-0015-S
XREF	IAVA:2024-A-0016-S

Plugin Information

Published: 2024/01/09, Modified: 2024/02/16

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5034122

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.19041.3803
    Should be      : 10.0.19041.3930
```

190468 - KB5034763: Windows 10 Version 21H2 / Windows 10 Version 22H2 Security Update (February 2024)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is missing security update 5034763. It is, therefore, affected by multiple vulnerabilities

- Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability (CVE-2024-21350, CVE-2024-21352, CVE-2024-21358, CVE-2024-21359, CVE-2024-21360, CVE-2024-21361, CVE-2024-21365, CVE-2024-21366, CVE-2024-21367, CVE-2024-21368, CVE-2024-21369, CVE-2024-21370, CVE-2024-21375, CVE-2024-21391, CVE-2024-21420)

- Windows Kernel Elevation of Privilege Vulnerability (CVE-2024-21338, CVE-2024-21371)

- Windows Kernel Information Disclosure Vulnerability (CVE-2024-21340)

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/5034763

Solution

Apply Security Update 5034763

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

9.0

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-2024-21304
CVE	CVE-2024-21338
CVE	CVE-2024-21339
CVE	CVE-2024-21340
CVE	CVE-2024-21341
CVE	CVE-2024-21343
CVE	CVE-2024-21344
CVE	CVE-2024-21347
CVE	CVE-2024-21348
CVE	CVE-2024-21349
CVE	CVE-2024-21350
CVE	CVE-2024-21351
CVE	CVE-2024-21352
CVE	CVE-2024-21354
CVE	CVE-2024-21355
CVE	CVE-2024-21356
CVE	CVE-2024-21357
CVE	CVE-2024-21358
CVE	CVE-2024-21359
CVE	CVE-2024-21360
CVE	CVE-2024-21361
CVE	CVE-2024-21362
CVE	CVE-2024-21363
CVE	CVE-2024-21365
CVE	CVE-2024-21366
CVE	CVE-2024-21367
CVE	CVE-2024-21368
CVE	CVE-2024-21369
CVE	CVE-2024-21370
CVE	CVE-2024-21371
CVE	CVE-2024-21372
CVE	CVE-2024-21375
CVE	CVE-2024-21377
CVE	CVE-2024-21391

CVE	CVE-2024-21405
CVE	CVE-2024-21406
CVE	CVE-2024-21412
CVE	CVE-2024-21420
MSKB	5034763
XREF	CISA-KNOWN-EXPLOITED:2024/03/05
XREF	MSFT:MS24-5034763
XREF	IAVA:2024-A-0092
XREF	IAVA:2024-A-0091

Plugin Information

Published: 2024/02/13, Modified: 2024/02/16

Plugin Output

tcp/445/cifs

```
The remote host is missing one of the following rollup KBs :
  - 5034763

  - C:\Windows\system32\ntoskrnl.exe has not been patched.
    Remote version : 10.0.19041.3803
    Should be      : 10.0.19041.4046
```

141430 - Microsoft 3D Viewer Base3D Code Execution (October 2020)

Synopsis

The Windows app installed on the remote host is affected by a code execution vulnerability.

Description

The Microsoft 3D Viewer app installed on the remote host is affected by a code execution vulnerability when the Base3D rendering engine improperly handles memory. An attacker who successfully exploited the vulnerability would gain execution on a victim system.

See Also

http://www.nessus.org/u?4a0fa39f

http://www.nessus.org/u?baf22b1a

https://www.zerodayinitiative.com/advisories/ZDI-20-1246/

Solution

Upgrade to app version 7.2009.29132.0 or later via the Microsoft Store.

Risk Factor

High

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

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-16918
CVE	CVE-2020-17003
XREF	ZDI:ZDI-20-1246
XREF	CEA-ID:CEA-2020-0126

Plugin Information

Published: 2020/10/13, Modified: 2024/02/15

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.Microsoft3DViewer_6.1908.2042.0_x64__8wekyb3d8bbwe
  Installed version : 6.1908.2042.0
  Fixed version     : 7.2009.29132.0
```

150352 - Microsoft 3D Viewer Multiple Vulnerabilities (June 2021)

Synopsis

The Windows app installed on the remote host is affected by multiple vulnerabilties.

Description

The Windows '3D Viewer' app installed on the remote host is affected by multiple vulnerabilities.

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2021-31942, CVE-2021-31943)

- An information disclosure vulnerability. An attacker can exploit this to disclose potentially sensitive information. (CVE-2021-31944)

See Also

http://www.nessus.org/u?e914ff80

http://www.nessus.org/u?5257edc0

http://www.nessus.org/u?bdd18cf9

Solution

Upgrade to app version 7.2105.4012.0, or later via the Microsoft Store.

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

7.4

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

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

References

CVE	CVE-2021-31942
CVE	CVE-2021-31943
CVE	CVE-2021-31944

Plugin Information

Published: 2021/06/08, Modified: 2023/12/27

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.Microsoft3DViewer_6.1908.2042.0_x64__8wekyb3d8bbwe
  Installed version : 6.1908.2042.0
  Fixed version     : 7.2105.4012.0
```

154988 - Microsoft 3D Viewer Multiple Vulnerabilities (November 2021)

Synopsis

The Windows app installed on the remote host is affected by multiple vulnerabilities.

Description

The version of the Microsoft 3D Viewer app installed on the remote host is prior to 7.2107.7012.0. It is, therefore, affected by multiple remote code execution vulnerabilities.

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43208

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43209

Solution

Upgrade to app version 7.2107.7012.0., or later via the Microsoft Store.

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

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-2021-43208
CVE	CVE-2021-43209

Plugin Information

Published: 2021/11/09, Modified: 2023/11/24

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.Microsoft3DViewer_6.1908.2042.0_x64__8wekyb3d8bbwe
  Installed version : 6.1908.2042.0
  Fixed version     : 7.2107.7012.0
```

181297 - Microsoft 3D Viewer app Multiple Remote Code Execution Vulnerabilities (September 2023)

Synopsis

The Microsoft 3D Viewer app installed on the remote host is affected by multiple remote code execution vulnerabilities.

Description

The version of the Microsoft 3D Viewer app installed on the remote Windows host is prior to 20.0.3.0. It is, therefore, affected by multiple unspecified remote code execution vulnerabilities:

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2023-36739, CVE-2023-36740, CVE-2023-36760)

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41303

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36739

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36740

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36760

Solution

Update to the latest Microsoft 3D Viewer app via the Windows App Store.

Risk Factor

High

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

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

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-41303
CVE	CVE-2023-36739
CVE	CVE-2023-36740
CVE	CVE-2023-36760

Plugin Information

Published: 2023/09/12, Modified: 2023/10/23

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.Microsoft3DViewer_6.1908.2042.0_x64__8wekyb3d8bbwe
  Installed version : 6.1908.2042.0
  Fixed version     : Update to the latest Microsoft 3D Viewer app via the Microsoft Store.
```

159465 - Microsoft Edge (Chromium) < 100.0.1185.29 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 100.0.1185.29. It is, therefore, affected by multiple vulnerabilities as referenced in the April 1, 2022 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-26891, CVE-2022-26894, CVE-2022-26895, CVE-2022-26900, CVE-2022-26908, CVE-2022-26909, CVE-2022-26912. (CVE-2022-24475)

- Microsoft Edge (Chromium-based) Spoofing Vulnerability. (CVE-2022-24523)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24475, CVE-2022-26894, CVE-2022-26895, CVE-2022-26900, CVE-2022-26908, CVE-2022-26909, CVE-2022-26912. (CVE-2022-26891)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24475, CVE-2022-26891, CVE-2022-26895, CVE-2022-26900, CVE-2022-26908, CVE-2022-26909, CVE-2022-26912. (CVE-2022-26894)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24475, CVE-2022-26891, CVE-2022-26894, CVE-2022-26900, CVE-2022-26908, CVE-2022-26909, CVE-2022-26912. (CVE-2022-26895)

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?471a8cda

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1125

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1127

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1128

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1129

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1130

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1131

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1133

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1134

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1135

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1136

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1137

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1138

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1139

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1143
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1145
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1146
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26894
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26895
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26900
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26908
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26909
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26912

Solution

Upgrade to Microsoft Edge version 100.0.1185.29 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

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

VPR Score

8.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-1125
CVE	CVE-2022-1127

CVE	CVE-2022-1128
CVE	CVE-2022-1129
CVE	CVE-2022-1130
CVE	CVE-2022-1131
CVE	CVE-2022-1133
CVE	CVE-2022-1134
CVE	CVE-2022-1135
CVE	CVE-2022-1136
CVE	CVE-2022-1137
CVE	CVE-2022-1138
CVE	CVE-2022-1139
CVE	CVE-2022-1143
CVE	CVE-2022-1145
CVE	CVE-2022-1146
CVE	CVE-2022-24475
CVE	CVE-2022-24523
CVE	CVE-2022-26891
CVE	CVE-2022-26894
CVE	CVE-2022-26895
CVE	CVE-2022-26900
CVE	CVE-2022-26908
CVE	CVE-2022-26909
CVE	CVE-2022-26912
XREF	IAVA:2021-A-0544-S

Plugin Information

Published: 2022/04/01, Modified: 2023/11/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 100.0.1185.29
```

159592 - Microsoft Edge (Chromium) < 100.0.1185.36 Vulnerability

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 100.0.1185.36. It is, therefore, affected by a vulnerability as referenced in the April 7, 2022 advisory.

- Type confusion in V8 in Google Chrome prior to 100.0.4896.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1232)

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?cc9eba61

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1232

Solution

Upgrade to Microsoft Edge version 100.0.1185.36 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

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-2022-1232
XREF	IAVA:2022-A-0133-S

Plugin Information

Published: 2022/04/07, Modified: 2023/11/02

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 100.0.1185.36
```

160319 - Microsoft Edge (Chromium) < 101.0.1210.32 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 101.0.1210.32. It is, therefore, affected by multiple vulnerabilities as referenced in the April 28, 2022 advisory.

- Use after free in Dev Tools in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via specific and direct user interaction. (CVE-2022-1493)

- Use after free in Vulkan in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1477)

- Use after free in SwiftShader in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1478)

- Use after free in ANGLE in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1479)

- Use after free in Sharing in Google Chrome on Mac prior to 101.0.4951.41 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1481)

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?436625dd

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1477

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1478

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1479

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1481

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1482

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1483

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1484

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1485

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1486

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1487

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1488

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1490

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1491

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1492

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1493
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1494
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1495
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1497
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1498
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1499
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1500
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1501
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29146
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29147

Solution

Upgrade to Microsoft Edge version 101.0.1210.32 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

8.1

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-2022-1477

CVE	CVE-2022-1478
CVE	CVE-2022-1479
CVE	CVE-2022-1481
CVE	CVE-2022-1482
CVE	CVE-2022-1483
CVE	CVE-2022-1484
CVE	CVE-2022-1485
CVE	CVE-2022-1486
CVE	CVE-2022-1487
CVE	CVE-2022-1488
CVE	CVE-2022-1490
CVE	CVE-2022-1491
CVE	CVE-2022-1492
CVE	CVE-2022-1493
CVE	CVE-2022-1494
CVE	CVE-2022-1495
CVE	CVE-2022-1497
CVE	CVE-2022-1498
CVE	CVE-2022-1499
CVE	CVE-2022-1500
CVE	CVE-2022-1501
CVE	CVE-2022-29146
CVE	CVE-2022-29147
XREF	IAVA:2022-A-0183-S

Plugin Information

Published: 2022/04/28, Modified: 2023/03/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 101.0.1210.32
```

161198 - Microsoft Edge (Chromium) < 101.0.1210.47 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 101.0.1210.47. It is, therefore, affected by multiple vulnerabilities as referenced in the May 13, 2022 advisory.

- Use after free in Sharing in Google Chrome prior to 101.0.4951.64 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1640)

- Use after free in Browser UI in Google Chrome prior to 101.0.4951.64 allowed a remote attacker who had convinced a user to engage in specific UI interaction to potentially exploit heap corruption via specific user interactions. (CVE-2022-1634)

- Use after free in Permission Prompts in Google Chrome prior to 101.0.4951.64 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via specific user interactions. (CVE-2022-1635)

- Use after free in Performance APIs in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1636)

- Inappropriate implementation in Web Contents in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (CVE-2022-1637)

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?3405acc7

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1634

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1635

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1636

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1637

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1638

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1639

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1640

Solution

Upgrade to Microsoft Edge version 101.0.1210.47 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

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-2022-1634
CVE	CVE-2022-1635
CVE	CVE-2022-1636
CVE	CVE-2022-1637
CVE	CVE-2022-1638
CVE	CVE-2022-1639
CVE	CVE-2022-1640

Plugin Information

Published: 2022/05/14, Modified: 2023/03/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 101.0.1210.47
```

161989 - Microsoft Edge (Chromium) < 102.0.1245.39 Vulnerability

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 102.0.1245.39. It is, therefore, affected by a vulnerability as referenced in the June 9, 2022 advisory.

- Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability. (CVE-2022-22021)

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?c8dc918f

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22021

Solution

Upgrade to Microsoft Edge version 102.0.1245.39 or later.

Risk Factor

Medium

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

9.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-22021

Plugin Information

Published: 2022/06/09, Modified: 2023/03/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 102.0.1245.39
```

162503 - Microsoft Edge (Chromium) < 103.0.1264.37 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 103.0.1264.37. It is, therefore, affected by multiple vulnerabilities as referenced in the June 23, 2022 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30192, CVE-2022-33638. (CVE-2022-33639)

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?2b2d4e0f

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2156

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2157

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2158

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2160

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2161

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2162

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2163

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2164

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2165

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30192

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-33638

Solution

Upgrade to Microsoft Edge version 103.0.1264.37 or later.

Risk Factor

Medium

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

9.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-33639

Plugin Information

Published: 2022/06/23, Modified: 2023/03/21

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 103.0.1264.37
```

162624 - Microsoft Edge (Chromium) < 103.0.1264.44 Vulnerability

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 103.0.1264.44. It is, therefore, affected by a vulnerability as referenced in the June 30, 2022 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-30192, CVE-2022-33638, CVE-2022-33639. (CVE-2022-33680)

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?83620a15

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-33680

Solution

Upgrade to Microsoft Edge version 103.0.1264.44 or later.

Risk Factor

Medium

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-33680

Plugin Information

Published: 2022/06/30, Modified: 2023/03/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 103.0.1264.44
```

162776 - Microsoft Edge (Chromium) < 103.0.1264.49 Vulnerability

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 103.0.1264.49. It is, therefore, affected by a vulnerability as referenced in the July 6, 2022 advisory.

- Heap buffer overflow in WebRTC in Google Chrome prior to 103.0.5060.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-2294)

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?c255ed38

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2294

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2295

Solution

Upgrade to Microsoft Edge version 103.0.1264.49 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

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

VPR Score

7.4

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-2022-2294
XREF	IAVA:2022-A-0262-S
XREF	CISA-KNOWN-EXPLOITED:2022/09/15

Plugin Information

Published: 2022/07/07, Modified: 2023/10/19

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 103.0.1264.49
```

163415 - Microsoft Edge (Chromium) < 103.0.1264.71 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 103.0.1264.71. It is, therefore, affected by multiple vulnerabilities as referenced in the July 22, 2022 advisory.

- : Use after free in Guest View. (CVE-2022-2477)

- : Use after free in PDF. (CVE-2022-2478)

- : Insufficient validation of untrusted input in File. (CVE-2022-2479)

- : Use after free in Service Worker API. (CVE-2022-2480)

- Use after free in Views. (CVE-2022-2481)

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?4d376e5a

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2477

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2478

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2479

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2480

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2481

Solution

Upgrade to Microsoft Edge version 103.0.1264.71 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

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-2022-2477
CVE	CVE-2022-2478
CVE	CVE-2022-2479
CVE	CVE-2022-2480
CVE	CVE-2022-2481

Plugin Information

Published: 2022/07/23, Modified: 2023/03/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 103.0.1264.71
```

164293 - Microsoft Edge (Chromium) < 104.0.1293.63 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 104.0.1293.63. It is, therefore, affected by multiple vulnerabilities as referenced in the August 19, 2022 advisory.

- Use after free in FedCM. (CVE-2022-2852)

- Heap buffer overflow in Downloads. (CVE-2022-2853)

- Use after free in SwiftShader. (CVE-2022-2854)

- Use after free in ANGLE. (CVE-2022-2855)

- Use after free in Blink. (CVE-2022-2857)

- Use after free in Sign-In Flow. (CVE-2022-2858)

- Insufficient policy enforcement in Cookies. (CVE-2022-2860)

- Inappropriate implementation in Extensions API. (CVE-2022-2861)

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?4ce23d54

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2852

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2853

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2854

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2855

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2857

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2858

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2860

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2861

Solution

Upgrade to Microsoft Edge version 104.0.1293.63 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

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-2022-2852
CVE	CVE-2022-2853
CVE	CVE-2022-2854
CVE	CVE-2022-2855
CVE	CVE-2022-2857
CVE	CVE-2022-2858
CVE	CVE-2022-2860
CVE	CVE-2022-2861

Plugin Information

Published: 2022/08/19, Modified: 2022/10/21

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 104.0.1293.63
```

164638 - Microsoft Edge (Chromium) < 105.0.1343.25 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 105.0.1343.25. It is, therefore, affected by multiple vulnerabilities as referenced in the September 1, 2022 advisory.

- Use after free in Network Service. (CVE-2022-3038)

- Use after free in WebSQL. (CVE-2022-3039, CVE-2022-3041)

- Use after free in Layout. (CVE-2022-3040)

- Inappropriate implementation in Site Isolation. (CVE-2022-3044)

- Insufficient validation of untrusted input in V8. (CVE-2022-3045)

- Use after free in Browser Tag. (CVE-2022-3046)

- Insufficient policy enforcement in Extensions API. (CVE-2022-3047)

- Inappropriate implementation in Pointer Lock. (CVE-2022-3053)

- Insufficient policy enforcement in DevTools. (CVE-2022-3054)

- Use after free in Passwords. (CVE-2022-3055)

- Insufficient policy enforcement in Content Security Policy. (CVE-2022-3056)

- Inappropriate implementation in iframe Sandbox. (CVE-2022-3057)

- Use after free in Sign-In Flow. (CVE-2022-3058)

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?31d28038

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3038

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3039

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3040

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3041

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3044

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3045

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3046

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3047

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3053
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3054
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3055
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3056
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3057
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3058
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38012

Solution

Upgrade to Microsoft Edge version 105.0.1343.25 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

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

VPR Score

8.1

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-2022-3038
CVE	CVE-2022-3039
CVE	CVE-2022-3040
CVE	CVE-2022-3041
CVE	CVE-2022-3044

CVE	CVE-2022-3045
CVE	CVE-2022-3046
CVE	CVE-2022-3047
CVE	CVE-2022-3053
CVE	CVE-2022-3054
CVE	CVE-2022-3055
CVE	CVE-2022-3056
CVE	CVE-2022-3057
CVE	CVE-2022-3058
CVE	CVE-2022-38012
XREF	IAVA:2022-A-0361-S
XREF	CISA-KNOWN-EXPLOITED:2023/04/20

Plugin Information

Published: 2022/09/02, Modified: 2023/10/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 105.0.1343.25
```

165210 - Microsoft Edge (Chromium) < 105.0.1343.42 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 105.0.1343.42. It is, therefore, affected by multiple vulnerabilities as referenced in the September 15, 2022 advisory.

- Out of bounds write in Storage. (CVE-2022-3195)

- Use after free in PDF. (CVE-2022-3196, CVE-2022-3197, CVE-2022-3198)

- Use after free in Frames. (CVE-2022-3199)

- Heap buffer overflow in Internals. (CVE-2022-3200)

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?e8ee04b1

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3195

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3196

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3197

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3198

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3199

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3200

Solution

Upgrade to Microsoft Edge version 105.0.1343.42 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

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-2022-3195
CVE	CVE-2022-3196
CVE	CVE-2022-3197
CVE	CVE-2022-3198
CVE	CVE-2022-3199
CVE	CVE-2022-3200
XREF	IAVA:2022-A-0379-S
XREF	IAVA:2022-A-0396-S

Plugin Information

Published: 2022/09/16, Modified: 2023/10/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 105.0.1343.42
```

165721 - Microsoft Edge (Chromium) < 106.0.1370.34 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 106.0.1370.34. It is, therefore, affected by multiple vulnerabilities as referenced in the October 3, 2022 advisory.

- Use after free in CSS. (CVE-2022-3304)

- Use after free in Media. (CVE-2022-3307)

- Insufficient policy enforcement in Developer Tools. (CVE-2022-3308)

- Insufficient policy enforcement in Custom Tabs. (CVE-2022-3310)

- Use after free in Import. (CVE-2022-3311)

- Incorrect security UI in Full Screen. (CVE-2022-3313)

- Type confusion in Blink. (CVE-2022-3315)

- Insufficient validation of untrusted input in Safe Browsing. (CVE-2022-3316)

- Insufficient validation of untrusted input in Intents. (CVE-2022-3317)

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?2c48e7f3
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3304
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3307
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3308
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3310
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3311
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3313
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3315
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3316
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3317
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41035

Solution

Upgrade to Microsoft Edge version 106.0.1370.34 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

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-2022-3370
CVE	CVE-2022-3373
XREF	IAVA:2022-A-0396-S

Plugin Information

Published: 2022/10/06, Modified: 2023/10/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 106.0.1370.34
```

166145 - Microsoft Edge (Chromium) < 106.0.1370.47 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 106.0.1370.47. It is, therefore, affected by multiple vulnerabilities as referenced in the October 14, 2022 advisory.

