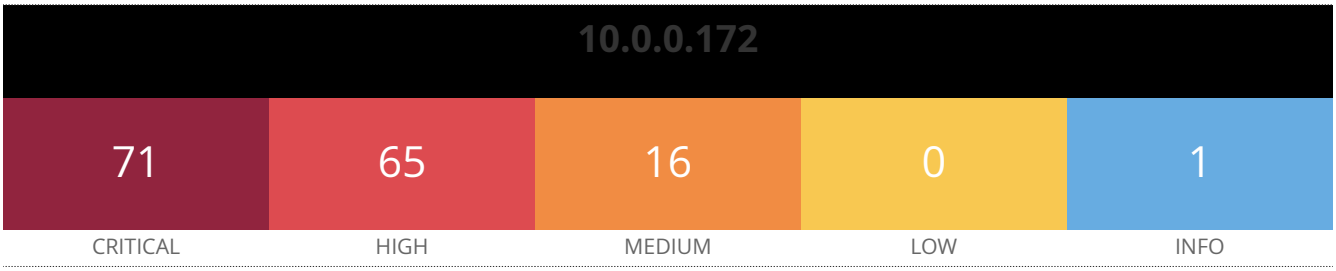
Windows Scanner Lab

Report generated by Nessus™ Sun, 07 Aug 2022 21:12:15 Central Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host



Scan Information

Start time:	Sun Aug 7 20:55:36 2022
End time:	Sun Aug 7 21:12:15 2022

Host Information

Netbios Name:	DESKTOP-O5BOULF
IP:	10.0.0.172
MAC Address:	22:A3:38:26:F5:44 00:0C:29:0D:AC:C2
OS:	Microsoft Windows 10 Pro

Vulnerabilities

60043 - Firefox < 14.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 14.0 and thus, 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, CVE-2012-1949)

- 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)

- An out-of-bounds read error exists related to the color management library (QCMS). (CVE-2012-1960)

- 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 '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/mfsa2012-50/

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/mfsa2012-55/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-56/

Solution

Upgrade to Firefox 14.0 or later.

Risk Factor

Critical

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	54572
BID	54573
BID	54574
BID	54575
BID	54576
BID	54577
BID	54578
BID	54579
BID	54580
BID	54582
BID	54583
BID	54584
BID	54585
BID	54586
CVE	CVE-2012-1948
CVE	CVE-2012-1949
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-2012-1960
CVE	CVE-2012-1961
CVE	CVE-2012-1962
CVE	CVE-2012-1963
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 : 3.6.12
Fixed version     : 14.0
```

61715 - Firefox < 15.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 15.0 and thus, is potentially affected by the following security issues :

- An error exists related to 'Object.defineProperty'

and the location object and can allow cross-site scripting attacks. (CVE-2012-1956)

- Unspecified memory safety issues exist. (CVE-2012-1970, CVE-2012-1971)

- 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 'about:newtab' and the browser's history. This error can allow a newly opened tab to further open a new window and navigate to the privileged 'about:newtab' page leading to possible privilege escalation. (CVE-2012-3965)

- 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)

- A 'Graphite 2' library memory corruption error exists.

(CVE-2012-3971)

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

- Remote debugging is possible even when disabled and the 'HTTPMonitor' extension is enabled. (CVE-2012-3973)

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

- The DOM parser can unintentionally load linked resources in extensions. (CVE-2012-3975)

- 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)

- SPDY's request header compression leads to information leakage, which can allow private data such as session cookies to be extracted, even over an SSL connection.

(CVE-2012-4930)

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/mfsa2012-59/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-60/
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/mfsa2012-64/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-65/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-66/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-67/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-68/
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/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-73/

Solution

Upgrade to Firefox 15.0 or later.

Risk Factor

Critical

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	55256

BID	55257
BID	55260
BID	55264
BID	55266
BID	55274
BID	55276
BID	55278
BID	55292
BID	55304
BID	55306
BID	55308
BID	55310
BID	55311
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-2012-1956
CVE	CVE-2012-1970
CVE	CVE-2012-1971
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-2012-3965
CVE	CVE-2012-3966
CVE	CVE-2012-3968
CVE	CVE-2012-3969
CVE	CVE-2012-3970
CVE	CVE-2012-3971
CVE	CVE-2012-3972
CVE	CVE-2012-3973
CVE	CVE-2012-3974
CVE	CVE-2012-3975
CVE	CVE-2012-3976
CVE	CVE-2012-3978
CVE	CVE-2012-3980
CVE	CVE-2012-4930
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: 2012/08/29, Modified: 2019/12/04

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
  Fixed version     : 15.0
```