- Use after free in Skia. (CVE-2022-3445)

- Heap buffer overflow in WebSQL. (CVE-2022-3446)

- Inappropriate implementation in Custom Tabs. (CVE-2022-3447)

- Use after free in Safe Browsing. (CVE-2022-3449)

- Use after free in Peer Connection. (CVE-2022-3450)

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?e2630fd9

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3445

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3446

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3447

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3449

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3450

Solution

Upgrade to Microsoft Edge version 106.0.1370.47 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

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-2022-3445
CVE	CVE-2022-3446
CVE	CVE-2022-3447
CVE	CVE-2022-3449
CVE	CVE-2022-3450
XREF	IAVA:2022-A-0437-S

Plugin Information

Published: 2022/10/14, Modified: 2022/11/11

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 106.0.1370.47
```

166629 - Microsoft Edge (Chromium) < 107.0.1418.24 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 107.0.1418.24. It is, therefore, affected by multiple vulnerabilities as referenced in the October 27, 2022 advisory.

- Type Confusion in V8. (CVE-2022-3652)

- Heap buffer overflow in Vulkan. (CVE-2022-3653)

- Use after free in Layout. (CVE-2022-3654)

- Heap buffer overflow in Media Galleries. (CVE-2022-3655)

- Insufficient data validation in File System. (CVE-2022-3656)

- Use after free in Extensions. (CVE-2022-3657)

- Inappropriate implementation in Full screen mode. (CVE-2022-3660)

- Insufficient data validation in Extensions. (CVE-2022-3661)

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?57027261

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3652

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3653

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3654

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3655

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3656

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3657

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3660

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3661

Solution

Upgrade to Microsoft Edge version 107.0.1418.24 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

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-2022-3652
CVE	CVE-2022-3653
CVE	CVE-2022-3654
CVE	CVE-2022-3655
CVE	CVE-2022-3656
CVE	CVE-2022-3657
CVE	CVE-2022-3660
CVE	CVE-2022-3661
XREF	IAVA:2022-A-0446-S
XREF	IAVA:2022-A-0454-S

Plugin Information

Published: 2022/10/27, Modified: 2022/11/28

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Microsoft\Edge\Application
  Installed version : 92.0.902.67
```

```
    Fixed version     : 107.0.1418.24
```

166749 - Microsoft Edge (Chromium) < 107.0.1418.26 Vulnerability

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 107.0.1418.26. It is, therefore, affected by a vulnerability as referenced in the October 31, 2022 advisory.

- Type Confusion in V8. (CVE-2022-3723)

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?ff54e40b

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3723

Solution

Upgrade to Microsoft Edge version 107.0.1418.26 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

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

VPR Score

7.4

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-2022-3723
XREF	CISA-KNOWN-EXPLOITED:2022/11/18
XREF	IAVA:2022-A-0453-S

Plugin Information

Published: 2022/11/01, Modified: 2023/10/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 106.0.1370.61 (Extended Stable Channel) / 107.0.1418.26 (Stable Channel)
```

168406 - Microsoft Edge (Chromium) < 108.0.1462.41 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 108.0.1462.41. It is, therefore, affected by multiple vulnerabilities as referenced in the December 5, 2022 advisory.

- Type confusion in V8 in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4174)

- Use after free in Camera Capture in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4175)

- Use after free in Extensions in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install an extension to potentially exploit heap corruption via a crafted Chrome Extension and UI interaction. (Chromium security severity: High) (CVE-2022-4177)

- Use after free in Mojo in Google Chrome prior to 108.0.5359.71 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4178)

- Use after free in Audio in Google Chrome prior to 108.0.5359.71 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-2022-4179)

- Use after free in Mojo in Google Chrome prior to 108.0.5359.71 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-2022-4180)

- Use after free in Forms in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4181)

- Inappropriate implementation in Fenced Frames in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass fenced frame restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4182)

- Insufficient policy enforcement in Popup Blocker in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4183)

- Insufficient policy enforcement in Autofill in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass autofill restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4184)

- Inappropriate implementation in Navigation in Google Chrome on iOS prior to 108.0.5359.71 allowed a remote attacker to spoof the contents of the modal dialogue via a crafted HTML page. (Chromium security severity:

Medium) (CVE-2022-4185)

- Insufficient validation of untrusted input in Downloads in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install a malicious extension to bypass Downloads restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4186)

- Insufficient policy enforcement in DevTools in Google Chrome on Windows prior to 108.0.5359.71 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4187)

- Insufficient validation of untrusted input in CORS in Google Chrome on Android prior to 108.0.5359.71 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4188)

- Insufficient policy enforcement in DevTools in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium) (CVE-2022-4189)

- Insufficient data validation in Directory in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass file system restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4190)

- Use after free in Sign-In in Google Chrome prior to 108.0.5359.71 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via profile destruction. (Chromium security severity: Medium) (CVE-2022-4191)

- Use after free in Live Caption in Google Chrome prior to 108.0.5359.71 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via UI interaction. (Chromium security severity: Medium) (CVE-2022-4192)

- Insufficient policy enforcement in File System API in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass file system restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4193)

- Use after free in Accessibility in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4194)

- Insufficient policy enforcement in Safe Browsing in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass Safe Browsing warnings via a malicious file. (Chromium security severity: Medium) (CVE-2022-4195)

- Type confusion in V8 in Google Chrome prior to 108.0.5359.94 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4262)

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?26b297b9

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41115

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4174

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4175

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4177

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4178

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4179
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4180
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4181
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4182
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4183
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4184
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4185
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4186
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4187
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4188
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4189
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4190
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4191
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4192
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4193
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4194
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4195
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4262
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44688
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44708

Solution

Upgrade to Microsoft Edge version 108.0.1462.41 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

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

VPR Score

9.2

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-2022-4174
CVE	CVE-2022-4175
CVE	CVE-2022-4177
CVE	CVE-2022-4178
CVE	CVE-2022-4179
CVE	CVE-2022-4180
CVE	CVE-2022-4181
CVE	CVE-2022-4182
CVE	CVE-2022-4183
CVE	CVE-2022-4184
CVE	CVE-2022-4185
CVE	CVE-2022-4186
CVE	CVE-2022-4187
CVE	CVE-2022-4188
CVE	CVE-2022-4189
CVE	CVE-2022-4190
CVE	CVE-2022-4191
CVE	CVE-2022-4192
CVE	CVE-2022-4193
CVE	CVE-2022-4194
CVE	CVE-2022-4195
CVE	CVE-2022-4262
CVE	CVE-2022-41115
CVE	CVE-2022-44688
CVE	CVE-2022-44708
XREF	CISA-KNOWN-EXPLOITED:2022/12/26
XREF	IAVA:2022-A-0507-S
XREF	IAVA:2022-A-0510-S

Plugin Information

Published: 2022/12/05, Modified: 2023/09/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 108.0.1462.41
```

171333 - Microsoft Edge (Chromium) < 108.0.1462.42 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 108.0.1462.42. It is, therefore, affected by multiple vulnerabilities as referenced in the December 5, 2022 advisory.

- Type confusion in V8 in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4174)

- Use after free in Camera Capture in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4175)

- Use after free in Extensions in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install an extension to potentially exploit heap corruption via a crafted Chrome Extension and UI interaction. (Chromium security severity: High) (CVE-2022-4177)

- Use after free in Mojo in Google Chrome prior to 108.0.5359.71 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4178)

- Use after free in Audio in Google Chrome prior to 108.0.5359.71 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-2022-4179)

- Use after free in Mojo in Google Chrome prior to 108.0.5359.71 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-2022-4180)

- Use after free in Forms in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4181)

- Inappropriate implementation in Fenced Frames in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass fenced frame restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4182)

- Insufficient policy enforcement in Popup Blocker in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4183)

- Insufficient policy enforcement in Autofill in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass autofill restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4184)

- Inappropriate implementation in Navigation in Google Chrome on iOS prior to 108.0.5359.71 allowed a remote attacker to spoof the contents of the modal dialogue via a crafted HTML page. (Chromium security severity:

Medium) (CVE-2022-4185)

- Insufficient validation of untrusted input in Downloads in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install a malicious extension to bypass Downloads restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4186)

- Insufficient policy enforcement in DevTools in Google Chrome on Windows prior to 108.0.5359.71 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4187)

- Insufficient validation of untrusted input in CORS in Google Chrome on Android prior to 108.0.5359.71 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4188)

- Insufficient policy enforcement in DevTools in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium) (CVE-2022-4189)

- Insufficient data validation in Directory in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass file system restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4190)

- Use after free in Sign-In in Google Chrome prior to 108.0.5359.71 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via profile destruction. (Chromium security severity: Medium) (CVE-2022-4191)

- Use after free in Live Caption in Google Chrome prior to 108.0.5359.71 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via UI interaction. (Chromium security severity: Medium) (CVE-2022-4192)

- Insufficient policy enforcement in File System API in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass file system restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4193)

- Use after free in Accessibility in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4194)

- Insufficient policy enforcement in Safe Browsing in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to bypass Safe Browsing warnings via a malicious file. (Chromium security severity: Medium) (CVE-2022-4195)

- Type confusion in V8 in Google Chrome prior to 108.0.5359.94 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4262)

- Microsoft Edge (Chromium-based) Spoofing Vulnerability. (CVE-2022-44688)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. (CVE-2022-44708)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4174

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4175

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4177
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4178
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4179
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4180
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4181
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4182
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4183
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4184
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4185
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4186
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4187
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4188
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4189
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4190
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4191
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4192
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4193
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4194
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4195
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4262
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44688
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44708

Solution

Upgrade to Microsoft Edge version 108.0.1462.42 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

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

VPR Score

9.2

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)

References

CVE	CVE-2022-4174
CVE	CVE-2022-4175
CVE	CVE-2022-4177
CVE	CVE-2022-4178
CVE	CVE-2022-4179
CVE	CVE-2022-4180
CVE	CVE-2022-4181
CVE	CVE-2022-4182
CVE	CVE-2022-4183
CVE	CVE-2022-4184
CVE	CVE-2022-4185
CVE	CVE-2022-4186
CVE	CVE-2022-4187
CVE	CVE-2022-4188
CVE	CVE-2022-4189
CVE	CVE-2022-4190
CVE	CVE-2022-4191
CVE	CVE-2022-4192
CVE	CVE-2022-4193
CVE	CVE-2022-4194
CVE	CVE-2022-4195
CVE	CVE-2022-4262
CVE	CVE-2022-44688
CVE	CVE-2022-44708
XREF	CISA-KNOWN-EXPLOITED:2022/12/26

Plugin Information

Published: 2023/02/10, Modified: 2023/09/04

Plugin Output

tcp/445/cifs

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

```
  Installed version : 92.0.902.67
  Fixed version     : 108.0.1462.42
```

168877 - Microsoft Edge (Chromium) < 108.0.1462.54 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 108.0.1462.54. It is, therefore, affected by multiple vulnerabilities as referenced in the December 16, 2022 advisory.

- Use after free in Blink Media in Google Chrome prior to 108.0.5359.124 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4436)

- Use after free in Mojo IPC in Google Chrome prior to 108.0.5359.124 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4437)

- Use after free in Blink Frames in Google Chrome prior to 108.0.5359.124 allowed a remote attacker who convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2022-4438)

- Use after free in Aura in Google Chrome on Windows prior to 108.0.5359.124 allowed a remote attacker who convinced the user to engage in specific UI interactions to potentially exploit heap corruption via specific UI interactions. (Chromium security severity: High) (CVE-2022-4439)

- Use after free in Profiles in Google Chrome prior to 108.0.5359.124 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2022-4440)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4436

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4437

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4438

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4439

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-4440

Solution

Upgrade to Microsoft Edge version 108.0.1462.54 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

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-2022-4436
CVE	CVE-2022-4437
CVE	CVE-2022-4438
CVE	CVE-2022-4439
CVE	CVE-2022-4440
XREF	IAVA:2023-A-0003-S

Plugin Information

Published: 2022/12/16, Modified: 2023/02/10

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 108.0.1462.54
```

170725 - Microsoft Edge (Chromium) < 109.0.1343.27 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 109.0.1343.27. It is, therefore, affected by multiple vulnerabilities as referenced in the January 26, 2023 advisory.

- Use after free in WebTransport. (CVE-2023-0471)

- Use after free in WebRTC. (CVE-2023-0472)

- Type Confusion in ServiceWorker API. (CVE-2023-0473)

- Use after free in GuestView. (CVE-2023-0474)

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?a883970b

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0471

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0472

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0473

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0474

Solution

Upgrade to Microsoft Edge version 109.0.1343.27 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

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-2023-0471
CVE	CVE-2023-0472
CVE	CVE-2023-0473
CVE	CVE-2023-0474

Plugin Information

Published: 2023/01/27, Modified: 2023/02/07

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 109.0.1343.27
```

170007 - Microsoft Edge (Chromium) < 109.0.1518.49 / 108.0.1462.83 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 109.0.1518.49 / 108.0.1462.83. It is, therefore, affected by multiple vulnerabilities as referenced in the January 12, 2023 advisory.

- Heap buffer overflow in Network Service in Google Chrome prior to 109.0.5414.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page and specific interactions. (Chromium security severity: High) (CVE-2023-0129)

- Inappropriate implementation in in Fullscreen API in Google Chrome on Android prior to 109.0.5414.74 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.

(Chromium security severity: Medium) (CVE-2023-0130)

- Inappropriate implementation in in iframe Sandbox in Google Chrome prior to 109.0.5414.74 allowed a remote attacker to bypass file download restrictions via a crafted HTML page. (Chromium security severity:

Medium) (CVE-2023-0131)

- Inappropriate implementation in in Permission prompts in Google Chrome on Windows prior to 109.0.5414.74 allowed a remote attacker to force acceptance of a permission prompt via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-0132)

- Inappropriate implementation in in Permission prompts in Google Chrome on Android prior to 109.0.5414.74 allowed a remote attacker to bypass main origin permission delegation via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-0133)

- Use after free in Cart in Google Chrome prior to 109.0.5414.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via database corruption and a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-0134, CVE-2023-0135)

- Inappropriate implementation in in Fullscreen API in Google Chrome on Android prior to 109.0.5414.74 allowed a remote attacker to execute incorrect security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-0136)

- Heap buffer overflow in libphonenumber in Google Chrome prior to 109.0.5414.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-0138)

- Insufficient validation of untrusted input in Downloads in Google Chrome on Windows prior to 109.0.5414.74 allowed a remote attacker to bypass download restrictions via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-0139)

- Inappropriate implementation in in File System API in Google Chrome on Windows prior to 109.0.5414.74 allowed a remote attacker to bypass file system restrictions via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-0140)

- Insufficient policy enforcement in CORS in Google Chrome prior to 109.0.5414.74 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-0141)

- Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability. (CVE-2023-21775)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2023-21795. (CVE-2023-21796)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0129

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0130

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0131

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0132

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0133

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0134

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0135

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0136

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0138

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0139

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0140

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0141

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21775

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21796

Solution

Upgrade to Microsoft Edge version 109.0.1518.49 / 108.0.1462.83 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

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-2023-0129
CVE	CVE-2023-0130
CVE	CVE-2023-0131
CVE	CVE-2023-0132
CVE	CVE-2023-0133
CVE	CVE-2023-0134
CVE	CVE-2023-0135
CVE	CVE-2023-0136
CVE	CVE-2023-0138
CVE	CVE-2023-0139
CVE	CVE-2023-0140
CVE	CVE-2023-0141
XREF	IAVA:2023-A-0034-S
XREF	IAVA:2023-A-0029-S

Plugin Information

Published: 2023/01/13, Modified: 2023/10/24

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 109.0.1518.49
```

170783 - Microsoft Edge (Chromium) < 109.0.1518.52 Elevation of Privilege (CVE-2023-21795)

Synopsis

The remote host has an web browser installed that is affected by elevation of privilege.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 109.0.1518.52. It is, therefore, affected by a vulnerability as referenced in the January 13, 2023 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2023-21796. (CVE-2023-21795)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21795

Solution

Upgrade to Microsoft Edge version 109.0.1518.52 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

9.2

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-2023-21795
XREF	IAVA:2023-A-0034-S

Plugin Information

Published: 2023/01/30, Modified: 2023/02/10

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 109.0.1518.52
```

171332 - Microsoft Edge (Chromium) < 109.0.1518.70 / 108.0.1462.95 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 109.0.1518.70 / 108.0.1462.95. It is, therefore, affected by multiple vulnerabilities as referenced in the January 26, 2023 advisory.

- Use after free in WebTransport in Google Chrome prior to 109.0.5414.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0471)

- Use after free in WebRTC in Google Chrome prior to 109.0.5414.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0472)

- Type Confusion in ServiceWorker API in Google Chrome prior to 109.0.5414.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-0473)

- Use after free in GuestView in Google Chrome prior to 109.0.5414.119 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a Chrome web app.

(Chromium security severity: Medium) (CVE-2023-0474)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0471

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0472

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0473

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0474

Solution

Upgrade to Microsoft Edge version 109.0.1518.70 / 108.0.1462.95 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

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-2023-0471
CVE	CVE-2023-0472
CVE	CVE-2023-0473
CVE	CVE-2023-0474

Plugin Information

Published: 2023/02/10, Modified: 2023/02/10

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 109.0.1518.70
```

171268 - Microsoft Edge (Chromium) < 110.0.1587.41 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 110.0.1587.41. It is, therefore, affected by multiple vulnerabilities as referenced in the February 9, 2023 advisory.

- Type confusion in V8 in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0696)

- Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 110.0.5481.77 allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0697)

- Out of bounds read in WebRTC in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0698)

- Use after free in GPU in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page and browser shutdown. (Chromium security severity: Medium) (CVE-2023-0699)

- Inappropriate implementation in Download in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-0700)

- Heap buffer overflow in WebUI in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via UI interaction . (Chromium security severity: Medium) (CVE-2023-0701)

- Type confusion in Data Transfer in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-0702)

- Type confusion in DevTools in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via UI interactions.

(Chromium security severity: Medium) (CVE-2023-0703)

- Insufficient policy enforcement in DevTools in Google Chrome prior to 110.0.5481.77 allowed a remote attacker to bypass same origin policy and proxy settings via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-0704)

- Integer overflow in Core in Google Chrome prior to 110.0.5481.77 allowed a remote attacker who had one a race condition to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-0705)

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?245dfb65
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0696
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0697
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0698
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0699
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0700
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0701
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0702
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0703
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0704
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0705
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21794

Solution

Upgrade to Microsoft Edge version 110.0.1587.41 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

9.2

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-2023-0696
CVE	CVE-2023-0697
CVE	CVE-2023-0698
CVE	CVE-2023-0699
CVE	CVE-2023-0700
CVE	CVE-2023-0701
CVE	CVE-2023-0702
CVE	CVE-2023-0703
CVE	CVE-2023-0704
CVE	CVE-2023-0705
CVE	CVE-2023-21794
CVE	CVE-2023-23374
XREF	IAVA:2023-A-0074-S
XREF	IAVA:2023-A-0075-S

Plugin Information

Published: 2023/02/09, Modified: 2023/09/05

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 110.0.1587.41
```

171927 - Microsoft Edge (Chromium) < 110.0.1587.56 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 110.0.1587.56. It is, therefore, affected by multiple vulnerabilities as referenced in the February 25, 2023 advisory.

- Use after free in Web Payments API in Google Chrome on Android prior to 110.0.5481.177 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0927)

- Use after free in SwiftShader in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0928)

- Use after free in Vulkan in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0929)

- Heap buffer overflow in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0930)

- Use after free in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0931)

- Use after free in WebRTC in Google Chrome on Windows prior to 110.0.5481.177 allowed a remote attacker who convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-0932)

- Integer overflow in PDF in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium) (CVE-2023-0933)

- Use after free in Prompts in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) (CVE-2023-0941)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0927

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0928

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0929

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0930

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0931
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0932
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0933
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-0941

Solution

Upgrade to Microsoft Edge version 110.0.1587.56 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

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

VPR Score

6.7

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-2023-0927
CVE	CVE-2023-0928
CVE	CVE-2023-0929
CVE	CVE-2023-0930
CVE	CVE-2023-0931
CVE	CVE-2023-0932
CVE	CVE-2023-0933
CVE	CVE-2023-0941

XREF IAVA:2023-A-0119-S

Plugin Information

Published: 2023/02/27, Modified: 2023/05/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 110.0.1587.56
```

172572 - Microsoft Edge (Chromium) < 111.0.1661.41 / 110.0.1587.69 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 111.0.1661.41 / 110.0.1587.69. It is, therefore, affected by multiple vulnerabilities as referenced in the March 13, 2023 advisory.

- Use after free in Swiftshader in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1213)

- Type confusion in V8 in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1214)

- Type confusion in CSS in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1215)

- Use after free in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had convienced the user to engage in direct UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1216)

- Stack buffer overflow in Crash reporting in Google Chrome on Windows prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1217)

- Use after free in WebRTC in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1218)

- Heap buffer overflow in Metrics in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1219)

- Heap buffer overflow in UMA in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-1220)

- Insufficient policy enforcement in Extensions API in Google Chrome prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium) (CVE-2023-1221)

- Heap buffer overflow in Web Audio API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-1222)

- Insufficient policy enforcement in Autofill in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-1223)

- Insufficient policy enforcement in Web Payments API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity:

Medium) (CVE-2023-1224)

- Insufficient policy enforcement in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity:

Medium) (CVE-2023-1228)

- Inappropriate implementation in Permission prompts in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity:

Medium) (CVE-2023-1229)

- Inappropriate implementation in WebApp Installs in Google Chrome on Android prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious WebApp to spoof the contents of the PWA installer via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-1230)

- Inappropriate implementation in Autofill in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to potentially spoof the contents of the omnibox via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-1231)

- Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to obtain potentially sensitive information from API via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-1232)

- Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from API via a crafted Chrome Extension. (Chromium security severity: Low) (CVE-2023-1233)

- Inappropriate implementation in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-1234)

- Type confusion in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted UI interaction.

(Chromium security severity: Low) (CVE-2023-1235)

- Inappropriate implementation in Internals in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to spoof the origin of an iframe via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-1236)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1213

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1214

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1215

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1216

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1217

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1218

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1219

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1220

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1221
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1222
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1223
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1224
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1228
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1229
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1230
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1231
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1232
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1233
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1234
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1235
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1236

Solution

Upgrade to Microsoft Edge version 111.0.1661.41 / 110.0.1587.69 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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-1213
CVE	CVE-2023-1214
CVE	CVE-2023-1215
CVE	CVE-2023-1216
CVE	CVE-2023-1217
CVE	CVE-2023-1218
CVE	CVE-2023-1219
CVE	CVE-2023-1220
CVE	CVE-2023-1221
CVE	CVE-2023-1222
CVE	CVE-2023-1223
CVE	CVE-2023-1224
CVE	CVE-2023-1228
CVE	CVE-2023-1229
CVE	CVE-2023-1230
CVE	CVE-2023-1231
CVE	CVE-2023-1232
CVE	CVE-2023-1233
CVE	CVE-2023-1234
CVE	CVE-2023-1235
CVE	CVE-2023-1236
XREF	IAVA:2023-A-0131-S

Plugin Information

Published: 2023/03/15, Modified: 2023/10/24

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 111.0.1661.41
```

174524 - Microsoft Edge (Chromium) < 112.0.1722.48

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 112.0.1722.48. It is, therefore, affected by a vulnerability as referenced in the April 15, 2023 advisory.

- Type confusion in V8 in Google Chrome prior to 112.0.5615.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-2033)

- A spoofing vulnerability could allow an attacker to bypass the Edge security warning message feature. (CVE-2023-29334)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2033

Solution

Upgrade to Microsoft Edge version 112.0.1722.48 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

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

VPR Score

9.0

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-2033
CVE	CVE-2023-29334
XREF	IAVA:2023-A-0204-S
XREF	IAVA:2023-A-0203-S
XREF	IAVA:2023-A-0232-S
XREF	CISA-KNOWN-EXPLOITED:2023/05/08

Plugin Information

Published: 2023/04/20, Modified: 2023/07/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 109.0.1518.100
```

174883 - Microsoft Edge (Chromium) < 112.0.1722.58 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 112.0.1722.58. It is, therefore, affected by multiple vulnerabilities as referenced in the April 21, 2023 advisory.

- Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-2133, CVE-2023-2134)

- Use after free in DevTools in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who convinced a user to enable specific preconditions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-2135)

- Heap buffer overflow in sqlite in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-2137)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2133

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2134

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2135

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2137

Solution

Upgrade to Microsoft Edge version 112.0.1722.58 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

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-2023-2133
CVE	CVE-2023-2134
CVE	CVE-2023-2135
CVE	CVE-2023-2137
XREF	IAVA:2023-A-0223-S

Plugin Information

Published: 2023/04/27, Modified: 2023/10/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 112.0.1722.58
```

175396 - Microsoft Edge (Chromium) < 113.0.1774.35 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 113.0.1774.35. It is, therefore, affected by multiple vulnerabilities as referenced in the May 5, 2023 advisory.

- Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to bypass permission restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-2459)

- Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to bypass file access checks via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-2460)

- Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to obfuscate main origin data via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-2462)

- Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-2463)

- Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to perform an origin spoof in the security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-2464)

- Inappropriate implementation in CORS in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-2465)

- Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-2466)

- Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-2467)

- Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who had compromised the renderer process to obfuscate the security UI via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-2468)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability (CVE-2023-29350)

- Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability (CVE-2023-29354)

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?245dfb65
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2459
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2460
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2462
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2463
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2464
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2465
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2466
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2467
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2468
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29350
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29354

Solution

Upgrade to Microsoft Edge version 113.0.1774.35 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-2459
CVE	CVE-2023-2460
CVE	CVE-2023-2462
CVE	CVE-2023-2463
CVE	CVE-2023-2464
CVE	CVE-2023-2465
CVE	CVE-2023-2466
CVE	CVE-2023-2467
CVE	CVE-2023-2468
CVE	CVE-2023-29350
CVE	CVE-2023-29354
XREF	IAVA:2023-A-0240-S

Plugin Information

Published: 2023/05/11, Modified: 2023/07/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 113.0.1774.35
```

176230 - Microsoft Edge (Chromium) < 113.0.1774.50 / 112.0.1722.84 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 113.0.1774.50 / 112.0.1722.84. It is, therefore, affected by multiple vulnerabilities as referenced in the May 18, 2023 advisory.

- Use after free in Navigation in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) (CVE-2023-2721)

- Use after free in Autofill UI in Google Chrome on Android prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-2722)

- Use after free in DevTools in Google Chrome prior to 113.0.5672.126 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-2723)

- Type confusion in V8 in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-2724)

- Use after free in Guest View in Google Chrome prior to 113.0.5672.126 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: High) (CVE-2023-2725)

- Inappropriate implementation in WebApp Installs in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious web app to bypass install dialog via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-2726)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2721

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2722

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2723

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2724

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2725

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2726

Solution

Upgrade to Microsoft Edge version 113.0.1774.50 / 112.0.1722.84 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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-2721
CVE	CVE-2023-2722
CVE	CVE-2023-2723
CVE	CVE-2023-2724
CVE	CVE-2023-2725
CVE	CVE-2023-2726
XREF	IAVA:2023-A-0265-S

Plugin Information

Published: 2023/05/23, Modified: 2023/07/07

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 113.0.1774.50
```

179408 - Microsoft Edge (Chromium) < 114.0.1823.106 / 115.0.1901.200 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 114.0.1823.106 / 115.0.1901.200. It is, therefore, affected by multiple vulnerabilities as referenced in the August 7, 2023 advisory.

- Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability (CVE-2023-38157)

- Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4068, CVE-2023-4070)

- Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4069)

- Heap buffer overflow in Visuals in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4071)

- Out of bounds read and write in WebGL in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4072)

- Out of bounds memory access in ANGLE in Google Chrome on Mac prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity:

High) (CVE-2023-4073)

- Use after free in Blink Task Scheduling in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4074)

- Use after free in Cast in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4075)

- Use after free in WebRTC in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted WebRTC session. (Chromium security severity: High) (CVE-2023-4076)

- Insufficient data validation in Extensions in Google Chrome prior to 115.0.5790.170 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: Medium) (CVE-2023-4077)

- Inappropriate implementation in Extensions in Google Chrome prior to 115.0.5790.170 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: Medium) (CVE-2023-4078)

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?ccceaa60
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38157
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4068
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4069
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4070
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4071
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4072
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4073
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4074
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4075
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4076
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4077
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4078

Solution

Upgrade to Microsoft Edge version 114.0.1823.106 / 115.0.1901.200 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

9.0

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-2023-4068
CVE	CVE-2023-4069
CVE	CVE-2023-4070
CVE	CVE-2023-4071
CVE	CVE-2023-4072
CVE	CVE-2023-4073
CVE	CVE-2023-4074
CVE	CVE-2023-4075
CVE	CVE-2023-4076
CVE	CVE-2023-4077
CVE	CVE-2023-4078
CVE	CVE-2023-38157
XREF	IAVA:2023-A-0401-S

Plugin Information

Published: 2023/08/07, Modified: 2023/10/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 115.0.1901.200
```

176838 - Microsoft Edge (Chromium) < 114.0.1823.41 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 114.0.1823.41. It is, therefore, affected by multiple vulnerabilities as referenced in the June 6, 2023 advisory.

- Type confusion in V8 in Google Chrome prior to 114.0.5735.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-3079)

- An information disclosure vulnerability. (CVE-2023-33145)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33145

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3079

Solution

Upgrade to Microsoft Edge version 114.0.1823.41 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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-3079
CVE	CVE-2023-33145
XREF	CISA-KNOWN-EXPLOITED:2023/06/28
XREF	IAVA:2023-A-0274-S
XREF	IAVA:2023-A-0302-S

Plugin Information

Published: 2023/06/07, Modified: 2023/07/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 114.0.1823.41
```

177519 - Microsoft Edge (Chromium) < 114.0.1823.51 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 114.0.1823.51. It is, therefore, affected by multiple vulnerabilities as referenced in the June 15, 2023 advisory.

- Use after free in Autofill payments in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) (CVE-2023-3214)

- Use after free in WebRTC in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-3215)

- Type confusion in V8 in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-3216)

- Use after free in WebXR in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-3217)

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-2023-3214

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3215

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3216

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3217

http://www.nessus.org/u?a084dba4

Solution

Upgrade to Microsoft Edge version 114.0.1823.51 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

6.7

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-2023-3214
CVE	CVE-2023-3215
CVE	CVE-2023-3216
CVE	CVE-2023-3217

Plugin Information

Published: 2023/06/22, Modified: 2023/07/18

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 114.0.1823.51
```

177820 - Microsoft Edge (Chromium) < 114.0.1823.67 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 114.0.1823.67. It is, therefore, affected by multiple vulnerabilities as referenced in the June 29, 2023 advisory.

- Type Confusion in V8 in Google Chrome prior to 114.0.5735.198 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-3420)

- Use after free in Media in Google Chrome prior to 114.0.5735.198 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-3421)

- Use after free in Guest View in Google Chrome prior to 114.0.5735.198 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: High) (CVE-2023-3422)

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?12f91dd6

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3420

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3421

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3422

Solution

Upgrade to Microsoft Edge version 114.0.1823.67 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

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

VPR Score

8.4

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-2023-3420
CVE	CVE-2023-3421
CVE	CVE-2023-3422

Plugin Information

Published: 2023/06/30, Modified: 2023/07/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 114.0.1823.67
```

178285 - Microsoft Edge (Chromium) < 114.0.1823.82 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 114.0.1823.82. It is, therefore, affected by multiple vulnerabilities as referenced in the July 13, 2023 advisory.

- Microsoft Edge for Android (Chromium-based) Tampering Vulnerability (CVE-2023-36888)

- Microsoft Edge for iOS Spoofing Vulnerability (CVE-2023-36883)

- Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability (CVE-2023-36887)

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?74e8a4a1

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36883

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36887

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36888

Solution

Upgrade to Microsoft Edge version 114.0.1823.82 or later.

Risk Factor

High

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

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-36883
CVE	CVE-2023-36887
CVE	CVE-2023-36888
XREF	IAVA:2023-A-0358-S

Plugin Information

Published: 2023/07/14, Modified: 2023/08/02

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 114.0.1823.82
```

178727 - Microsoft Edge (Chromium) < 114.0.1901.183 / 115.0.1901.183 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 114.0.1901.183 / 115.0.1901.183. It is, therefore, affected by multiple vulnerabilities as referenced in the July 21, 2023 advisory.

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2023-35392)

- Microsoft Edge for Android Spoofing Vulnerability (CVE-2023-38173)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability (CVE-2023-38187)

- Use after free in WebRTC. (CVE-2023-3727, CVE-2023-3728)

- Use after free in Tab Groups. (CVE-2023-3730)

- Out of bounds memory access in Mojo. (CVE-2023-3732)

- Inappropriate implementation in WebApp Installs. (CVE-2023-3733)

- Inappropriate implementation in Picture In Picture. (CVE-2023-3734)

- Inappropriate implementation in Web API Permission Prompts. (CVE-2023-3735)

- Inappropriate implementation in Custom Tabs. (CVE-2023-3736)

- Inappropriate implementation in Notifications. (CVE-2023-3737)

- Inappropriate implementation in Autofill. (CVE-2023-3738)

- Insufficient validation of untrusted input in Themes. (CVE-2023-3740)

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?09d3506d

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35392

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3727

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3728

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3730

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3732

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3733

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3734

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3735

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3736
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3737
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3738
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3740
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38173
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38187

Solution

Upgrade to Microsoft Edge version 114.0.1901.183 / 115.0.1901.183 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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-3727
CVE	CVE-2023-3728
CVE	CVE-2023-3730
CVE	CVE-2023-3732
CVE	CVE-2023-3733
CVE	CVE-2023-3734

CVE	CVE-2023-3735
CVE	CVE-2023-3736
CVE	CVE-2023-3737
CVE	CVE-2023-3738
CVE	CVE-2023-3740
CVE	CVE-2023-35392
CVE	CVE-2023-38173
CVE	CVE-2023-38187
XREF	IAVA:2023-A-0380-S

Plugin Information

Published: 2023/07/21, Modified: 2023/08/11

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 115.0.1901.183
```

180040 - Microsoft Edge (Chromium) < 116.0.1938.54 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 116.0.1938.54. It is, therefore, affected by multiple vulnerabilities as referenced in the August 21, 2023 advisory.

- Use after free in Offline in Google Chrome on Android prior to 116.0.5845.96 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.

(Chromium security severity: High) (CVE-2023-2312)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability (CVE-2023-36787)

- Microsoft Edge (Chromium-based) Information Disclosure Vulnerability (CVE-2023-38158)

- Use after free in Device Trust Connectors in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity:

High) (CVE-2023-4349)

- Inappropriate implementation in Fullscreen in Google Chrome on Android prior to 116.0.5845.96 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page.

(Chromium security severity: High) (CVE-2023-4350)

- Use after free in Network in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who has elicited a browser shutdown to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4351)

- Type confusion in V8 in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4352)

- Heap buffer overflow in ANGLE in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4353)

- Heap buffer overflow in Skia in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4354)

- Out of bounds memory access in V8 in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4355)

- Use after free in Audio in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who has convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4356)

- Insufficient validation of untrusted input in XML in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4357)

- Use after free in DNS in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4358)

- Inappropriate implementation in App Launcher in Google Chrome on iOS prior to 116.0.5845.96 allowed a remote attacker to potentially spoof elements of the security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4359)

- Inappropriate implementation in Color in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4360)

- Inappropriate implementation in Autofill in Google Chrome on Android prior to 116.0.5845.96 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4361)

- Heap buffer overflow in Mojom IDL in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who had compromised the renderer process and gained control of a WebUI process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4362)

- Inappropriate implementation in WebShare in Google Chrome on Android prior to 116.0.5845.96 allowed a remote attacker to spoof the contents of a dialog URL via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4363)

- Inappropriate implementation in Permission Prompts in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4364)

- Inappropriate implementation in Fullscreen in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4365)

- Use after free in Extensions in Google Chrome prior to 116.0.5845.96 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-2023-4366)

- Insufficient policy enforcement in Extensions API in Google Chrome prior to 116.0.5845.96 allowed an attacker who convinced a user to install a malicious extension to bypass an enterprise policy via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4367, CVE-2023-4368)

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?9ae99e73

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-2312

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36787

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38158

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4349

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4350

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4351

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4352

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4353
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4354
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4355
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4356
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4357
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4358
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4359
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4360
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4361
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4362
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4363
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4364
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4365
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4366
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4367
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4368

Solution

Upgrade to Microsoft Edge version 116.0.1938.54 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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-2312
CVE	CVE-2023-4349
CVE	CVE-2023-4350
CVE	CVE-2023-4351
CVE	CVE-2023-4352
CVE	CVE-2023-4353
CVE	CVE-2023-4354
CVE	CVE-2023-4355
CVE	CVE-2023-4356
CVE	CVE-2023-4357
CVE	CVE-2023-4358
CVE	CVE-2023-4359
CVE	CVE-2023-4360
CVE	CVE-2023-4361
CVE	CVE-2023-4362
CVE	CVE-2023-4363
CVE	CVE-2023-4364
CVE	CVE-2023-4365
CVE	CVE-2023-4366
CVE	CVE-2023-4367
CVE	CVE-2023-4368
CVE	CVE-2023-36787
CVE	CVE-2023-38158
XREF	IAVA:2023-A-0438-S

Plugin Information

Published: 2023/08/23, Modified: 2023/09/18

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 116.0.1938.54
```

180197 - Microsoft Edge (Chromium) < 116.0.1938.62 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 116.0.1938.62. It is, therefore, affected by multiple vulnerabilities as referenced in the August 25, 2023 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability (CVE-2023-36741)

- Out of bounds memory access in V8 in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4427)

- Out of bounds memory access in CSS in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4428)

- Use after free in Loader in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4429)

- Use after free in Vulkan in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4430)

- Out of bounds memory access in Fonts in Google Chrome prior to 116.0.5845.110 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-4431)

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?22854207

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36741

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4427

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4428

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4429

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4430

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4431

Solution

Upgrade to Microsoft Edge version 116.0.1938.62 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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-4427
CVE	CVE-2023-4428
CVE	CVE-2023-4429
CVE	CVE-2023-4430
CVE	CVE-2023-4431
CVE	CVE-2023-36741
XREF	IAVA:2023-A-0453-S

Plugin Information

Published: 2023/08/26, Modified: 2023/10/06

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Microsoft\Edge\Application
  Installed version : 92.0.902.67
```

```
    Fixed version     : 116.0.1938.62
```

180416 - Microsoft Edge (Chromium) < 116.0.1938.69 (CVE-2023-4572)

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 116.0.1938.69. It is, therefore, affected by a vulnerability as referenced in the August 31, 2023 advisory.

- Use after free in MediaStream in Google Chrome prior to 116.0.5845.140 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4572)

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?3a086c3d

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4572

Solution

Upgrade to Microsoft Edge version 116.0.1938.69 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

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-2023-4572

Plugin Information

Published: 2023/08/31, Modified: 2023/09/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 116.0.1938.69
```

181128 - Microsoft Edge (Chromium) < 116.0.1938.76 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 116.0.1938.76. It is, therefore, affected by multiple vulnerabilities as referenced in the September 7, 2023 advisory.

- Out of bounds memory access in FedCM in Google Chrome prior to 116.0.5845.179 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory read via a crafted HTML page.

(Chromium security severity: High) (CVE-2023-4761)

- Type Confusion in V8 in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4762)

- Use after free in Networks in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4763)

- Incorrect security UI in BFCache in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: High) (CVE-2023-4764)

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?0c1fe891

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4761

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4762

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4763

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4764

Solution

Upgrade to Microsoft Edge version 116.0.1938.76 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

8.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-4761
CVE	CVE-2023-4762
CVE	CVE-2023-4763
CVE	CVE-2023-4764
XREF	IAVA:2023-A-0457-S
XREF	CISA-KNOWN-EXPLOITED:2024/02/27

Plugin Information

Published: 2023/09/07, Modified: 2024/02/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 116.0.1938.76
```

181314 - Microsoft Edge (Chromium) < 116.0.1938.81 (CVE-2023-4863)

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 116.0.1938.81. It is, therefore, affected by a vulnerability as referenced in the September 12, 2023 advisory.

- Heap buffer overflow in WebP in Google Chrome prior to 116.0.5845.187 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical) (CVE-2023-4863)

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?2bde7861

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-4863

Solution

Upgrade to Microsoft Edge version 116.0.1938.81 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

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

VPR Score

9.8

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-2023-4863
XREF	CISA-KNOWN-EXPLOITED:2023/10/04
XREF	IAVA:2023-A-0494-S

Plugin Information

Published: 2023/09/12, Modified: 2023/10/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 116.0.1938.81
```

182419 - Microsoft Edge (Chromium) < 116.0.1938.98 / 117.0.2045.47 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 116.0.1938.98 / 117.0.2045.47. It is, therefore, affected by multiple vulnerabilities as referenced in the September 29, 2023 advisory.

- There exists a use after free/double free in libwebp. An attacker can use the ApplyFiltersAndEncode() function and loop through to free best.bw and assign best = trial pointer. The second loop will then return 0 because of an Out of memory error in VP8 encoder, the pointer is still assigned to trial and the AddressSanitizer will attempt a double free. (CVE-2023-1999)

- Use after free in Passwords in Google Chrome prior to 117.0.5938.132 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: High) (CVE-2023-5186)

- Use after free in Extensions in Google Chrome prior to 117.0.5938.132 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: High) (CVE-2023-5187)

- Heap buffer overflow in vp8 encoding in libvpx in Google Chrome prior to 117.0.5938.132 and libvpx 1.13.1 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-5217)

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?f89fc291

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-1999

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5186

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5187

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5217

Solution

Upgrade to Microsoft Edge version 116.0.1938.98 / 117.0.2045.47 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

9.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-1999
CVE	CVE-2023-5186
CVE	CVE-2023-5187
CVE	CVE-2023-5217
XREF	CISA-KNOWN-EXPLOITED:2023/10/23
XREF	IAVA:2023-A-0523-S

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 117.0.2045.47
```

182556 - Microsoft Edge (Chromium) < 117.0.2045.55 (CVE-2023-5346)

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 117.0.2045.55. It is, therefore, affected by a vulnerability as referenced in the October 4, 2023 advisory.

- Type Confusion in V8. (CVE-2023-5346)

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?91471929

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5346

Solution

Upgrade to Microsoft Edge version 117.0.2045.55 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

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-2023-5346

Plugin Information

Published: 2023/10/04, Modified: 2023/10/09

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 117.0.2045.55
```

185436 - Microsoft Edge (Chromium) < 118.0.2088.102 / 119.0.2151.58 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 118.0.2088.102 / 119.0.2151.58. It is, therefore, affected by multiple vulnerabilities as referenced in the November 9, 2023 advisory.

- Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability (CVE-2023-36014)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability (CVE-2023-36024)

- Use after free in WebAudio in Google Chrome prior to 119.0.6045.123 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-5996)

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?683f1aad

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36014

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36024

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5996

Solution

Upgrade to Microsoft Edge version 118.0.2088.102 / 119.0.2151.58 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

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-2023-36014
CVE	CVE-2023-36024
CVE	CVE-2023-5996
XREF	IAVA:2023-A-0610-S

Plugin Information

Published: 2023/11/09, Modified: 2024/01/26

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 119.0.2151.58
```

185901 - Microsoft Edge (Chromium) < 118.0.2088.109 / 119.0.2151.72 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 118.0.2088.109 / 119.0.2151.72. It is, therefore, affected by multiple vulnerabilities as referenced in the November 16, 2023 advisory.