62580 - Firefox < 16.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 16.0 and thus, 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)

- '<select>' elements can be abused to cover arbitrary portions of a newly loaded page and may also be utilized for click-jacking attacks. (CVE-2012-3984, CVE-2012-5354)

- A violation in the HTML specification for 'document.domain' behavior can be abused, potentially leading to cross-site scripting attacks. (CVE-2012-3985)

- 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)

- A potentially exploitable crash can be caused when making an invalid cast using the 'instanceof' operator on certain types of JavaScript objects. (CVE-2012-3989)

- 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/mfsa2012-80/
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/mfsa2012-76/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-75/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-74/

Solution

Upgrade to Firefox 16.0 or later.

Risk Factor

Critical

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	55926
BID	55927
BID	55930
BID	55931
BID	55932
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
BID	57181
CVE	CVE-2012-3982
CVE	CVE-2012-3983
CVE	CVE-2012-3984
CVE	CVE-2012-3985
CVE	CVE-2012-3986
CVE	CVE-2012-3988
CVE	CVE-2012-3989
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
CVE	CVE-2012-5354
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 : 3.6.12
Fixed version     : 16.0
```

62589 - Firefox < 16.0.1 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 16.0.1 and is therefore potentially affected by the following security issues :

- An unspecified error related to the WebSockets implementation and the function 'mozilla::net::FailDelayManager::Lookup' can allow application crashes and potentially, arbitrary code execution. (CVE-2012-4191)

- 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/mfsa2012-88/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-89/

Solution

Upgrade to Firefox 16.0.1 or later.

Risk Factor

Critical

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	56153
BID	56154
BID	56155

CVE	CVE-2012-4191
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 : 3.6.12
Fixed version     : 16.0.1
```

62998 - Firefox < 17.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 17.0 and thus, 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-2012-5842, 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 SVG text and CSS properties that could lead to application crashes. (CVE-2012-5836)

- A bookmarked, malicious 'javascript:' URL could allow execution of local executables. (CVE-2012-4203)

- The JavaScript function 'str_unescape' could allow arbitrary code execution. (CVE-2012-4204)

- 'XMLHttpRequest' objects inherit incorrect principals when created in sandboxes that could allow cross-site request forgery attacks (CSRF). (CVE-2012-4205)

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

- 'XrayWrappers' can expose DOM properties that are not meant to be accessible outside of the chrome compartment. (CVE-2012-4208)

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

charset, frames and the 'location' object, the 'Style Inspector', 'Developer Toolbar' 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-2012-5837, 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-2012-4212, CVE-2012-4213, CVE-2012-4214, CVE-2012-4215, CVE-2012-4216, CVE-2012-4217, CVE-2012-4218, CVE-2012-5829, CVE-2012-5830, CVE-2012-5833, CVE-2012-5835, CVE-2012-5838, CVE-2012-5839, CVE-2012-5840)

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/mfsa2012-94/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-95/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-96/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-97/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-99/
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/mfsa2012-102/
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 17.0 or later.