- Use after free in Garbage Collection in Google Chrome prior to 119.0.6045.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-5997)

- Use after free in Navigation in Google Chrome prior to 119.0.6045.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-6112)

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?7feca339

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36008

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36026

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5997

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6112

Solution

Upgrade to Microsoft Edge version 118.0.2088.109 / 119.0.2151.72 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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-5997
CVE	CVE-2023-6112
CVE	CVE-2023-36008
CVE	CVE-2023-36026
XREF	IAVA:2023-A-0649-S

Plugin Information

Published: 2023/11/16, Modified: 2024/01/29

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 119.0.2151.72
```

183055 - Microsoft Edge (Chromium) < 118.0.2088.46 Multiple Vulnerabilities

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 118.0.2088.46. It is, therefore, affected by multiple vulnerabilities as referenced in the October 13, 2023 advisory.

- Use after free in Site Isolation in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) (CVE-2023-5218)

- Use after free in Cast in Google Chrome prior to 118.0.5993.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-5473)

- Heap buffer overflow in PDF in Google Chrome prior to 118.0.5993.70 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium) (CVE-2023-5474)

- Inappropriate implementation in DevTools in Google Chrome prior to 118.0.5993.70 allowed an attacker who convinced a user to install a malicious extension to bypass discretionary access control via a crafted Chrome Extension. (Chromium security severity: Medium) (CVE-2023-5475)

- Use after free in Blink History in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-5476)

- Inappropriate implementation in Installer in Google Chrome prior to 118.0.5993.70 allowed a local attacker to bypass discretionary access control via a crafted command. (Chromium security severity: Low) (CVE-2023-5477)

- Inappropriate implementation in Autofill in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-5478)

- Inappropriate implementation in Extensions API in Google Chrome prior to 118.0.5993.70 allowed an attacker who convinced a user to install a malicious extension to bypass an enterprise policy via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-5479)

- Inappropriate implementation in Downloads in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-5481)

- Inappropriate implementation in Intents in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-5483)

- Inappropriate implementation in Navigation in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-5484)

- Inappropriate implementation in Autofill in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to bypass autofill restrictions via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-5485)

- Inappropriate implementation in Input in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-5486)

- Inappropriate implementation in Fullscreen in Google Chrome prior to 118.0.5993.70 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium) (CVE-2023-5487)

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?2945f274

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36409

Solution

Upgrade to Microsoft Edge version 118.0.2088.46 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

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-2023-5218
CVE	CVE-2023-5473
CVE	CVE-2023-5474
CVE	CVE-2023-5475
CVE	CVE-2023-5476
CVE	CVE-2023-5477
CVE	CVE-2023-5478
CVE	CVE-2023-5479
CVE	CVE-2023-5481
CVE	CVE-2023-5483
CVE	CVE-2023-5484
CVE	CVE-2023-5485
CVE	CVE-2023-5486
CVE	CVE-2023-5487
CVE	CVE-2023-36559
CVE	CVE-2023-36409
XREF	IAVA:2023-A-0566-S
XREF	IAVA:2023-A-0578-S

Plugin Information

Published: 2023/10/13, Modified: 2023/11/09

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 118.0.2088.46
```

183979 - Microsoft Edge (Chromium) < 118.0.2088.76 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 118.0.2088.76. It is, therefore, affected by multiple vulnerabilities as referenced in the October 27, 2023 advisory.

- Use after free in Profiles in Google Chrome prior to 118.0.5993.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-5472)

- Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. (CVE-2023-44323)

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?4f5c8cf8

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5472

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-44323

Solution

Upgrade to Microsoft Edge version 118.0.2088.76 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

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-2023-5472
CVE	CVE-2023-44323
XREF	IAVA:2023-A-0600-S

Plugin Information

Published: 2023/10/27, Modified: 2023/11/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 118.0.2088.76
```

184320 - Microsoft Edge (Chromium) < 118.0.2088.88 / 119.0.2151.44 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 118.0.2088.88 / 119.0.2151.44. It is, therefore, affected by multiple vulnerabilities as referenced in the November 2, 2023 advisory.

- Inappropriate implementation in Payments in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to bypass XSS preventions via a malicious file. (Chromium security severity: High) (CVE-2023-5480)

- Insufficient data validation in USB in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2023-5482)

- Integer overflow in USB in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2023-5849)

- Incorrect security UI in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Medium) (CVE-2023-5850)

- Inappropriate implementation in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-5851)

- Use after free in Printing in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium) (CVE-2023-5852)

- Incorrect security UI in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-5853)

- Use after free in Profiles in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium) (CVE-2023-5854)

- Use after free in Reading Mode in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium) (CVE-2023-5855)

- Use after free in Side Panel in Google Chrome prior to 119.0.6045.105 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-2023-5856)

- Inappropriate implementation in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially execute arbitrary code via a malicious file. (Chromium security severity: Medium) (CVE-2023-5857)

- Inappropriate implementation in WebApp Provider in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Low) (CVE-2023-5858)

- Incorrect security UI in Picture In Picture in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform domain spoofing via a crafted local HTML page. (Chromium security severity: Low) (CVE-2023-5859)

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?c1b5e0e7

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36022

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36029

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36034

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5480

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5482

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5849

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5850

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5851

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5852

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5853

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5854

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5855

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5856

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5857

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5858

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5859

Solution

Upgrade to Microsoft Edge version 118.0.2088.88 / 119.0.2151.44 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

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-2023-5480
CVE	CVE-2023-5482
CVE	CVE-2023-5849
CVE	CVE-2023-5850
CVE	CVE-2023-5851
CVE	CVE-2023-5852
CVE	CVE-2023-5853
CVE	CVE-2023-5854
CVE	CVE-2023-5855
CVE	CVE-2023-5856
CVE	CVE-2023-5857
CVE	CVE-2023-5858
CVE	CVE-2023-5859
CVE	CVE-2023-36022
CVE	CVE-2023-36029
CVE	CVE-2023-36034
XREF	IAVA:2023-A-0600-S

Plugin Information

Published: 2023/11/03, Modified: 2023/11/16

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Microsoft\Edge\Application
  Installed version : 92.0.902.67
```

```
    Fixed version     : 119.0.2151.44
```

187660 - Microsoft Edge (Chromium) < 120.0.2210.121 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 120.0.2210.121. It is, therefore, affected by multiple vulnerabilities as referenced in the January 5, 2024 advisory.

- Use after free in ANGLE in Google Chrome prior to 120.0.6099.199 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-0222)

- Heap buffer overflow in ANGLE in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-0223)

- Use after free in WebAudio in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-0224)

- Use after free in WebGPU in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-0225)

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?4aae3ac8

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0222

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0223

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0224

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0225

Solution

Upgrade to Microsoft Edge version 120.0.2210.121 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

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-2024-0222
CVE	CVE-2024-0223
CVE	CVE-2024-0224
CVE	CVE-2024-0225
XREF	IAVA:2024-A-0009-S

Plugin Information

Published: 2024/01/05, Modified: 2024/01/18

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 120.0.2210.121
```

189126 - Microsoft Edge (Chromium) < 120.0.2210.144 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 120.0.2210.144. It is, therefore, affected by multiple vulnerabilities as referenced in the January 17, 2024 advisory.

- Out of bounds write in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-0517)

- Type confusion in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-0518)

- Out of bounds memory access in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-0519)

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?baa12a23

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0517

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0518

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0519

Solution

Upgrade to Microsoft Edge version 120.0.2210.144 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

9.4

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-2024-0517
CVE	CVE-2024-0518
CVE	CVE-2024-0519
XREF	CISA-KNOWN-EXPLOITED:2024/02/07
XREF	IAVA:2024-A-0040-S

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 120.0.2210.144
```

186985 - Microsoft Edge (Chromium) < 120.0.2210.77 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 120.0.2210.77. It is, therefore, affected by multiple vulnerabilities as referenced in the December 14, 2023 advisory.

- Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability (CVE-2023-36878)

- Use after free in FedCM in Google Chrome prior to 120.0.6099.109 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page.

(Chromium security severity: High) (CVE-2023-6706)

- Use after free in CSS in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) (CVE-2023-6707)

- Type Confusion in V8. (CVE-2023-6702)

- Use after free in Blink. (CVE-2023-6703)

- Use after free in libavif. (CVE-2023-6704)

- Use after free in WebRTC. (CVE-2023-6705)

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?11cef5be

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36878

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6702

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6703

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6704

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6705

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6706

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-6707

Solution

Upgrade to Microsoft Edge version 120.0.2210.77 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

8.4

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-2023-6702
CVE	CVE-2023-6703
CVE	CVE-2023-6704
CVE	CVE-2023-6705
CVE	CVE-2023-6706
CVE	CVE-2023-6707
CVE	CVE-2023-36878
XREF	IAVA:2023-A-0696-S

Plugin Information

Published: 2023/12/15, Modified: 2024/01/12

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 120.0.2210.77
```

187184 - Microsoft Edge (Chromium) < 120.0.2210.91 (CVE-2023-7024)

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 120.0.2210.91. It is, therefore, affected by a vulnerability as referenced in the December 21, 2023 advisory.

- Heap buffer overflow in WebRTC. (CVE-2023-7024)

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?eaceba1a

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-7024

Solution

Upgrade to Microsoft Edge version 120.0.2210.91 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

9.2

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-2023-7024
XREF	CISA-KNOWN-EXPLOITED:2024/01/23

Plugin Information

Published: 2023/12/21, Modified: 2024/01/02

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 120.0.2210.91
```

191023 - Microsoft Edge (Chromium) < 122.0.2365.52 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 122.0.2365.52. It is, therefore, affected by multiple vulnerabilities as referenced in the February 23, 2024 advisory.

- Out of bounds memory access in Blink in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) (CVE-2024-1669)

- Use after free in Mojo in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-1670)

- Inappropriate implementation in Site Isolation in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-1671)

- Inappropriate implementation in Content Security Policy in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity:

Medium) (CVE-2024-1672)

- Use after free in Accessibility in Google Chrome prior to 122.0.6261.57 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via specific UI gestures.

(Chromium security severity: Medium) (CVE-2024-1673)

- Inappropriate implementation in Navigation in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-1674)

- Insufficient policy enforcement in Download in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. (Chromium security severity: Medium) (CVE-2024-1675)

- Inappropriate implementation in Navigation in Google Chrome prior to 122.0.6261.57 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Low) (CVE-2024-1676)

- Microsoft Edge (Chromium-based) Information Disclosure Vulnerability (CVE-2024-21423, CVE-2024-26192)

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2024-26188)

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?966a7e43

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1669

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1670
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1671
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1672
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1673
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1674
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1675
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1676
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21423
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26188
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26192

Solution

Upgrade to Microsoft Edge version 122.0.2365.52 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-1669

CVE	CVE-2024-1670
CVE	CVE-2024-1671
CVE	CVE-2024-1672
CVE	CVE-2024-1673
CVE	CVE-2024-1674
CVE	CVE-2024-1675
CVE	CVE-2024-1676
CVE	CVE-2024-21423
CVE	CVE-2024-26188
CVE	CVE-2024-26192
XREF	IAVA:2024-A-0116

Plugin Information

Published: 2024/02/26, Modified: 2024/03/01

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 122.0.2365.52
```

191442 - Microsoft Edge (Chromium) < 122.0.2365.63 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 122.0.2365.63. It is, therefore, affected by multiple vulnerabilities as referenced in the February 29, 2024 advisory.

- Type Confusion in V8 in Google Chrome prior to 122.0.6261.94 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-1938)

- Type Confusion in V8 in Google Chrome prior to 122.0.6261.94 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) (CVE-2024-1939)

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?2570be35

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1938

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1939

Solution

Upgrade to Microsoft Edge version 122.0.2365.63 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

6.7

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-2024-1938
CVE	CVE-2024-1939
XREF	IAVA:2024-A-0116

Plugin Information

Published: 2024/02/29, Modified: 2024/03/01

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 122.0.2365.63
```

152685 - Microsoft Edge (Chromium) < 92.0.902.78 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 92.0.902.78. It is, therefore, affected by multiple vulnerabilities as referenced in the August 19, 2021 advisory.

- Use after free in ANGLE in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-30604)

- Type confusion in V8 in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (CVE-2021-30598, CVE-2021-30599)

- Use after free in Extensions API in Google Chrome prior to 92.0.4515.159 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.

(CVE-2021-30601)

- Use after free in WebRTC in Google Chrome prior to 92.0.4515.159 allowed an attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page.

(CVE-2021-30602)

- Data race in WebAudio in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-30603)

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?97c3a98d

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30598

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30599

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30601

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30602

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30603

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30604

Solution

Upgrade to Microsoft Edge version 92.0.902.78 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

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

VPR Score

6.7

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

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

References

CVE	CVE-2021-30598
CVE	CVE-2021-30599
CVE	CVE-2021-30601
CVE	CVE-2021-30602
CVE	CVE-2021-30603
CVE	CVE-2021-30604

Plugin Information

Published: 2021/08/19, Modified: 2021/09/24

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 92.0.902.78
```

155601 - Microsoft Edge (Chromium) < 93.0.961.38 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 93.0.961.38. It is, therefore, affected by multiple vulnerabilities as referenced in the September 2, 2021 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-36930. (CVE-2021-26436)

- Microsoft Edge for Android Information Disclosure Vulnerability (CVE-2021-26439)

- Chromium: CVE-2021-30606 Use after free in Blink (CVE-2021-30606)

- Chromium: CVE-2021-30607 Use after free in Permissions (CVE-2021-30607)

- Chromium: CVE-2021-30608 Use after free in Web Share (CVE-2021-30608)

- Chromium: CVE-2021-30609 Use after free in Sign-In (CVE-2021-30609)

- Chromium: CVE-2021-30610 Use after free in Extensions API (CVE-2021-30610)

- Chromium: CVE-2021-30611 Use after free in WebRTC (CVE-2021-30611)

- Chromium: CVE-2021-30612 Use after free in WebRTC (CVE-2021-30612)

- Chromium: CVE-2021-30613 Use after free in Base internals (CVE-2021-30613)

- Chromium: CVE-2021-30614 Heap buffer overflow in TabStrip (CVE-2021-30614)

- Chromium: CVE-2021-30615 Cross-origin data leak in Navigation (CVE-2021-30615)

- Chromium: CVE-2021-30616 Use after free in Media (CVE-2021-30616)

- Chromium: CVE-2021-30617 Policy bypass in Blink (CVE-2021-30617)

- Chromium: CVE-2021-30618 Inappropriate implementation in DevTools (CVE-2021-30618)

- Chromium: CVE-2021-30619 UI Spoofing in Autofill (CVE-2021-30619)

- Chromium: CVE-2021-30620 Insufficient policy enforcement in Blink (CVE-2021-30620)

- Chromium: CVE-2021-30621 UI Spoofing in Autofill (CVE-2021-30621)

- Chromium: CVE-2021-30622 Use after free in WebApp Installs (CVE-2021-30622)

- Chromium: CVE-2021-30623 Use after free in Bookmarks (CVE-2021-30623)

- Chromium: CVE-2021-30624 Use after free in Autofill (CVE-2021-30624)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-26436. (CVE-2021-36930)

- Microsoft Edge for Android Spoofing Vulnerability (CVE-2021-38641)

- Microsoft Edge for iOS Spoofing Vulnerability (CVE-2021-38642)

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?eab98635
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26436
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26439
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30606
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30607
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30608
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30609
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30610
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30611
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30612
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30613
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30614
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30615
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30616
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30617
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30618
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30619
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30620
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30621
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30622
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30623
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30624
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36930
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38641
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38642

Solution

Upgrade to Microsoft Edge version 93.0.961.38 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

7.4

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)

STIG Severity

I

References

CVE	CVE-2021-26436
CVE	CVE-2021-26439
CVE	CVE-2021-30606
CVE	CVE-2021-30607
CVE	CVE-2021-30608
CVE	CVE-2021-30609
CVE	CVE-2021-30610
CVE	CVE-2021-30611
CVE	CVE-2021-30612
CVE	CVE-2021-30613
CVE	CVE-2021-30614
CVE	CVE-2021-30615
CVE	CVE-2021-30616
CVE	CVE-2021-30617
CVE	CVE-2021-30618
CVE	CVE-2021-30619
CVE	CVE-2021-30620
CVE	CVE-2021-30621
CVE	CVE-2021-30622
CVE	CVE-2021-30623
CVE	CVE-2021-30624
CVE	CVE-2021-36930

CVE	CVE-2021-38641
CVE	CVE-2021-38642
XREF	IAVA:2021-A-0401-S
XREF	IAVA:2021-A-0432-S

Plugin Information

Published: 2021/11/18, Modified: 2022/05/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 93.0.961.38
```

153369 - Microsoft Edge (Chromium) < 93.0.961.47 Vulnerability

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 93.0.961.47. It is, therefore, affected by a vulnerability as referenced in the September 14, 2021 advisory.

- Out of bounds write in V8 in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-30632)

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?78d37aa2

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30632

Solution

Upgrade to Microsoft Edge version 93.0.4577.82 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

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

VPR Score

8.9

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

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

References

CVE	CVE-2021-30632
XREF	CISA-KNOWN-EXPLOITED:2021/11/17

Plugin Information

Published: 2021/09/14, Modified: 2021/11/30

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 93.0.961.47
```

153839 - Microsoft Edge (Chromium) < 94.0.992.38 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 94.0.992.38. It is, therefore, affected by multiple vulnerabilities as referenced in the October 1, 2021 advisory.

- Use after free in V8 in Google Chrome prior to 94.0.4606.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-37975)

- Use after free in Safebrowsing in Google Chrome prior to 94.0.4606.71 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
(CVE-2021-37974)

- Inappropriate implementation in Memory in Google Chrome prior to 94.0.4606.71 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (CVE-2021-37976)

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?fc68e93b

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37974

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37975

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37976

Solution

Upgrade to Microsoft Edge version 94.0.992.38 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

7.4

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

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

STIG Severity

I

References

CVE	CVE-2021-37974
CVE	CVE-2021-37975
CVE	CVE-2021-37976
XREF	IAVA:2021-A-0449-S
XREF	CISA-KNOWN-EXPLOITED:2021/11/17

Plugin Information

Published: 2021/10/01, Modified: 2023/04/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 94.0.992.38
```

153995 - Microsoft Edge (Chromium) < 94.0.992.47 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 94.0.992.47. It is, therefore, affected by multiple vulnerabilities as referenced in the October 11, 2021 advisory.

- heap buffer overflow in WebRTC in Google Chrome prior to 94.0.4606.81 allowed a remote attacker who convinced a user to browse to a malicious website to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-37979)

- Use after free in Garbage Collection in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-37977)

- Heap buffer overflow in Blink in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-37978)

- Inappropriate implementation in Sandbox in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially bypass site isolation via Windows. (CVE-2021-37980)

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?3a3f355a

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37977

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37978

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37979

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-37980

Solution

Upgrade to Microsoft Edge version 94.0.992.47 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

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

VPR Score

6.7

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

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

STIG Severity

I

References

CVE	CVE-2021-37977
CVE	CVE-2021-37978
CVE	CVE-2021-37979
CVE	CVE-2021-37980
XREF	IAVA:2021-A-0459-S

Plugin Information

Published: 2021/10/11, Modified: 2023/11/28

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 94.0.992.47
```

156011 - Microsoft Edge (Chromium) < 96.0.1054.53 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 96.0.1054.53. It is, therefore, affected by multiple vulnerabilities as referenced in the December 10, 2021 advisory.

- Use after free in window manager in Google Chrome on ChromeOS prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-4067)

- Use after free in web apps in Google Chrome prior to 96.0.4664.93 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (CVE-2021-4052)

- Use after free in UI in Google Chrome on Linux prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-4053)

- Incorrect security UI in autofill in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (CVE-2021-4054)

- Heap buffer overflow in extensions in Google Chrome prior to 96.0.4664.93 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (CVE-2021-4055)

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?10871512

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4052

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4053

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4054

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4055

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4056

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4057

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4058

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4059

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4061

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4062

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4063

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4064

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4065

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4066
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4067
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4068

Solution

Upgrade to Microsoft Edge version 96.0.1054.53 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

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

VPR Score

6.7

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

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

References

CVE	CVE-2021-4052
CVE	CVE-2021-4053
CVE	CVE-2021-4054
CVE	CVE-2021-4055
CVE	CVE-2021-4056
CVE	CVE-2021-4057
CVE	CVE-2021-4058
CVE	CVE-2021-4059
CVE	CVE-2021-4061
CVE	CVE-2021-4062
CVE	CVE-2021-4063
CVE	CVE-2021-4064
CVE	CVE-2021-4065

CVE	CVE-2021-4066
CVE	CVE-2021-4067
CVE	CVE-2021-4068

Plugin Information

Published: 2021/12/11, Modified: 2022/01/11

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 96.0.1054.53
```

156077 - Microsoft Edge (Chromium) < 96.0.1054.57 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 96.0.1054.57. It is, therefore, affected by multiple vulnerabilities as referenced in the December 14, 2021 advisory.

- Use after free in V8 in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-4102)

- Insufficient data validation in Mojo in Google Chrome prior to 96.0.4664.110 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

(CVE-2021-4098)

- Use after free in Swiftshader in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-4099)

- Object lifecycle issue in ANGLE in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-4100)

- Heap buffer overflow in Swiftshader in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2021-4101)

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?f5dd1e14

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4098

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4099

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4100

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4101

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-4102

Solution

Upgrade to Microsoft Edge version 96.0.1054.57 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

7.4

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

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

STIG Severity

I

References

CVE	CVE-2021-4098
CVE	CVE-2021-4099
CVE	CVE-2021-4100
CVE	CVE-2021-4101
CVE	CVE-2021-4102
XREF	CISA-KNOWN-EXPLOITED:2021/12/29
XREF	IAVA:2021-A-0576-S

Plugin Information

Published: 2021/12/14, Modified: 2023/04/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 96.0.1054.57
```

157369 - Microsoft Edge (Chromium) < 98.0.1108.43 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 98.0.1108.43. It is, therefore, affected by multiple vulnerabilities as referenced in the February 3, 2022 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23262. (CVE-2022-23263)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23263. (CVE-2022-23262)

- Microsoft Edge (Chromium-based) Tampering Vulnerability. (CVE-2022-23261)

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?c8cf985b

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23261

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23262

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23263

Solution

Upgrade to Microsoft Edge version 98.0.1108.43 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.1

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-2022-23261
CVE	CVE-2022-23262
CVE	CVE-2022-23263

Plugin Information

Published: 2022/02/03, Modified: 2022/05/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 98.0.1108.43
```

158097 - Microsoft Edge (Chromium) < 98.0.1108.55 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 98.0.1108.55. It is, therefore, affected by multiple vulnerabilities as referenced in the February 16, 2022 advisory.

- Inappropriate implementation in Gamepad API in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-0610)

- Use after free in File Manager in Google Chrome on Chrome OS prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-0603)

- Heap buffer overflow in Tab Groups in Google Chrome prior to 98.0.4758.102 allowed an attacker who convinced a user to install a malicious extension and engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-0604)

- Use after free in Webstore API in Google Chrome prior to 98.0.4758.102 allowed an attacker who convinced a user to install a malicious extension and convinced a user to enage in specific user interaction to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-0605)

- Use after free in ANGLE in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-0606)

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?e17239f6

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0603

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0604

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0605

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0606

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0607

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0608

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0609

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0610

Solution

Upgrade to Microsoft Edge version 98.0.1108.55 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

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

VPR Score

9.0

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

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

STIG Severity

I

References

CVE	CVE-2022-0603
CVE	CVE-2022-0604
CVE	CVE-2022-0605
CVE	CVE-2022-0606
CVE	CVE-2022-0607
CVE	CVE-2022-0608
CVE	CVE-2022-0609
CVE	CVE-2022-0610
XREF	CISA-KNOWN-EXPLOITED:2022/03/01
XREF	IAVA:2022-A-0086-S

Plugin Information

Published: 2022/02/16, Modified: 2022/05/03

Plugin Output

tcp/445/cifs

```
    Path              : C:\Program Files (x86)\Microsoft\Edge\Application
    Installed version : 92.0.902.67
    Fixed version     : 98.0.1108.55
```

159239 - Microsoft Edge (Chromium) < 99.0.1150.55 Vulnerability

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 99.0.1150.55. It is, therefore, affected by a vulnerability as referenced in the March 26, 2022 advisory.

- Type confusion in V8 in Google Chrome prior to 99.0.4844.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (CVE-2022-1096)

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?991726b8

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-1096

Solution

Upgrade to Microsoft Edge version 99.0.1150.55 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

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-2022-1096
XREF	CISA-KNOWN-EXPLOITED:2022/04/18
XREF	IAVA:2022-A-0126-S
XREF	IAVA:2021-A-0544-S

Plugin Information

Published: 2022/03/26, Modified: 2023/11/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 99.0.1150.55
```

178245 - Microsoft Paint 3D Code Execution (July 2023)

Synopsis

The Windows app installed on the remote host is affected by code execution vulnerabilities.

Description

The Windows 'Paint 3D' app installed on the remote host is affected by multiple code execution vulnerabilities. An attacker who successfully exploited one of the vulnerabilities could execute arbitrary code. Exploitation of the vulnerabilities requires that a program process a specially crafted file.

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-2023-32047

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35374

Solution

Upgrade to app version 6.2305.16087.0, or later via the Microsoft Store.

Risk Factor

High

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

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-32047
CVE	CVE-2023-35374

Plugin Information

Published: 2023/07/13, Modified: 2023/07/14

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.MSPaint_6.1907.29027.0_x64__8wekyb3d8bbwe
  Installed version : 6.1907.29027.0
  Fixed version     : 6.2305.16087.0
```

158710 - Microsoft Paint 3D Code Execution (March 2022)

Synopsis

The Windows app installed on the remote host is affected by a code execution vulnerability..

Description

The Windows 'Paint 3D' app installed on the remote host is affected by a code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23282

Solution

Upgrade to app version 6.2105.4017.0, or later via the Microsoft Store.

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

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

VPR Score

6.7

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-2022-23282

Plugin Information

Published: 2022/03/08, Modified: 2022/03/09

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.MSPaint_6.1907.29027.0_x64__8wekyb3d8bbwe
  Installed version : 6.1907.29027.0
  Fixed version     : 6.2105.4017.0
```

150373 - Microsoft Paint 3D Multiple Vulnerabilities (June 2021)

Synopsis

The Windows app installed on the remote host is affected by multiple vulnerabilities.

Description

The Windows 'Paint 3D' app installed on the remote host is affected by multiple remote code execution vulnerabilities. An attacker can exploit these to bypass authentication and execute unauthorized arbitrary commands.

See Also

http://www.nessus.org/u?941966fe

http://www.nessus.org/u?a40919a7

http://www.nessus.org/u?99b641c8

Solution

Upgrade to app version 6.2105.4017.0, or later via the Microsoft Store.

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

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-2021-31945
CVE	CVE-2021-31946
CVE	CVE-2021-31983

Plugin Information

Published: 2021/06/08, Modified: 2023/12/27

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.MSPaint_6.1907.29027.0_x64__8wekyb3d8bbwe
  Installed version : 6.1907.29027.0
  Fixed version     : 6.2105.4017.0
```

140132 - Microsoft Windows Defender Elevation of Privilege Vulnerability (CVE-2020-1163 & CVE-2020-1170)

Synopsis

An antimalware application installed on the remote host is affected by an elevation of privilege vulnerability.

Description

The version of Microsoft Windows Defender component MpCmdRun.exe installed on the remote Windows host is prior to 4.18.2005.1. It is, therefore, affected by a elevation of privilege vulnerability which could allow an attacker who successfully exploited this vulnerability to elevate privileges on the system.

See Also

http://www.nessus.org/u?949ab302

http://www.nessus.org/u?32b38eb5

Solution

Enable automatic updates to update the scan engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

Risk Factor

High

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

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2020-1163
CVE	CVE-2020-1170
XREF	IAVA:2019-A-0294
XREF	CWE:269

Plugin Information

Published: 2020/09/02, Modified: 2024/02/22

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 4.18.1909.6
Fixed version     : 4.18.2005.1
```

158708 - Microsoft Windows HEIF Image Extensions RCE (March 2022)

Synopsis

The Windows app installed on the remote host is affected by a remote code execution vulnerability.

Description

The Windows HEIF Image Extension app installed on the remote host is affected by a remote code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24457

Solution

Upgrade to app version 1.0.43012.0 or later via the Microsoft Store.

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

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

VPR Score

6.7

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-2022-24457

Plugin Information

Published: 2022/03/08, Modified: 2022/03/09

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.HEIFImageExtension_1.0.22742.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22742.0
  Fixed version     : 1.0.43012.0
```

158706 - Microsoft Windows VP9 Video Extensions Library Multiple Vulnerabilities (March 2022)

Synopsis

The Windows app installed on the remote host is affected by a multiple code execution vulnerabilities.

Description

The Windows 'VP9 Extensions' app installed on the remote host is affected by multiple code execution vulnerabilities. An attacker who successfully exploited the vulnerabilities could execute arbitrary code. Exploitation of the vulnerabilities require that a program process a specially crafted file.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24451

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24501

Solution

Upgrade to app version 1.0.42791.0, or later via the Microsoft Store.

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

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

VPR Score

6.7

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-2022-24451

CVE CVE-2022-24501

Plugin Information

Published: 2022/03/08, Modified: 2023/11/06

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22681.0
  Fixed version     : 1.0.42791.0
```

148484 - Microsoft Windows VP9 Video Extensions Library RCE (April 2021)

Synopsis

The Windows app installed on the remote host is affected by a remote code execution vulnerability.

Description

The Windows 'VP9 Extensions' app installed on the remote host is affected by a remote code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

See Also

http://www.nessus.org/u?4bb22046

Solution

Upgrade to app version 1.0.40631.0, or later via the Microsoft Store.

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

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

VPR Score

6.7

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-2021-28464

Plugin Information

Published: 2021/04/13, Modified: 2021/04/13

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22681.0
  Fixed version     : 1.0.40631.0
```

157438 - Microsoft Windows VP9 Video Extensions Library RCE (February 2022)

Synopsis

The Windows app installed on the remote host is affected by a remote code execution vulnerability.

Description

The Windows 'VP9 Extensions' app installed on the remote host is affected by a remote code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

See Also

http://www.nessus.org/u?0c177c5b

Solution

Upgrade to app version 1.0.42791.0, or later via the Microsoft Store.

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

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

VPR Score

6.7

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-2022-22709

Plugin Information

Published: 2022/02/08, Modified: 2022/02/09

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22681.0
  Fixed version     : 1.0.42791.0
```

150355 - Microsoft Windows VP9 Video Extensions Library RCE (June 2021)

Synopsis

The Windows app installed on the remote host is affected by a remote code execution vulnerability.

Description

The Windows 'VP9 Extensions' app installed on the remote host is affected by a remote code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file.

See Also

http://www.nessus.org/u?af8af611

Solution

Upgrade to app version 1.0.41182.0, or later via the Microsoft Store.

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

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-2021-31967

Plugin Information

Published: 2021/06/08, Modified: 2023/12/27

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22681.0
  Fixed version     : 1.0.41182.0
```

149388 - Microsoft Windows Web Media Extensions Library RCE (May 2021)

Synopsis

The Windows app installed on the remote host is affected by a remote code execution vulnerability.

Description

The Windows 'Web Media Extensions' app installed on the remote host is affected by a remote code execution vulnerability. An attacker who successfully exploited the vulnerability could execute arbitrary code. Exploitation of the vulnerability requires that a program process a specially crafted file. (CVE-2021-28465)

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28465

Solution

Upgrade to app version 1.0.40831.0, or later via the Microsoft Store.

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

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-2021-28465

Plugin Information

Published: 2021/05/11, Modified: 2024/01/02

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.WebMediaExtensions_1.0.20875.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.20875.0
  Fixed version     : 1.0.40831.0
```

122194 - Mozilla Firefox ESR < 60.5.1

Synopsis

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

Description

The version of Firefox ESR installed on the remote Windows host is prior to 60.5.1. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2019-05 advisory.

- A use-after-free vulnerability in the Skia library can occur when creating a path, leading to a potentially exploitable crash. (CVE-2018-18356)

- An integer overflow vulnerability in the Skia library can occur after specific transform operations, leading to a potentially exploitable crash. (CVE-2019-5785)

- A buffer overflow vulnerability in the Skia library can occur with Canvas 2D acceleration on macOS. This issue was addressed by disabling Canvas 2D acceleration in Firefox ESR. *Note: this does not affect other versions and platforms where Canvas 2D acceleration is already disabled by default.* (CVE-2018-18335)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2019-05/

https://bugzilla.mozilla.org/show_bug.cgi?id=1525817

https://bugzilla.mozilla.org/show_bug.cgi?id=1525433

http://www.nessus.org/u?127cc4df

https://bugzilla.mozilla.org/show_bug.cgi?id=1525815

Solution

Upgrade to Mozilla Firefox ESR version 60.5.1 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

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-2018-18335
CVE	CVE-2018-18356
CVE	CVE-2019-5785
XREF	MFSA:2019-05

Plugin Information

Published: 2019/02/15, Modified: 2019/10/31

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 60.5.1 ESR
```

133677 - Mozilla Firefox ESR < 68.5 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 68.5. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-06 advisory. Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2020-06/

Solution

Upgrade to Mozilla Firefox ESR version 68.5 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

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-2020-6796
CVE	CVE-2020-6798
CVE	CVE-2020-6799
CVE	CVE-2020-6800
XREF	MFSA:2020-06
XREF	IAVA:2020-A-0072-S

Plugin Information

Published: 2020/02/13, Modified: 2020/05/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 68.5 ESR
```

146332 - Security Update for Forefront Endpoint Protection (February 2021)

Synopsis

An antimalware application installed on the remote host is affected by a privilege escalation vulnerability.

Description

The Malware Protection Engine version of Forefront Endpoint Protection installed on the remote Windows host is equal or prior to 1.1.17700.4. It is, therefore, affected by a unspecified privilege escalation vulnerability. An authenticated, local attacker can exploit this to gain administrator access to the system.

See Also

http://www.nessus.org/u?ba846d3c

Solution

Enable automatic updates to update the malware engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

Risk Factor

Medium

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

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-24092

Plugin Information

Published: 2021/02/09, Modified: 2021/03/05

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.17800.5
```

144886 - Security Update for Forefront Endpoint Protection (January 2021)

Synopsis

An antimalware application installed on the remote host is affected by a remote code execution vulnerability.

Description

The Malware Protection Engine version of Forefront Endpoint Protection installed on the remote Windows host is prior to 1.1.17600.5. It is, therefore, affected by an unspecified remote code execution vulnerability. An authenticated, local attacker can exploit this to bypass authentication and execute arbitrary code with administrator privileges.

See Also

http://www.nessus.org/u?66e83fa0

Solution

Enable automatic updates to update the malware engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

Risk Factor

High

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

9.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-1647
XREF	CISA-KNOWN-EXPLOITED:2021/11/17
XREF	CEA-ID:CEA-2021-0001

Plugin Information

Published: 2021/01/12, Modified: 2022/12/07

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.17700.4
```

150361 - Security Update for Forefront Endpoint Protection (June 2021)

Synopsis

An antimalware application installed on the remote host is affected by multiple vulnerabilities.

Description

The Malware Protection Engine version of Forefront Endpoint Protection installed on the remote Windows host is equal or prior to 1.1.17800.5. It is, therefore, affected by multiple vulnerabilities.

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2021-31985)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2021-31978)

See Also

http://www.nessus.org/u?db0f474f

http://www.nessus.org/u?51ebd435

Solution

Enable automatic updates to update the malware engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

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

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)

STIG Severity

I

References

CVE	CVE-2021-31978
CVE	CVE-2021-31985
XREF	IAVA:2021-A-0273-S

Plugin Information

Published: 2021/06/08, Modified: 2023/12/27

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.18200.3
```

152427 - Security Update for Windows Defender (August 2021)

Synopsis

An antimalware application installed on the remote host is affected by privilege escalation vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is equal or prior to 1.1.18400.4. It is, therefore, affected by a unspecified privilege escalation vulnerability. An authenticated, local attacker can exploit this to gain administrator access to the system.

See Also

http://www.nessus.org/u?9c1e6309

http://www.nessus.org/u?3bed4ba6

Solution

Enable automatic updates to update the malware engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

Risk Factor

Medium

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

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-34471
XREF	IAVA:2021-A-0372

Plugin Information

Published: 2021/08/10, Modified: 2021/08/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.18400.4
```

146334 - Security Update for Windows Defender (February 2021)

Synopsis

An antimalware application installed on the remote host is affected by privilege escalation vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is equal or prior to 1.1.17700.4. It is, therefore, affected by a unspecified privilege escalation vulnerability. An authenticated, local attacker can exploit this to gain administrator access to the system.

See Also

http://www.nessus.org/u?ba846d3c

Solution

Enable automatic updates to update the malware engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

Risk Factor

Medium

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

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-24092

Plugin Information

Published: 2021/02/09, Modified: 2021/03/05

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.17800.5
```

144876 - Security Update for Windows Defender (January 2021)

Synopsis

An antimalware application installed on the remote host is affected by a remote code execution vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is prior to 1.1.17600.5. It is, therefore, affected by an unspecified remote code execution vulnerability. An authenticated, local attacker can exploit this to bypass authentication and execute arbitrary code with administrator privileges.

See Also

http://www.nessus.org/u?66e83fa0

Solution

Enable automatic updates to update the malware engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

Risk Factor

High

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

9.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-1647
XREF	CISA-KNOWN-EXPLOITED:2021/11/17
XREF	CEA-ID:CEA-2021-0001

Plugin Information

Published: 2021/01/12, Modified: 2022/12/07

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.17700.4
```

151647 - Security Update for Windows Defender (July 2021)

Synopsis

An antimalware application installed on the remote host is affected by multiple vulnerabilities.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is prior to 1.1.18242.0. It is, therefore, affected by multiple remote code execution vulnerabilities. An attacker can exploit one of these vulnerabilities to bypass authentication and execute unauthorized 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

http://www.nessus.org/u?5ff8e1a1

http://www.nessus.org/u?d20e15da

Solution

Enable automatic updates to update the malware engine for the relevant antimalware applications.

Risk Factor

High

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-34464
CVE	CVE-2021-34522

Plugin Information

Published: 2021/07/15, Modified: 2023/12/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.18242.0
```

150359 - Security Update for Windows Defender (June 2021)

Synopsis

An antimalware application installed on the remote host is affected by multiple vulnerabilities.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is equal or prior to 1.1.17800.5. It is, therefore, affected by multiple vulnerabilities.

- A remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands. (CVE-2021-31985)

- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2021-31978)

See Also

http://www.nessus.org/u?db0f474f

http://www.nessus.org/u?51ebd435

Solution

Enable automatic updates to update the malware engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

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

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)

STIG Severity

I

References

CVE	CVE-2021-31978
CVE	CVE-2021-31985
XREF	IAVA:2021-A-0273-S

Plugin Information

Published: 2021/06/08, Modified: 2023/12/27

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.18200.3
```

135719 - Security Updates for Windows Defender (April 2020)

Synopsis

An antimalware application installed on the remote host is affected by a hard link elevation of privilege vulnerability.

Description

The engine version of Microsoft Windows Defender installed on the remote Windows host is prior to 4.18.2001.112. It is, therefore, affected by a hard link elevation of privilege vulnerability which could allow an attacker who successfully exploited this vulnerability to elevate privileges on the system.

See Also

http://www.nessus.org/u?5520b9d8

Solution

Enable automatic updates to update the scan engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

Risk Factor

High

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

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

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2020-0835

Plugin Information

Published: 2020/04/17, Modified: 2020/05/19

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 4.18.1909.6
Fixed version     : 4.18.2001.112
```

174162 - Security Updates for Windows Defender (April 2023)

Synopsis

An antimalware application installed on the remote host is affected by a denial of service vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is prior to 1.1.20200.4. It is, therefore, affected by a denial of service vulnerability.

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?3bed4ba6

Solution

Microsoft has released KB2267602 to address this issue.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-24860

MSKB	2267602
XREF	MSFT:MS23-2267602

Plugin Information

Published: 2023/04/12, Modified: 2023/04/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.20200.4
```

179675 - Security Updates for Windows Defender (August 2023)

Synopsis

An antimalware application installed on the remote host is affected by a privilege escalation vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is prior to 1.1.23060.3001. It is, therefore, affected by a privilege escalation vulnerability.

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?3bed4ba6

http://www.nessus.org/u?8f15daf6

Solution

Enable automatic updates to update the malware engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

Risk Factor

Medium

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

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2023-38175

Plugin Information

Published: 2023/08/10, Modified: 2023/08/11

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.23060.3001
```

186903 - Security Updates for Windows Defender (December 2023)

Synopsis

An antimalware application installed on the remote host is affected by a denial of service vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is prior to 4.18.23110.3. It is, therefore, affected by a denial of service vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services.

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?3bed4ba6

Solution

Update Microsoft Defender version 4.18.23110.3 to address this issue.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-36010
XREF	IAVA:2023-A-0688

Plugin Information

Published: 2023/12/14, Modified: 2023/12/15

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 4.18.1909.6
Fixed version     : 4.18.23110.3
```

178243 - Security Updates for Windows Defender (July 2023)

Synopsis

An antimalware application installed on the remote host is affected by an elevation of privilege vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is prior to 1.1.23050.3. It is, therefore, affected by an elevation of privilege vulnerability.

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?3bed4ba6

Solution

Microsoft has released KB2267602 to address this issue.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-33156
MSKB	2267602
XREF	MSFT:MS23-2267602

Plugin Information

Published: 2023/07/13, Modified: 2023/07/17

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.23050.3
```

154991 - Security Updates for Windows Defender (November 2021)

Synopsis

An antimalware application installed on the remote host is affected by a remote code execution vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is equal or prior to 1.1.18700.3. It is, therefore, affected by a remote code execution vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42298

http://www.nessus.org/u?3bed4ba6

Solution

Enable automatic updates to update the malware engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.

Risk Factor

High

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-42298
XREF	IAVA:2022-A-0005

Plugin Information

Published: 2021/11/09, Modified: 2023/11/24

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.18700.3
```

185900 - Security Updates for Windows Defender (November 2023)

Synopsis

An antimalware application installed on the remote host is affected by a privilege escalation vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is prior to 4.18.23100.2009. It is, therefore, affected by a privilege escalation vulnerability. An authenticated attacker can exploit this to gain elevated privileges.

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?3bed4ba6

Solution

Update Microsoft Defender version 4.18.23100.2009 to address this issue.

Risk Factor

Medium

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

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-36422
XREF	IAVA:2023-A-0646-S

Plugin Information

Published: 2023/11/16, Modified: 2023/12/15

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 4.18.1909.6
Fixed version     : 4.18.23100.2009
```

166769 - Security Updates for Windows Defender (October 2022)

Synopsis

An antimalware application installed on the remote host is affected by a privilege escalation vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is prior to 1.1.19700.3. It is, therefore, affected by a privilege escalation vulnerability. An authenticated attacker can exploit this to gain elevated privileges.

See Also

http://www.nessus.org/u?3bed4ba6

Solution

Microsoft has released KB4052623 to address this issue.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-37971
MSKB	4052623

XREF MSFT:MS22-4052623

Plugin Information

Published: 2022/11/01, Modified: 2023/10/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.19700.3
```

181341 - Security Updates for Windows Defender (September 2023)

Synopsis

An antimalware application installed on the remote host is affected by an attack surface reduction vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is prior to 1.1.23080.2005. It is, therefore, affected by an attack surface reduction vulnerability due to security features bypass. A remote attacker can trick a victim to open a specially crafted file and bypass the Windows Defender Attack Surface Reduction blocking feature.

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?3bed4ba6

Solution

Update Microsoft Defender to engine version 1.1.23080.2005 to address this issue.

Risk Factor

High

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

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

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-38163
XREF	IAVA:2023-A-0488-S

Plugin Information

Published: 2023/09/13, Modified: 2023/12/01

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.23080.2005
```

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

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

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

VPR Score

8.9

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: 2023/12/26

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.
```

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: 2020/10/16

Plugin Output

tcp/445/cifs

```
Malware Signature Timestamp : Sep. 24, 2019 at 05:12:58 GMT
Malware Signature Version   : 1.303.25.0
```

62743 - Firefox 10.x < 10.0.10 Multiple Vulnerabilities

Synopsis

The remote Windows host contains a web browser that is affected by multiple vulnerabilities.

Description

The installed version of Firefox 10.x is potentially affected by the following security issues :

- The true value of 'window.location' can be shadowed by user content through the use of the 'valueOf' method, which can be combined with some plugins to perform cross-site scripting attacks. (CVE-2012-4194)

- The 'CheckURL' function of 'window.location' can be forced to return the wrong calling document and principal, allowing a cross-site scripting attack.

(CVE-2012-4195)

- It is possible to use property injection by prototype to bypass security wrapper protections on the 'Location'

object, allowing the cross-origin reading of the 'Location' object. (CVE-2012-4196)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2012-90/

Solution

Upgrade to Firefox 10.0.10 ESR or later.

Risk Factor

Medium

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	56301
BID	56302

BID	56306
CVE	CVE-2012-4194
CVE	CVE-2012-4195
CVE	CVE-2012-4196
XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information

Published: 2012/10/29, Modified: 2019/12/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 10.0.10 ESR
```

85274 - Firefox ESR < 38.1.1 PDF Reader Arbitrary File Access

Synopsis

The remote Windows host contains a web browser that is affected by an arbitrary file access vulnerability.

Description

The version of Firefox ESR installed on the remote Windows host is prior to 38.1.1. It is, therefore, affected by a vulnerability in the same origin policy in which an attacker can inject script code into a non-privileged part of browser's built-in PDF reader, resulting in gaining access to sensitive local files.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-78/

https://bugzilla.mozilla.org/show_bug.cgi?id=1179262

Solution

Upgrade to Firefox ESR 38.1.1 or later.

Risk Factor

Medium

VPR Score

8.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2015-4495
XREF	CISA-KNOWN-EXPLOITED:2022/06/15

Exploitable With

CANVAS (true)

Plugin Information

Published: 2015/08/07, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 10.0.1 ESR
Fixed version     : 38.1.1 ESR
```

164253 - Microsoft Edge (Chromium) < 104.0.1293.60 Vulnerability

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 104.0.1293.60. It is, therefore, affected by a vulnerability as referenced in the August 17, 2022 advisory.

- Insufficient validation of untrusted input in Intents. (CVE-2022-2856)

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?b53011a2

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-2856

Solution

Upgrade to Microsoft Edge version 104.0.1293.60 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:N/I:H/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

5.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-2856
XREF	CISA-KNOWN-EXPLOITED:2022/09/08

Plugin Information

Published: 2022/08/18, Modified: 2023/10/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 104.0.1293.60
```

170690 - Microsoft Edge (Chromium) < 109.0.1518.61 Security Feature Bypass (CVE-2023-21719)

Synopsis

The remote host has an web browser installed that is affected by security feature bypass.

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 109.0.1518.61. It is, therefore, affected by a vulnerability as referenced in the January 19, 2023 advisory.

- Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability. (CVE-2023-21719)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21719

Solution

Upgrade to Microsoft Edge version 109.0.1518.61 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

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-2023-21719
XREF	IAVA:2023-A-0051-S

Plugin Information

Published: 2023/01/27, Modified: 2023/02/10

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 109.0.1518.61
```

171334 - Microsoft Edge (Chromium) < 109.0.1518.78 Tampering (CVE-2023-21720)

Synopsis

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

Description

The version of Microsoft Edge installed on the remote Windows host is prior to 109.0.1518.78. It is, therefore, affected by a vulnerability as referenced in the February 2, 2023 advisory.

- Microsoft Edge (Chromium-based) Tampering Vulnerability (CVE-2023-21720)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21720

Solution

Upgrade to Microsoft Edge version 109.0.1518.78 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-21720
XREF	IAVA:2023-A-0071-S

Plugin Information

Published: 2023/02/10, Modified: 2023/02/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 109.0.1518.78
```

174286 - Microsoft Edge (Chromium) < 112.0.1722.34 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 112.0.1722.34. It is, therefore, affected by multiple vulnerabilities as referenced in the April 6, 2023 advisory.

- Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability (CVE-2023-28284)

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2023-24935)

- Microsoft Edge (Chromium-based) Tampering Vulnerability (CVE-2023-28301)

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?245dfb65

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24935

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28284

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28301

Solution

Upgrade to Microsoft Edge version 112.0.1722.34 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.0

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-2023-24935
CVE	CVE-2023-28284
CVE	CVE-2023-28301
XREF	IAVA:2023-A-0180-S

Plugin Information

Published: 2023/04/14, Modified: 2023/05/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 112.0.1722.34
```

189188 - Microsoft Edge (Chromium) < 120.0.2210.133 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 120.0.2210.133. It is, therefore, affected by multiple vulnerabilities as referenced in the January 11, 2024 advisory.

- Insufficient data validation in Extensions in Google Chrome prior to 120.0.6099.216 allowed an attacker in a privileged network position to install a malicious extension via a crafted HTML page. (Chromium security severity: High) (CVE-2024-0333)

- Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability (CVE-2024-20675)

- Acrobat Reader T5 (MSFT Edge) versions 120.0.2210.91 and earlier are affected by an Improper Input Validation vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. (CVE-2024-20709, CVE-2024-20721)

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability (CVE-2024-21337)

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?3844aad0

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0333

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20675

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20709

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20721

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21337

Solution

Upgrade to Microsoft Edge version 120.0.2210.133 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-0333
CVE	CVE-2024-20675
CVE	CVE-2024-20709
CVE	CVE-2024-20721
CVE	CVE-2024-21337
XREF	IAVA:2024-A-0040-S

Plugin Information

Published: 2024/01/18, Modified: 2024/02/02

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 120.0.2210.133
```

189605 - Microsoft Edge (Chromium) < 120.0.2210.160 / 121.0.2277.83 (CVE-2024-21388)

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 120.0.2210.160 / 121.0.2277.83. It is, therefore, affected by a vulnerability as referenced in the January 30, 2024 advisory.

- Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability (CVE-2024-21388)

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?d0503752

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21388

Solution

Upgrade to Microsoft Edge version 120.0.2210.160 / 121.0.2277.83 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-21388
XREF	IAVA:2024-A-0060-S

Plugin Information

Published: 2024/01/25, Modified: 2024/02/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 121.0.2277.83
```

153368 - Microsoft Edge (Chromium) < 93.0.961.44 Vulnerability

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 93.0.961.44. It is, therefore, affected by a vulnerability as referenced in the September 9, 2021 advisory.

- Microsoft Edge (Chromium-based) Tampering Vulnerability (CVE-2021-38669)

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?5b26fe9e

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38669

Solution

Upgrade to Microsoft Edge version 93.0.961.44 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.0

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-38669
XREF	IAVA:2021-A-0432-S

Plugin Information

Published: 2021/09/14, Modified: 2023/12/29

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 93.0.961.44
```

156916 - Microsoft Edge (Chromium) < 97.0.1072.69 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 97.0.1072.69. It is, therefore, affected by multiple vulnerabilities as referenced in the January 20, 2022 advisory.

- Microsoft Edge for Android Spoofing Vulnerability. (CVE-2022-23258)

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?4c365598

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0289

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0290

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0291

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0292

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0293

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0294

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0295

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0296

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0297

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0298

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0300

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0301

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0302

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0303

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0304

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0305

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0306

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0307

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0308

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0309

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0310

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-0311

Solution

Upgrade to Microsoft Edge version 97.0.1072.69 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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2022-23258

Plugin Information

Published: 2022/01/20, Modified: 2022/05/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 97.0.1072.69
```

157881 - Microsoft Edge (Chromium) < 98.0.1108.50 Vulnerability

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 98.0.1108.50. It is, therefore, affected by a vulnerability as referenced in the February 10, 2022 advisory.

- Microsoft Edge (Chromium-based) Spoofing Vulnerability (CVE-2022-23264)

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?fe909fdc

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23264

Solution

Upgrade to Microsoft Edge version 98.0.1108.50 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.6

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-2022-23264
XREF	IAVA:2023-A-0071-S

Plugin Information

Published: 2022/02/10, Modified: 2023/11/09

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Microsoft\Edge\Application
Installed version : 92.0.902.67
Fixed version     : 98.0.1108.50
```

177383 - Microsoft OneNote Spoofing(June 2023)

Synopsis

The Microsoft OneNote Products are affected by a spoofing vulnerability.

Description

The Microsoft OneNote Products are missing a security update. It is, therefore, affected by a spoofing 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

http://www.nessus.org/u?b315068b

http://www.nessus.org/u?5931548c

http://www.nessus.org/u?18e4c958

Solution

Upgrade to app version 16.0.14326.21450 or later via the Microsoft Store.

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

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2023-33140
XREF	IAVA:2023-A-0303-S

Plugin Information

Published: 2023/06/16, Modified: 2023/08/17

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.Office.OneNote_16001.12026.20112.0_x64__8wekyb3d8bbwe
  Installed version : 16001.12026.20112.0
  Fixed version     : 16001.14326.21450.0
```

158205 - Microsoft Windows VP9 Video Extensions Library Information Disclosure (December 2021)

Synopsis

The Windows app installed on the remote host is affected by an information disclosure vulnerability.

Description

The Windows 'VP9 Extensions' app installed on the remote host is affected by an information disclosure vulnerability.

An authenticated, local 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43243

Solution

Upgrade to app version 1.0.42791.0, or later via the Microsoft Store.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-43243

Plugin Information

Published: 2022/02/21, Modified: 2022/02/22

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22681.0
  Fixed version     : 1.0.42791.0
```

140596 - Microsoft Windows WebP Image Extension RCE (August 2020)

Synopsis

The Windows app installed on the remote host is affected by a Remote Code Execution Vulnerability.

Description

The Windows 'WebP Image Extension' or 'WebP from Device Manufacturer' app installed on the remote host is affected by a remote code execution vulnerability.

An unauthenticated, remote attacker can exploit this vulnerability via an specially crafted image to execute code and gain control of the system.

See Also

http://www.nessus.org/u?f2638e5b

Solution

Upgrade to app version 1.0.31251.0 or later via the Microsoft Store.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2020-1574
XREF	IAVA:2020-A-0361-S
XREF	CEA-ID:CEA-2020-0101

Plugin Information

Published: 2020/09/15, Modified: 2024/02/20

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.WebpImageExtension_1.0.22753.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22753.0
  Fixed version     : 1.0.31251.0
```

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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)

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

178241 - Security Updates for Microsoft Windows VP9 Video Extensions Library (July 2023)

Synopsis

The Windows app installed on the remote host is affected by an information disclosure vulnerability.

Description

The Windows 'VP9 Extensions' app installed on the remote host is affected by an information disclosure vulnerability. An attacker who successfully exploited this vulnerability could potentially read small portions of heap memory.

Exploitation of the vulnerability requires that an attacker must send the user a malicious file and convince them to open it.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36872

Solution

Upgrade to app version 1.0.61591.0, or later via the Microsoft Store.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-36872
XREF	IAVA:2023-A-0345-S

Plugin Information

Published: 2023/07/13, Modified: 2023/08/11

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.VP9VideoExtensions_1.0.22681.0_x64__8wekyb3d8bbwe
  Installed version : 1.0.22681.0
  Fixed version     : 1.0.61591.0
```

159916 - Security Updates for Windows Defender (April 2022)

Synopsis

An antimalware application installed on the remote host is affected by a denial of service vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is equal or prior to 1.1.19100.5. It is, therefore, affected by a denial of service vulnerability. An attacker can exploit this to bypass authentication and execute unauthorized arbitrary commands.

See Also

http://www.nessus.org/u?3bed4ba6

Solution

Microsoft has released KB4052623 to address this issue.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-24548
MSKB	4052623

XREF MSFT:MS22-4052623

Plugin Information

Published: 2022/04/20, Modified: 2023/11/01

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.19100.5
```

172577 - Security Updates for Windows Defender (March 2023)

Synopsis

An antimalware application installed on the remote host is affected by a privilege escalation vulnerability.

Description

The Malware Protection Engine version of Microsoft Windows Defender installed on the remote Windows host is prior to 1.1.20000.2. It is, therefore, affected by a privilege escalation vulnerability. An authenticated attacker can exploit this to gain elevated privileges.

See Also

http://www.nessus.org/u?3bed4ba6

Solution

Microsoft has released KB4052623 to address this issue.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-23389
MSKB	4052623

XREF MSFT:MS22-4052623

Plugin Information

Published: 2023/03/15, Modified: 2023/03/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files\Windows Defender\
Installed version : 1.1.16400.2
Fixed version     : 1.1.20000.2
```

177217 - Windows Snip & Sketch/ Snipping Tool CVE-2023-28303 (Acropalypse)

Synopsis

The remote web server hosts an application that is affected by an information disclosure vulnerability.

Description

An information disclosure vulnerability exists in Windows Snip & Sketch (Windows 10) and Snipping Tool (Windows 11) where parts of a cropped image that were to be removed are not completely deleted and can be restored if saved to the cropped image file.

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?ad297874

Solution

Upgrade to Snip & Sketch 10.2008.3001.0 for Windows 10, Snipping Tool 11.2302.20.0 for Windows 11, or later.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-28303

Plugin Information

Published: 2023/06/13, Modified: 2023/06/14

Plugin Output

tcp/0

```
  Path              : C:\Program Files\WindowsApps
\Microsoft.ScreenSketch_10.1907.2471.0_x64__8wekyb3d8bbwe
  Installed version : 10.1907.2471.0
  Fixed version     : 10.2008.3001.0
```

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:\Program Files\Windows Defender\
  Version                      : 4.18.1909.6
  Engine version               : 1.1.16400.2
  Antivirus signature version  : 1.303.25.0
  Antispyware signature version : 1.303.25.0

The antivirus signatures are out of date. The last known updated
version from the vendor is : 1.305.1053.0
The antispyware signatures are out of date. The last known updated
version from the vendor is : 1.305.1053.0
```

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.
```

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: 2024/02/22

Plugin Output

tcp/0

```
Vendor       : Phoenix Technologies LTD
Version      : 6.00
Release date : 20201112000000.000000+000
UUID         : 9C0A4D56-4E05-36DF-D135-6B4108B7F132
Secure boot  : disabled
```

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: 2024/02/22

Plugin Output

tcp/0

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

  cpe:/o:microsoft:windows_10 -> Microsoft Windows 10 64-bit

Following application CPE's matched on the remote system :

  cpe:/a:haxx:curl:8.4.0.0 -> Haxx Curl
  cpe:/a:microsoft:.net_framework:4.8 -> Microsoft .NET Framework
  cpe:/a:microsoft:.net_framework:4.8.4682.0 -> Microsoft .NET Framework
  cpe:/a:microsoft:edge:92.0.902.67 -> Microsoft Edge
  cpe:/a:microsoft:ie:11.3636.19041.0 -> Microsoft Internet Explorer
  cpe:/a:microsoft:internet_explorer:11.0.19041.3803 -> Microsoft Internet Explorer
  cpe:/a:microsoft:onedrive:19.43.304.13 -> Microsoft OneDrive
  cpe:/a:microsoft:remote_desktop_connection:10.0.19041.3758 -> Microsoft Remote Desktop Connection
  cpe:/a:microsoft:system_center_endpoint_protection:4.18.1909.6 -> Microsoft System Center Endpoint
 Protection
  cpe:/a:microsoft:windows_app_store:0.19051.7.0
  cpe:/a:microsoft:windows_app_store:1.0.20875.0
```

```
cpe:/a:microsoft:windows_app_store:1.0.22681.0
cpe:/a:microsoft:windows_app_store:1.0.22742.0
cpe:/a:microsoft:windows_app_store:1.0.22753.0
cpe:/a:microsoft:windows_app_store:1.0.30251.0
cpe:/a:microsoft:windows_app_store:1.14.10.19041
cpe:/a:microsoft:windows_app_store:1.17.29001.0
cpe:/a:microsoft:windows_app_store:1.1907.3152.0
cpe:/a:microsoft:windows_app_store:1.1911.21713.0
cpe:/a:microsoft:windows_app_store:1.23.28002.0
cpe:/a:microsoft:windows_app_store:1.46.11001.0
cpe:/a:microsoft:windows_app_store:1.7.25531.0
cpe:/a:microsoft:windows_app_store:10.0.18101.0
cpe:/a:microsoft:windows_app_store:10.0.19041.3636
cpe:/a:microsoft:windows_app_store:10.0.2.1000
cpe:/a:microsoft:windows_app_store:10.1706.13331.0
cpe:/a:microsoft:windows_app_store:10.1808.3.0
cpe:/a:microsoft:windows_app_store:10.1902.633.0
cpe:/a:microsoft:windows_app_store:10.1906.1972.0
cpe:/a:microsoft:windows_app_store:10.1906.2182.0
cpe:/a:microsoft:windows_app_store:10.1906.55.0
cpe:/a:microsoft:windows_app_store:10.1907.2471.0
cpe:/a:microsoft:windows_app_store:10.19071.19 [...]
```

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: 2024/02/22

Plugin Output

tcp/0

```
Computer Manufacturer : VMware, Inc.
Computer Model : VMware Virtual Platform
Computer SerialNumber : VMware-56 4d 0a 9c 05 4e df 36-d1 35 6b 41 08 b7 f1 32
Computer Type : Other

Computer Physical CPU's : 2
Computer Logical CPU's  : 2
  CPU0
    Architecture  : x64
    Physical Cores: 1
    Logical Cores : 1
  CPU1
    Architecture  : x64
    Physical Cores: 1
    Logical Cores : 1

Computer Memory : 7999 MB
  RAM slot #0
    Form Factor: DIMM
    Type       : DRAM
    Capacity   : 4096 MB
  RAM slot #1
    Form Factor: DIMM
    Type       : DRAM
    Capacity   : 2048 MB
  RAM slot #2
    Form Factor: DIMM
    Type       : DRAM
    Capacity   : 1024 MB
```

```
    RAM slot #3
      Form Factor: DIMM
      Type       : DRAM
      Capacity   : 512 MB
    RAM slot #4
      Form Factor: DIMM
      Type       : DRAM
      Capacity   : 256 MB
    RAM slot #5
      Form Factor: DIMM
      Type       : DRAM
      Capacity   : 64 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: 2024/02/22

Plugin Output

tcp/0

```
Nessus detected 2 installs of Curl:

  Path          : C:\Windows\SysWOW64\curl.exe
  Version       : 8.4.0.0
  Managed by OS : True

  Path          : C:\Windows\System32\curl.exe
  Version       : 8.4.0.0
  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 : \\DESKTOP-96HJG8C

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 : \\DESKTOP-96HJG8C

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\DESKTOP-96HJG8C

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 : \\DESKTOP-96HJG8C

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 : \\DESKTOP-96HJG8C

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
Netbios name : \\DESKTOP-96HJG8C

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\DESKTOP-96HJG8C

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\DESKTOP-96HJG8C

Object UUID : b08669ee-8cb5-43a5-a017 [...]
```

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 : 192.168.128.129

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 : 192.168.128.129

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 : 192.168.128.129

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 : 192.168.128.129
```

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 : 192.168.128.129
```

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 : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49666
IP : 192.168.128.129
```

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 : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.128.129

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 : 49667
IP : 192.168.128.129
```

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 : 192.168.128.129

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 : 192.168.128.129

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 : 192.168.128.129

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 : 192.168.128.129

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 : 192.168.128.129
```

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 : 192.168.128.129
```

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/49670/dce-rpc

```
The following DCERPC services are available on TCP port 49670 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49670
IP : 192.168.128.129
```

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: 2024/02/22

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~~10.0.19041.3636
State        : Installed
Release Type : OnDemand Pack
Install Time : 04/12/2023 02:56

Package      : Microsoft-OneCore-DirectX-Database-FOD-Package~31bf3856ad364e35~amd64~~10.0.19041.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 07/12/2019 09:53

Package      : Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~10.0.19041.3803
State        : Installed
Release Type : Language Pack
Install Time : 04/12/2023 02:56

Package      : Microsoft-Windows-FodMetadata-Package~31bf3856ad364e35~amd64~~10.0.19041.1
State        : Installed
Release Type : Feature Pack
Install Time : 07/12/2019 09:50

Package      : Microsoft-Windows-Foundation-Package~31bf3856ad364e35~amd64~~10.0.19041.1
```

```
State        : Installed
Release Type : Foundation
Install Time : 07/12/2019 09:18

Package      : Microsoft-Windows-Hello-Face-Package~31bf3856ad364e35~amd64~~10.0.19041.3636
State        : Installed
Release Type : OnDemand Pack
Install Time : 04/12/2023 02:56

Package      : Microsoft-Windows-InternetExplorer-Optional-
Package~31bf3856ad364e35~amd64~~11.0.19041.3636
State        : Installed
Release Type : OnDemand Pack
Install Time : 04/12/2023 02:56

Package      : Microsoft-Windows-LanguageFeatures-Basic-en-us-
Package~31bf3856ad364e35~amd64~~10.0.19041.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 07/12/2019 09:52

Package      : Microsoft-Windows-LanguageFeatures-Handwriting-en-us-
Package~31bf3856ad364e35~amd64~~10.0.19041.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 07/12/2019 09:52

Package      : Microsoft-Windows-LanguageFeatures-OCR-en-us-
Package~31bf3856ad364e35~amd64~~10.0.19041.1
State        : Installed
Release Type : OnDemand Pack
Install Time : 07/12/2019 09:52

Package      : Microsoft-Windows-LanguageFeatures-Speech-en-us [...]
```

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: 2024/02/22

Plugin Output

tcp/0

```
Hostname : DESKTOP-96HJG8C
  DESKTOP-96HJG8C (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: 2022/09/09

Plugin Output

tcp/0

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

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: 2024/02/22

Plugin Output

tcp/0

```
Group Name : Access Control Assistance Operators
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-579
Members    :

Group Name : Administrators
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-544
Members    :
  Name : Administrator
    Domain : DESKTOP-96HJG8C
    Class  : Win32_UserAccount
    SID    : S-1-5-21-3315527792-3692112875-3820317123-500
  Name : Windows10 VM
    Domain : DESKTOP-96HJG8C
    Class  : Win32_UserAccount
    SID    : S-1-5-21-3315527792-3692112875-3820317123-1001

Group Name : Backup Operators
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-551
Members    :

Group Name : Cryptographic Operators
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-569
Members    :

Group Name : Device Owners
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-583
Members    :
```

```
Group Name : Distributed COM Users
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-562
Members    :

Group Name : Event Log Readers
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-573
Members    :

Group Name : Guests
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-546
Members    :
  Name : Guest
    Domain : DESKTOP-96HJG8C
    Class  : Win32_UserAccount
    SID    : S-1-5-21-3315527792-3692112875-3820317123-501

Group Name : Hyper-V Administrators
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-578
Members    :

Group Name : IIS_IUSRS
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-568
Members    :
  Name : IUSR
    Domain : DESKTOP-96HJG8C
    Class  : Win32_SystemAccount
    SID    : S-1-5-17

Group Name : Network Configuration Operators
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-556
Members    :

Group Name : Performance Log Users
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-559
Members    :

Group Name : Performance Monitor Users
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-558
Members    :

Group Name : Power Users
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-547
Members    :

Group Name : Remote Desktop Users
Host Name  : DESKTOP-96HJG8C
Group SID  : S-1-5-32-555
Memb [...]
```

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: 2024/02/22

Plugin Output

tcp/0

```
Name            : Administrator
SID             : S-1-5-21-3315527792-3692112875-3820317123-500
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

Name            : DefaultAccount
SID             : S-1-5-21-3315527792-3692112875-3820317123-503
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

Name            : Guest
SID             : S-1-5-21-3315527792-3692112875-3820317123-501
Disabled        : True
Lockout         : False
Change password : False
Source          : Local

Name            : WDAGUtilityAccount
SID             : S-1-5-21-3315527792-3692112875-3820317123-504
Disabled        : True
Lockout         : False
Change password : True
Source          : Local

Name            : Windows10 VM
```

```
SID             : S-1-5-21-3315527792-3692112875-3820317123-1001
Disabled        : False
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: 2024/02/22

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\Windows10 VM\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 :

00:0C:29:B7:F1:32 : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 00:0C:29:B7:F1:32
```

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: 2017/04/14

Plugin Output

tcp/0

```
192.168.128.129 resolves as DESKTOP-96HJG8C.
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

icmp/0

```
The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is -28739 seconds.
```

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: 2024/02/22

Plugin Output

tcp/0

```
+ Loopback Pseudo-Interface 1
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ Bluetooth Network Connection
  + IPv4
    - Address       : 169.254.105.180
      Assign Method : dynamic
  + IPv6
    - Address       : fe80::e44:8e33:1f0b:565c%2
      Assign Method : dynamic
+ Ethernet0
  + IPv4
    - Address       : 192.168.128.129
      Assign Method : dynamic
  + IPv6
    - Address       : fe80::a94e:30a0:e7f4:46cf%14
      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: 2024/02/22

Plugin Output

tcp/135/epmap

```
Nessus was able to extract the following cpuid: 906A4
```

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://crucialsecurityblog.harris.com/2011/03/14/typedurls-part-1/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2018/05/16

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

```
@tzres.dll,-352 : FLE Standard Time
@tzres.dll,-671 : AUS Eastern Daylight Time
@tzres.dll,-2980 : (UTC+03:00) Moscow, St. Petersburg
@%systemroot%\system32\axinstsv.dll,-103 : ActiveX Installer (AxInstSV)
@%systemroot%\system32\appxdeploymentserver.dll,-1 : AppX Deployment Service (AppXSVC)
@tzres.dll,-630 : (UTC+09:00) Osaka, Sapporo, Tokyo
@%systemroot%\system32\wlidsvc.dll,-100 : Microsoft Account Sign-in Assistant
@%systemroot%\system32\wcncsvc.dll,-3 : Windows Connect Now - Config Registrar
@%windir%\system32\drivers\pacer.sys,-101 : QoS Packet Scheduler
@%systemroot%\system32\efssvc.dll,-100 : Encrypting File System (EFS)
@%systemroot%\system32\lltdres.dll,-6 : Link-Layer Topology Discovery Mapper I/O Driver
@tzres.dll,-252 : Dateline Standard Time
@tzres.dll,-401 : Arabic Daylight Time
@tzres.dll,-2890 : (UTC+02:00) Khartoum
@tzres.dll,-82 : Atlantic Standard Time
@%systemroot%\system32\aphostres.dll,-10002 : Sync Host
@tzres.dll,-620 : (UTC+09:00) Seoul
@tzres.dll,-372 : Jerusalem Standard Time
@%systemroot%\system32\ci.dll,-100 : Isolated User Mode (IUM)
@%systemroot%\system32\wscsvc.dll,-200 : Security Center
@%systemroot%\system32\qwave.dll,-1 : Quality Windows Audio Video Experience
@%systemroot%\system32\cloudidsvc.dll,-100 : Microsoft Cloud Identity Service
```

```
@%systemroot%\system32\wiarpc.dll,-2 : Still Image Acquisition Events
@tzres.dll,-104 : Central Brazilian Daylight Time
@tzres.dll,-2450 : (UTC-03:00) Saint Pierre and Miquelon
@tzres.dll,-2631 : Norfolk Daylight Time
@tzres.dll,-221 : Alaskan Daylight Time
@%systemroot%\system32\tapisrv.dll,-10100 : Telephony
@tzres.dll,-2552 : W. Mongolia Standard Time
@tzres.dll,-2161 : Altai Daylight Time
@%systemroot%\system32\wpcrefreshtask.dll,-100 : Parental Controls
@c:\windows\system32\ieframe.dll,-12385 : Favorites Bar
@tzres.dll,-2752 : Tomsk Standard Time
@tzres.dll,-2390 : (UTC-10:00) Aleutian Islands
@%systemroot%\system32\rmapi.dll,-1001 : Radio Management Service
@%systemroot%\system32\p2psvc.dll,-8006 : Peer Networking Grouping
@tzres.dll,-1252  [...]
```

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
  Full Version : 4.8.04084
  Install Type : Full
  Release      : 528372

  Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
  Version      : 4.8
  Full Version : 4.8.04084
  Install Type : Client
  Release      : 528372
```

99364 - Microsoft .NET Security Rollup Enumeration

Synopsis

This plugin enumerates installed Microsoft .NET security rollups.

Description

Nessus was able to enumerate the Microsoft .NET security rollups installed on the remote Windows host.

See Also

http://www.nessus.org/u?662e30c9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/04/14, Modified: 2024/01/10

Plugin Output

tcp/445/cifs

```
Path                          : C:\Windows\Microsoft.NET\Framework\v4.0.30319\system.web.dll
Version                       : 4.8.4682.0
.NET Version                  : 4.8
Associated KB                 : 5031988
Latest effective update level : 11_2023
```

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: 2024/02/22

Plugin Output

tcp/445/cifs

```
Path    : C:\Program Files (x86)\Microsoft\Edge\Application
Version : 92.0.902.67
```

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: 2024/02/22

Plugin Output

tcp/0

```
Path    : C:\Windows\system32\mshtml.dll
Version : 11.0.19041.3803
```

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  : 11.3636.19041.0
```

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: 2024/02/22

Plugin Output

tcp/445/cifs

```
Path    : C:\Users\Windows10 VM\AppData\Local\Microsoft\OneDrive\
Version : 19.43.304.13
```

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 : 10.0.19041.3758
```

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: 2023/06/26

Plugin Output

tcp/445/cifs

```
Cumulative Rollup : 12_2023 [KB5033372]
Cumulative Rollup : 11_2023
Cumulative Rollup : 10_2023
Cumulative Rollup : 09_2023
Cumulative Rollup : 08_2023
Cumulative Rollup : 07_2023
Cumulative Rollup : 06_2023
Cumulative Rollup : 05_2023
Cumulative Rollup : 04_2023
Cumulative Rollup : 03_2023
Cumulative Rollup : 02_2023
Cumulative Rollup : 01_2023
Cumulative Rollup : 12_2022
Cumulative Rollup : 11_2022

Latest effective update level : 12_2023
File checked                  : C:\Windows\system32\ntoskrnl.exe
File version                  : 10.0.19041.3803
Associated KB                 : 5033372
```

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 :

  - DESKTOP-96HJG8C\Administrator (User)
  - DESKTOP-96HJG8C\Windows10 VM (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 users have never changed their passwords :\n
  - 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.
```

10916 - Microsoft Windows - Local Users Information : Passwords Never Expire

Synopsis

At least one local user has a password that never expires.

Description

Using the supplied credentials, Nessus was able to list local users that are enabled and whose passwords never expire.

Solution

Allow or require users to change their passwords regularly.

Risk Factor

None

Plugin Information

Published: 2002/03/17, Modified: 2018/08/13

Plugin Output

tcp/0

```
The following local user has a password that never expires :

  - Windows10 VM


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 this plugin, 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: 2024/02/22

Plugin Output

tcp/0

```
192.168.128.1 : 00-50-56-c0-00-01
192.168.128.255 : 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.
```

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 : 2
  username : SYSTEM
  os : Windows_NT
  temp : %SystemRoot%\TEMP
  processor_revision : 9a04
  path : %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%
\System32\WindowsPowerShell\v1.0\;%SYSTEMROOT%\System32\OpenSSH\
  tmp : %SystemRoot%\TEMP
  processor_identifier : Intel64 Family 6 Model 154 Stepping 4, 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-1-5-21-3315527792-3692112875-3820317123-1001
    onedrive : C:\Users\Windows10 VM\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: 2024/02/27

Plugin Output

tcp/0

```
OS Name      : Microsoft Windows 10 22H2
Vendor       : Microsoft
Product      : Windows
Release      : 10 22H2
Edition      : Pro
Version      : 10.0.19045.3803
Role         : client
Kernel       : Windows NT 10.0
Architecture : x64
CPE v2.2     : cpe:/o:microsoft:windows_10_22h2:10.0.19045.3803:-
CPE v2.3     : cpe:2.3:o:microsoft:windows_10_22h2:10.0.19045.3803:-:any:*:pro:*: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 92.0.902.67]  [installed on 2024/03/02]
Microsoft Edge Update  [version 1.3.173.55]
Microsoft Edge WebView2 Runtime  [version 122.0.2365.59]  [installed on 2024/03/03]
Mozilla Firefox 10.0.1 (x86 en-US)  [version 10.0.1]
```

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: 2023/07/18

Plugin Output

tcp/445/cifs

```
The following software information is available on the remote host :

 - Microsoft Edge Update
     Best Confidence Version  : 1.3.173.55
     Version Confidence Level : 2
     All Possible Versions    :  1.3.173.55
     Other Version Data
       [Version] :
           Raw Value           : 1.3.173.55
       [DisplayName] :
           Raw Value           : Microsoft Edge Update
       [DisplayVersion] :
           Raw Value           : 1.3.173.55

 - Microsoft Edge WebView2 Runtime
     Best Confidence Version  : 122.0.2365.59
     Version Confidence Level : 3
     All Possible Versions    :  122.0.2365.59
     Other Version Data
       [InstallDate] :
           Raw Value           : 2024/03/03
       [DisplayIcon] :
```

```
            Raw Value           : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\122.0.2365.59\msedgewebview2.exe,0
            Parsed File Path    : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\122.0.2365.59\msedgewebview2.exe
            Parsed File Version : 122.0.2365.59
        [InstallLocation] :
            Raw Value           : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
        [UninstallString] :
            Raw Value           : "C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\122.0.2365.59\Installer\setup.exe" --uninstall --msedgewebview --system-level --verbose-logging
            Parsed File Path    : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\122.0.2365.59\Installer\setup.exe
            Parsed File Version : 122.0.2365.59
        [VersionMinor] :
            Raw Value           : 59
        [Version] :
            Raw Value           : 122.0.2365.59
        [VersionMajor] :
            Raw Value           : 2365
        [DisplayVersion] :
            Raw Value           : 122.0.2365.59
        [DisplayName] :
            Raw Value           : Microsoft Edge WebView2 Runtime

 - Mozilla Firefox 10.0.1 (x86 en-US)
     Best Confidence Version  : 1.0.0.0
     Version Confidence Level : 3
     All Possible Versions    :  1.0.0.0, 10.0.1, [...]
```

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 : 2024-03-02T22:22:20-08:00 (20240302222220.625531-480)
```

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-1-5-21-3315527792-3692112875-3820317123-1001
    Domain   : DESKTOP-96HJG8C
    Username : Windows10 VM
```

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\d:
  Data     : \??\SCSI#CdRom&Ven_NECVMWar&Prod_VMware_SATA_CD01#5&260e6d66&0&010000#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f004e00450043005600 4d005700610072002600 5

  Name     : \??\volume{e859a8d6-d919-11ee-b5b4-806e6f6e6963}
  Data     : \??\SCSI#CdRom&Ven_NECVMWar&Prod_VMware_SATA_CD01#5&260e6d66&0&010000#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c0053004300530049002300430064005200 6f006d002600560065006e005f004e00450043005600 4d005700610072002600 5

  Name     : \dosdevices\c:
  Data     : *0
  Raw data : 2a8a85800000300300000000
```

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: 2024/02/22

Plugin Output

tcp/0

```
NBT information attached.
First 10 lines of all CSVs:
nbtstat_local.csv:
Interface,Name,Suffix,Type,Status,MAC
192.168.128.129,DESKTOP-96HJG8C,<20>,UNIQUE,Registered,00:0C:29:B7:F1:32
192.168.128.129,DESKTOP-96HJG8C,<00>,UNIQUE,Registered,00:0C:29:B7:F1:32
192.168.128.129,WORKGROUP,<00>,GROUP,Registered,00:0C:29:B7:F1:32
```

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) 82574L Gigabit Network Connection
Network Adapter Driver Version     : 12.17.10.8
```

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: 2024/02/22

Plugin Output

tcp/0

```
Process Overview :
SID: Process (PID)
 0 : System Idle Process (0)
 0 : |- System (4)
 0 :    |- Memory Compression (2024)
 0 :    |- smss.exe (300)
 0 : csrss.exe (408)
 1 : explorer.exe (4356)
 1 : |- msedge.exe (5428)
 1 :    |- msedge.exe (1564)
 1 :    |- msedge.exe (2004)
 1 :    |- msedge.exe (5052)
 1 :    |- msedge.exe (7416)
 1 :    |- msedge.exe (7428)
 1 :    |- msedge.exe (7464)
 1 :    |- msedge.exe (7552)
 1 :    |- msedge.exe (8556)
 1 : |- SecurityHealthSystray.exe (6672)
 1 : |- OneDrive.exe (6776)
 1 : |- cmd.exe (7140)
 1 :    |- conhost.exe (6920)
 1 : csrss.exe (484)
 0 : wininit.exe (492)
 0 : |- services.exe (636)
 0 :    |- svchost.exe (1084)
 0 :    |- svchost.exe (1096)
 0 :    |- svchost.exe (1104)
 0 :    |- svchost.exe (1120)
```

```
0 :    |- svchost.exe (1168)
0 :    |- svchost.exe (1184)
0 :    |- svchost.exe (1284)
0 :    |- svchost.exe (1316)
0 :    |- svchost.exe (1332)
1 :       |- taskhostw.exe (3132)
0 :    |- svchost.exe (1408)
0 :    |- svchost.exe (1484)
0 :    |- svchost.exe (1544)
1 :       |- ctfmon.exe (6008)
1 :       |- TabTip.exe (6056)
0 :    |- svchost.exe (1556)
0 :    |- svchost.exe (1620)
1 :       |- sihost.exe (2876)
0 :    |- svchost.exe (1692)
0 :    |- svchost.exe (1760)
0 :    |- svchost.exe (1776)
0 :    |- svchost.exe (1796)
0 :    |- svchost.exe (1816)
0 :    |- svchost.exe (1908)
0 :    |- svchost.exe (1916)
0 :    |- SgrmBroker.exe (1948)
0 :    |- svchost.exe (2036)
0 :    |- svchost.exe (2080)
0 :    |- svchost.exe (2088)
0 :    |- svchost.exe (2236)
0 :    |- svchost.exe (2260)
0 :       |- audiodg.exe (324)
0 :    |- svchost.exe (2324)
0 :    |- svchost.exe (2332)
0 :    |- svchost.exe (2344)
0 :    |- svchost.exe (2448)
0 :    |- svchost.exe (2532)
0 :    |- svchost.exe (2612)
0 :    |- spoolsv.exe (2656)
0 :    |- svchost.exe (2764)
0 :    |- svchost.exe (2800)
0 :    |- svchost.exe (2820)
0 :    |- svchost.exe (2860)
1 :    |- svchost.exe (2976)
[...]
```

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: 2024/02/22

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: 2024/02/22

Plugin Output

tcp/135/epmap

```
The Win32 process 'svchost.exe' is listening on this port (pid 892).

This process 'svchost.exe' (pid 892) 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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

Plugin Output

udp/500

```
The Win32 process 'svchost.exe' is listening on this port (pid 3232).

This process 'svchost.exe' (pid 3232) 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: 2024/02/22

Plugin Output

udp/1900

```
The Win32 process 'svchost.exe' is listening on this port (pid 956).

This process 'svchost.exe' (pid 956) 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: 2024/02/22

Plugin Output

udp/4500

```
The Win32 process 'svchost.exe' is listening on this port (pid 3232).

This process 'svchost.exe' (pid 3232) 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: 2024/02/22

Plugin Output

tcp/5040

```
The Win32 process 'svchost.exe' is listening on this port (pid 4048).

This process 'svchost.exe' (pid 4048) 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: 2024/02/22

Plugin Output

udp/5050

```
The Win32 process 'svchost.exe' is listening on this port (pid 4048).

This process 'svchost.exe' (pid 4048) 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: 2024/02/22

Plugin Output

udp/5353

```
The Win32 process 'msedge.exe' is listening on this port (pid 5428).
```

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: 2024/02/22

Plugin Output

udp/5355

```
The Win32 process 'svchost.exe' is listening on this port (pid 2324).

This process 'svchost.exe' (pid 2324) 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: 2024/02/22

Plugin Output

tcp/7680

```
The Win32 process 'svchost.exe' is listening on this port (pid 8252).

This process 'svchost.exe' (pid 8252) 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: 2024/02/22

Plugin Output

tcp/49664/dce-rpc

```
The Win32 process 'lsass.exe' is listening on this port (pid 656).

This process 'lsass.exe' (pid 656) 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: 2024/02/22

Plugin Output

tcp/49665/dce-rpc

```
The Win32 process 'wininit.exe' is listening on this port (pid 492).
```

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: 2024/02/22

Plugin Output

tcp/49666/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 1316).

This process 'svchost.exe' (pid 1316) 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: 2024/02/22

Plugin Output

tcp/49667/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 1332).

This process 'svchost.exe' (pid 1332) 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: 2024/02/22

Plugin Output

tcp/49668/dce-rpc

```
The Win32 process 'spoolsv.exe' is listening on this port (pid 2656).

This process 'spoolsv.exe' (pid 2656) 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: 2024/02/22

Plugin Output

tcp/49669/dce-rpc

```
The Win32 process 'services.exe' is listening on this port (pid 636).
```

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: 2024/02/22

Plugin Output

tcp/49670/dce-rpc

```
The Win32 process 'svchost.exe' is listening on this port (pid 3224).

This process 'svchost.exe' (pid 3224) is hosting the following Windows services :
PolicyAgent (@%SystemRoot%\System32\polstore.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: 2024/02/22

Plugin Output

tcp/49674

```
The Win32 process 'svchost.exe' is listening on this port (pid 3340).

This process 'svchost.exe' (pid 3340) 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: 2024/02/22

Plugin Output

udp/58558

```
The Win32 process 'svchost.exe' is listening on this port (pid 956).

This process 'svchost.exe' (pid 956) 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 : .\Windows10 VM
```

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: 2023/07/25

Plugin Output

tcp/445/cifs

```
- The SMB tests will be done as windows10 vm/******
```

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-1-5-21-3315527792-3692112875-3820317123

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: DESKTOP-96HJG8C
NetBIOS Domain Name: DESKTOP-96HJG8C
NetBIOS Computer Name: DESKTOP-96HJG8C
DNS Domain Name: DESKTOP-96HJG8C
DNS Computer Name: DESKTOP-96HJG8C
DNS Tree Name: unknown
Product Version: 10.0.19041
```

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 = 10.19045
Architecture = x64
Build lab extended = 19041.1.amd64fre.vb_release.191206-1406
```

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_22bbe startup parameters :
    Display name : CDPUserSvc_22bbe
    Service name : CDPUserSvc_22bbe
    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 : C:\Windows\system32\svchost [...]
```

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 Information [ Appinfo ]
Windows Audio Endpoint Builder [ AudioEndpointBuilder ]
Windows Audio [ Audiosrv ]
Base Filtering Engine [ BFE ]
Background Tasks Infrastructure Service [ BrokerInfrastructure ]
Bluetooth Audio Gateway Service [ BTAGService ]
AVCTP service [ BthAvctpSvc ]
Bluetooth Support Service [ bthserv ]
Connected Devices Platform Service [ CDPSvc ]
CoreMessaging [ CoreMessagingRegistrar ]
Cryptographic Services [ CryptSvc ]
DCOM Server Process Launcher [ DcomLaunch ]
Device Association Service [ DeviceAssociationService ]
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 ]
IKE and AuthIP IPsec Keying Modules [ IKEEXT ]
Microsoft Store Install Service [ InstallService ]
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 ]
Windows Defender Firewall [ mpssvc ]
Network Connection Broker [ NcbService ]
Network List Service [ netprofm ]
Network Location Awareness [ NlaSvc ]
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 [ SamSs ]
Task Scheduler [ Schedule ]
Windows Security Service [ SecurityHealthService ]
Payments and NFC/SE Manager [ SEMgrSvc ]
System Event Notification Servi [...]
```

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: 2024/02/22

Plugin Output

tcp/0

```
windows10

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_10.0.19041.3636_none_8262c6fdaad12a1c\MsoIrmProtector.doc
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.19041.3636_none_8cb7714fdf31ec17\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_10.0.19041.3636_none_8262c6fdaad12a1c\MsoIrmProtector.ppt
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.19041.3636_none_8cb7714fdf31ec17\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_10.0.19041.3636_none_8262c6fdaad12a1c\MsoIrmProtector.xls
    - C:\Windows\WinSxS\wow64_microsoft-windows-r..t-office-
protectors_31bf3856ad364e35_10.0.19041.3636_none_8cb7714fdf31ec17\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:\Program Files\WindowsApps\Microsoft.XboxApp_48.49.31001.0_x64__8wekyb3d8bbwe\Assets
\AchievementUnlocked.mp3
C:\Program Files\WindowsApps\Microsoft.ZuneVideo_10.19071.19011.0_x64__8wekyb3d8bbwe\Assets
\ImmersiveControl_Slider_Click_Sound.wma
```

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 windows10 vm :

- ADMIN$  - (readable,writable)
  + Content of this share :
..
addins
appcompat
apppatch
AppReadiness
assembly
bcastdvr
bfsvc.exe
BitLockerDiscoveryVolumeContents
Boot
bootstat.dat
Branding
CbsTemp
Containers
CSC
Cursors
debug
diagnostics
DiagTrack
DigitalLocker
Downloaded Program Files
DtcInstall.log
```

```
ELAMBKUP
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
PrintDialog
Professional.xml
Provisioning
regedit.exe
Registration
RemotePackages
rescache
Resources
SchCache
schemas
security
ServiceProfiles
ServiceState
servicing
Setup
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
Vss
```

```
- 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
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 windows10 vm:

  - 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.
```

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
```

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 :

 - KB5033909 ( https://support.microsoft.com/en-us/help/5033909 )
 - KB5034122 ( https://support.microsoft.com/en-us/help/5034122 )
 - KB5034763 ( https://support.microsoft.com/en-us/help/5034763 )
```

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 : Pacific Standard Time
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardName : @tzres.dll,-212
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightName : @tzres.dll,-211
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 : 0x000001E0
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\ActiveTimeBias : 0x000001E0
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightStart :
 00000300020002000000000000000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardStart :
 00000b000100020000000000000000
```

20862 - Mozilla Foundation Application Detection

Synopsis

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

Description

There is at least one instance of Firefox, Thunderbird, SeaMonkey, or the Mozilla browser installed on the remote Windows host.

See Also

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0672

Plugin Information

Published: 2006/02/05, Modified: 2023/08/10

Plugin Output

tcp/445/cifs

```
Product : Mozilla Firefox ESR
Path    : C:\Program Files (x86)\Mozilla Firefox
Version : 10.0.1
```

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: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.7.1
Nessus build : 20016
Plugin feed version : 202403021238
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Windows 10 VM Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.128.1
Port scanner(s) : wmi_netstat
Port range : 1-65535
Ping RTT : 14.565 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : yes, as '192.168.128.129\windows10 vm' via SMB
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
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 : 2024/3/3 0:52 GMT Standard Time
Scan duration : 1169 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: 2024/02/22

Plugin Output

tcp/0

```
Nessus was able to find 24 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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

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: 2024/02/22

Plugin Output

tcp/49670/dce-rpc

```
Port 49670/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: 2024/02/22

Plugin Output

tcp/49674

```
Port 49674/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: 2024/02/22

Plugin Output

udp/58558

```
Port 58558/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: 2024/02/22

Plugin Output

tcp/0

```
+ Network Interface Information :

 - Network Interface = [00000002] Intel(R) 82574L Gigabit Network Connection
 - MAC Address = 00:0C:29:B7:F1:32
 - IPAddress/IPSubnet = 192.168.128.129/255.255.255.0
 - IPAddress/IPSubnet = fe80::a94e:30a0:e7f4:46cf/64


+ Routing Information :

    Destination     Netmask         Gateway
    -----------     -------         -------
    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
    192.168.128.0   255.255.255.0   0.0.0.0
    192.168.128.129 255.255.255.255 0.0.0.0
    192.168.128.255 255.255.255.255 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
```

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: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows 10 Pro Build 19045
Confidence level : 100
Method : SMB_OS

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SinFP:!:
   P1:B11113:F0x12:W65392:O0204ffff:M1460:
   P2:B11113:F0x12:W65535:O0204ffff0103030801010402:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190801_7_p=49674


The remote host is running Microsoft Windows 10 Pro Build 19045
```

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  : 192.168.128.129\windows10 vm
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: 2024/02/21

Plugin Output

tcp/0

```
. You need to take the following 9 actions :

+ Install the following Microsoft patches :
- KB5034763 (2 vulnerabilities)
- KB5033909

[ Microsoft 3D Viewer app Multiple Remote Code Execution Vulnerabilities (September 2023) (181297) ]

+ Action to take : Update to the latest Microsoft 3D Viewer app via the Windows App Store.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).


[ Microsoft Edge (Chromium) < 122.0.2365.63 Multiple Vulnerabilities (191442) ]

+ Action to take : Upgrade to Microsoft Edge version 122.0.2365.63 or later.

+Impact : Taking this action will resolve 687 different vulnerabilities (CVEs).


[ Mozilla Firefox ESR < 68.5  Multiple Vulnerabilities (133677) ]

+ Action to take : Upgrade to Mozilla Firefox ESR version 68.5 or later.
```

```
+Impact : Taking this action will resolve 162 different vulnerabilities (CVEs).


[ Mozilla Firefox ESR < 68.6 Multiple Vulnerabilities (134407) ]

+ Action to take : Upgrade to Mozilla Firefox ESR version 68.6 or later.

+Impact : Taking this action will resolve 122 different vulnerabilities (CVEs).


[ Security Update for Forefront Endpoint Protection (June 2021) (150361) ]

+ Action to take : Enable automatic updates to update the malware engine for the relevant
 antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify
 that MMPE has been updated.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).


[ Security Updates for Windows Defender (November 2021) (154991) ]

+ Action to take : Enable automatic updates to update the malware engine for the relevant
 antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify
 that MMPE has been updated.

+Impact : Taking this action will resolve 10 different vulnerabilities (CVEs).


[ Windows Snip & Sketch/ Snipping Tool CVE-2023-28303 (Acropalypse) (177217) ]

+ Action to take : Upgrade to Snip & Sketch 10.2008.3001.0 for Windows 10, Snipping Tool
 11.2302.20.0 for Windows 11, or late [...]
```

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2023/07/31

Plugin Output

tcp/0

```
The remote host is up
The host replied to an ARP who-is query.
Hardware address : 00:0c:29:b7:f1:32
```

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-1-5-21-3315527792-3692112875-3820317123-1000
C:\\$Recycle.Bin\\S-1-5-21-3315527792-3692112875-3820317123-1001
C:\\$Recycle.Bin\\S-1-5-21-3315527792-3692112875-3820317123-1000\.
C:\\$Recycle.Bin\\S-1-5-21-3315527792-3692112875-3820317123-1000\..
C:\\$Recycle.Bin\\S-1-5-21-3315527792-3692112875-3820317123-1000\desktop.ini
C:\\$Recycle.Bin\\S-1-5-21-3315527792-3692112875-3820317123-1001\.
C:\\$Recycle.Bin\\S-1-5-21-3315527792-3692112875-3820317123-1001\..
C:\\$Recycle.Bin\\S-1-5-21-3315527792-3692112875-3820317123-1001\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

```
Windows10 VM
  - Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```

62042 - SMB QuickFixEngineering (QFE) Enumeration

Synopsis

The remote host has quick-fix engineering updates installed.

Description

By connecting to the host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via the registry.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/09/11, Modified: 2022/02/01

Plugin Output

tcp/0

```
Here is a list of quick-fix engineering updates installed on the
remote system :

KB5014032, Installed on: 2023/12/04
KB5015684, Installed on: 2023/12/04
KB5031988, Installed on: 2023/12/04
```

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)
  - Windows10 VM (id 1001)

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.
```

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

Synopsis

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

Description

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

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

Please note the following :

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

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

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

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0520

Plugin Information

Published: 2018/05/24, Modified: 2024/01/22

Plugin Output

tcp/445/cifs

```
Nessus was able to log into the remote host with no privilege or access
problems via the following :

User:       '192.168.128.129\windows10 vm'
Port:       445
Proto:      SMB
Method:     password
```

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: 2024/01/22

Plugin Output

tcp/445/cifs

```
Nessus was able to log in to the remote host via the following :

User:       '192.168.128.129\windows10 vm'
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

```
20240302222220.625531-480
```

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 192.168.128.1 to 192.168.128.129 :
192.168.128.1
192.168.128.129

Hop Count: 1
```

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\Public\Downloads\desktop.ini
C:\\Users\Windows10 VM\Downloads\desktop.ini
C:\\Users\Windows10 VM\Downloads\Firefox Setup 10.0.1esr.exe

Download folder content report attached.
```

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

```
Windows10 VM
  - {7d1d3a04-debb-4115-95cf-2f29da2920da} : C:\Users\Windows10 VM\Searches
  - {1b3ea5dc-b587-4786-b4ef-bd1dc332aeae} : C:\Users\Windows10 VM\AppData\Roaming\Microsoft\Windows
\Libraries
  - {374de290-123f-4565-9164-39c4925e467b} : C:\Users\Windows10 VM\Downloads
  - recent : C:\Users\Windows10 VM\AppData\Roaming\Microsoft\Windows\Recent
  - my video : C:\Users\Windows10 VM\Videos
  - my music : C:\Users\Windows10 VM\Music
  - {56784854-c6cb-462b-8169-88e350acb882} : C:\Users\Windows10 VM\Contacts
  - {bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968} : C:\Users\Windows10 VM\Links
  - {a520a1a4-1780-4ff6-bd18-167343c5af16} : C:\Users\Windows10 VM\AppData\LocalLow
  - sendto : C:\Users\Windows10 VM\AppData\Roaming\Microsoft\Windows\SendTo
  - start menu : C:\Users\Windows10 VM\AppData\Roaming\Microsoft\Windows\Start Menu
  - cookies : C:\Users\Windows10 VM\AppData\Local\Microsoft\Windows\INetCookies
  - personal : C:\Users\Windows10 VM\Documents
  - administrative tools : C:\Users\Windows10 VM\AppData\Roaming\Microsoft\Windows\Start Menu
\Programs\Administrative Tools
  - startup : C:\Users\Windows10 VM\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
  - nethood : C:\Users\Windows10 VM\AppData\Roaming\Microsoft\Windows\Network Shortcuts
  - history : C:\Users\Windows10 VM\AppData\Local\Microsoft\Windows\History
  - {4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4} : C:\Users\Windows10 VM\Saved Games
  - {00bcfc5a-ed94-4e48-96a1-3f6217f21990} : C:\Users\Windows10 VM\AppData\Local\Microsoft\Windows
\RoamingTiles
  - !do not use this registry key : Use the SHGetFolderPath or SHGetKnownFolderPath function instead
  - local appdata : C:\Users\Windows10 VM\AppData\Local
  - my pictures : C:\Users\Windows10 VM\Pictures
  - templates : C:\Users\Windows10 VM\AppData\Roaming\Microsoft\Windows\Templates
  - printhood : C:\Users\Windows10 VM\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
  - cache : C:\Users\Windows10 VM\AppData\Local\Microsoft\Windows\INetCache
  - desktop : C:\Users\Windows10 VM\Desktop
  - programs : [...]
```

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

```
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\services.exe
microsoft.windows.controlpanel
microsoft.getstarted_8wekyb3d8bbwe!app
c:\users\windows10 vm\downloads\firefox setup 10.0.1esr.exe
microsoft.windowscalculator_8wekyb3d8bbwe!app
microsoft.people_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x
microsoft.lockapp_cw5n1h2txyewy!windowsdefaultlockscreen
microsoft.windowsfeedbackhub_8wekyb3d8bbwe!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\services.msc
microsoft.windows.search_cw5n1h2txyewy!cortanaui
microsoft.windows.shell.rundialog
e7cf176e110c211b
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\administrative tools\services.lnk
microsoft.microsoftstickynotes_8wekyb3d8bbwe!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\useraccountcontrolsettings.exe
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\accessories\paint.lnk
ueme_ctlcuacount:ctor
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\microsoft edge.lnk
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\cmd.exe
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\ipconfig.exe
{f38bf404-1d43-42f2-9305-67de0b28fc23}\regedit.exe
msedge
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\snippingtool.exe
microsoft.windows.explorer
```

```
{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\system tools\command prompt.lnk
microsoft.windowsmaps_8wekyb3d8bbwe!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\mspaint.exe
ueme_ctlsession
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\administrative tools\registry editor.lnk
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\accessories\snipping tool.lnk
microsoft.windows.shellexperiencehost_cw5n1h2txyewy!app

Extended userassist report attached.
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

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: 2024/02/22

Plugin Output

tcp/445/cifs

```
The remote host returned the following caption from Win32_OperatingSystem:

Microsoft Windows 10 Pro
```

43830 - WMI Bluetooth Network Adapter Enumeration

Synopsis

The remote Windows host has a Bluetooth network adapter enabled.

Description

By connecting to the remote host with the supplied credentials, this plugin uses WMI to enumerate Bluetooth network adapters that are enabled on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/desktop/CIMWin32Prov/win32-networkadapter

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/01/08, Modified: 2024/02/22

Plugin Output

tcp/0

```
Here is the list of Bluetooth network adapters enabled on the remote
system :

+ [00000001] Bluetooth Device (Personal Area Network)

  - System Name  : DESKTOP-96HJG8C
  - Service Name : BthPan
  - Product Name : Bluetooth Device (Personal Area Network)
  - Name         : Bluetooth Device (Personal Area Network)
  - Manufacturer : Microsoft
  - MAC Address  : 14:13:33:8B:8B:06
```

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: 2024/02/22

Plugin Output

tcp/0

```
Here is a list of encryptable volumes available on the remote system :

+ DriveLetter C:

  - BitLocker Version : None
  - Conversion Status : Fully Decrypted
  - DeviceID : \\?\Volume{80858a2a-0000-0000-0000-300300000000}\
  - Encryption Method : None
  - Identification Field : None
  - Key Protectors : None Found
  - Lock Status : Unlocked
  - Percentage Encrypted : 0.0%
  - Protection Status : Protection Off
  - Size : 59.41 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: 2024/02/22

Plugin Output

tcp/0

```
Here is a list of quick-fix engineering updates installed on the
remote system :

+ KB5031988
  - Description : Update
  - InstalledOn : 12/4/2023

+ KB5015684
  - Description : Update
  - InstalledOn : 12/4/2023

+ KB5033372
  - Description : Security Update
  - InstalledOn : 12/4/2023

+ KB5014032
  - Description : Security Update
  - InstalledOn : 12/4/2023

+ KB5032907
  - Description : Update
  - InstalledOn : 12/4/2023
```

```
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'.
```

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: 2024/02/22

Plugin Output

tcp/0

```
Nessus enumerated the following Windows features :

  - Internet-Explorer-Optional-amd64
  - MSRDC-Infrastructure
  - MediaPlayback
  - MicrosoftWindowsPowerShellV2
  - MicrosoftWindowsPowerShellV2Root
  - NetFx4-AdvSrvs
  - Printing-Foundation-Features
  - Printing-Foundation-InternetPrinting-Client
  - Printing-PrintToPDFServices-Features
  - Printing-XPSServices-Features
```

```
  - SearchEngine-Client-Package
  - SmbDirect
  - WCF-Services45
  - WCF-TCP-PortSharing45
  - Windows-Defender-Default-Definitions
  - 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-1-5-21-3315527792-3692112875-3820317123-1001
```

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: 2024/02/22

Plugin Output

tcp/0

```
+ Computer System Product
  - IdentifyingNumber : VMware-56 4d 0a 9c 05 4e df 36-d1 35 6b 41 08 b7 f1 32
  - Description       : Computer System Product
  - Vendor            : VMware, Inc.
  - Name              : VMware Virtual Platform
  - UUID              : 9C0A4D56-4E05-36DF-D135-6B4108B7F132
  - Version           : None
```

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: {ce802571-3cfc-4623-baff-2528e93cd16c}
Network Connection : Ethernet0
DhcpNameServer: 192.168.128.1

Interface: Default
DhcpNameServer: 192.168.128.1
```

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: 2024/02/22

Plugin Output

tcp/0

```
Path                          : C:\Program Files\Windows Defender\
Version                       : 4.18.1909.6
Engine Version                : 1.1.16400.2
Malware Signature Timestamp : Sep. 24, 2019 at 05:12:58 GMT
Malware Signature Version   : 1.303.25.0
```

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: DefaultAccount
  SID: S-1-5-21-3315527792-3692112875-3820317123-503
  DisableCMD: Unset

Username: Administrator
  SID: S-1-5-21-3315527792-3692112875-3820317123-500
  DisableCMD: Unset

Username: Windows10 VM
  SID: S-1-5-21-3315527792-3692112875-3820317123-1001
  DisableCMD: Unset

Username: WDAGUtilityAccount
  SID: S-1-5-21-3315527792-3692112875-3820317123-504
```

```
    DisableCMD: Unset

  Username: Guest
    SID: S-1-5-21-3315527792-3692112875-3820317123-501
    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: 2024/02/22

Plugin Output

tcp/0

```
Device Name         : Microsoft Basic Display Adapter
Driver File Version : 10.0.19041.3636
Driver Date         : 06/21/2006
Video Processor     : V M ware, Inc. VBE support 2.0
```

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: 2024/02/28

Plugin Output

tcp/0

```
Windows accounts enumerated. Results output to DB.
User data gathered in scan starting at : 2024/3/3 0:52 GMT Standard Time
```

92423 - Windows Explorer Recently Executed Programs

Synopsis

Nessus was able to enumerate recently executed programs on the remote host.

Description

Nessus was able to find evidence of program execution using Windows Explorer registry logs and settings.

See Also

http://www.forensicswiki.org/wiki/LastVisitedMRU

http://www.nessus.org/u?7e00b191

http://www.nessus.org/u?ac4dd3fb

http://www.nessus.org/u?c409cb41

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/07/19, Modified: 2019/08/15

Plugin Output

tcp/0

```
a
services\1

 MRU programs details in attached report.
```

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

```
LSA Protection Key \SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL not found.
```

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: 1033

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 :

 DESKTOP-96HJG8C  = File Server Service
 DESKTOP-96HJG8C  = Computer name
 WORKGROUP        = Workgroup / Domain name

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

   00:0c:29:b7:f1:32
```

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\APPLICATIONFRAMEHOST.EXE-CCEEF759.pf
  - \Windows\prefetch\ARP.EXE-2BC38967.pf
  - \Windows\prefetch\AUDIODG.EXE-BDFD3029.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-9BA7511C.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-AA318346.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-BB001E4D.pf
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-298EACB3.pf
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-CC9DA465.pf
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-D679F7DE.pf
  - \Windows\prefetch\BYTECODEGENERATOR.EXE-C1E9BCE6.pf
  - \Windows\prefetch\CMD.EXE-4A81B364.pf
  - \Windows\prefetch\CONHOST.EXE-1F3E9D7E.pf
  - \Windows\prefetch\CONSENT.EXE-531BD9EA.pf
  - \Windows\prefetch\CSC.EXE-67679278.pf
```

```
  - \Windows\prefetch\CSRSS.EXE-3FE41F7E.pf
  - \Windows\prefetch\CTFMON.EXE-9450846B.pf
  - \Windows\prefetch\CVTRES.EXE-F2B7602E.pf
  - \Windows\prefetch\DEFRAG.EXE-588F90AD.pf
  - \Windows\prefetch\DISM.EXE-DE199F71.pf
  - \Windows\prefetch\DISMHOST.EXE-878F82CE.pf
  - \Windows\prefetch\DLLHOST.EXE-0F564EEF.pf
  - \Windows\prefetch\DLLHOST.EXE-28A8211F.pf
  - \Windows\prefetch\DLLHOST.EXE-504C779A.pf
  - \Windows\prefetch\DLLHOST.EXE-570206E5.pf
  - \Windows\prefetch\DLLHOST.EXE-5E46FA0D.pf
  - \Windows\prefetch\DLLHOST.EXE-61F58501.pf
  - \Windows\prefetch\DLLHOST.EXE-766398D2.pf
  - \Windows\prefetch\DLLHOST.EXE-7CE224E3.pf
  - \Windows\prefetch\DLLHOST.EXE-A8DE6D5B.pf
  - \Windows\prefetch\DLLHOST.EXE-BFD940A4.pf
  - \Windows\prefetch\DLLHOST.EXE-D8E67ED6.pf
  - \Windows\prefetch\DLLHOST.EXE-ECB71776.pf
  - \Windows\prefetch\DLLHOST.EXE-F2DCEF0D.pf
  - \Windows\prefetch\DLLHOST.EXE-FC981FFE.pf
  - \Windows\prefetch\DRVINST.EXE-4CB4314A.pf
  - \Windows\prefetch\DWM.EXE-6FFD3DA8.pf
  - \Windows\prefetch\ELEVATION_SERVICE.EXE-B812699C.pf
  - \Windows\prefetch\EXPLORER.EXE-A80E4F97.pf
  - \Windows\prefetch\FILESYNCCONFIG.EXE-14FB515D.pf
  - \W [...]
```

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: 2024/02/22

Plugin Output

tcp/445/cifs

```
--- Microsoft Shared Fax Driver ---

  Path               : C:\Windows\system32\spool\DRIVERS\x64\3\FXSDRV.DLL
  Version            : 10.0.19041.3636
  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            : 10.0.19041.3803
  Supported Platform : Windows x64

  Path               : C:\Windows\system32\spool\DRIVERS\W32X86\3\mxdwdrv.dll
  Version            : 10.0.19041.3803
  Supported Platform : Windows NT x86

--- Microsoft Print To PDF ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_906f4b456b58c7f3\Amd64\mxdwdrv.dll
  Version            : 10.0.19041.3636
  Supported Platform : Windows x64
```

```
--- Microsoft Software Printer Driver ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_906f4b456b58c7f3\Amd64\mxdwdrv.dll
  Version            : 10.0.19041.1
  Supported Platform : Windows x64

--- Microsoft XPS Document Writer v4 ---

  Path               : C:\Windows\System32\DriverStore\FileRepository
\ntprint.inf_amd64_906f4b456b58c7f3\Amd64\mxdwdrv.dll
  Version            : 10.0.19041.3636
  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-3V66T

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: 2024/02/22

Plugin Output

tcp/445/cifs

```
  -1527c705-839a-4832-9118-54d4Bd6a0c89
      Version : 10.0.19041.3636
      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 : 10.0.19041.3636
      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 : 10.0.19041.3636
      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 : 10.0.19041.3636
      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 : 1000.19041.3636.0
    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 : 10.0.19041.3636
    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 : 10.0.19041.3636
    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 : 10.0.1 [...]
```