Risk Factor

Critical

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	56611
BID	56612
BID	56613
BID	56614
BID	56616
BID	56618
BID	56621
BID	56623
BID	56625
BID	56627
BID	56628
BID	56629
BID	56630
BID	56631
BID	56632
BID	56633

BID	56634
BID	56635
BID	56636
BID	56637
BID	56638
BID	56639
BID	56640
BID	56641
BID	56642
BID	56643
BID	56644
BID	56645
BID	56646
CVE	CVE-2012-4201
CVE	CVE-2012-4202
CVE	CVE-2012-4203
CVE	CVE-2012-4204
CVE	CVE-2012-4205
CVE	CVE-2012-4206
CVE	CVE-2012-4207
CVE	CVE-2012-4208
CVE	CVE-2012-4209
CVE	CVE-2012-4210
CVE	CVE-2012-4212
CVE	CVE-2012-4213
CVE	CVE-2012-4214
CVE	CVE-2012-4215
CVE	CVE-2012-4216
CVE	CVE-2012-4217
CVE	CVE-2012-4218
CVE	CVE-2012-5829
CVE	CVE-2012-5830
CVE	CVE-2012-5833
CVE	CVE-2012-5835
CVE	CVE-2012-5836
CVE	CVE-2012-5837
CVE	CVE-2012-5838
CVE	CVE-2012-5839
CVE	CVE-2012-5840
CVE	CVE-2012-5841
CVE	CVE-2012-5842
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 : 3.6.12
Fixed version     : 17.0
```

63551 - Firefox < 18.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 18.0 and thus, is potentially affected by the following security issues :

- Multiple, unspecified use-after-free, out-of-bounds read and buffer overflow errors exist. (CVE-2012-5829, CVE-2013-0760, 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 can lead potentially exploitable crashes. (CVE-2013-0746)

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

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

- An unspecified memory corruption issue exists.
(CVE-2013-0749, CVE-2013-0769, CVE-2013-0770)

- 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 and can allow arbitrary code execution. (CVE-2013-0757)

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

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

- An error exists related to SSL and threading that can 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)

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 18.0 or later.

Risk Factor

Critical

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	57199
BID	57203
BID	57204
BID	57205
BID	57207
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-2013-0760
CVE	CVE-2013-0761
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-2013-0770
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 : 3.6.12
Fixed version     : 18.0
```

64723 - Firefox < 19.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 19.0 and thus, is potentially affected by the following security issues :

- Numerous memory safety errors exist. (CVE-2013-0783, CVE-2013-0784)

- An out-of-bounds read error exists related to the handling of GIF images. (CVE-2013-0772)

- An error exists related to 'WebIDL' object wrapping that has an unspecified impact. (CVE-2013-0765)

- An error exists related to Chrome Object Wrappers (COW) or System Only Wrappers (SOW) that could allow security bypass. (CVE-2013-0773)

- The file system location of the active browser profile could be disclosed and used in further attacks. (CVE-2013-0774)

- A use-after-free error exists in the function 'nsImageLoadingContent'. (CVE-2013-0775)

- Spoofing HTTPS URLs is possible due to an error related to proxy '407' responses and embedded script code. (CVE-2013-0776)

- A heap-based use-after-free error exists in the function 'nsDisplayBoxShadowOuter::Paint'. (CVE-2013-0777)

- An out-of-bounds read error exists in the function 'ClusterIterator::NextCluster'. (CVE-2013-0778)

- An out-of-bounds read error exists in the function 'nsCodingStateMachine::NextState'. (CVE-2013-0779)

- A heap-based use-after-free error exists in the function 'nsOverflowContinuationTracker::Finish'. (CVE-2013-0780)

- A heap-based use-after-free error exists in the function 'nsPrintEngine::CommonPrint'. (CVE-2013-0781)

- A heap-based buffer overflow error exists in the function 'nsSaveAsCharset::DoCharsetConversion'. (CVE-2013-0782)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2013-21/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-22/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-23/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-24/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-25/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-26/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-27/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-28/

Solution

Upgrade to Firefox 19.0 or later.

Risk Factor

Critical

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	58034
BID	58036
BID	58037
BID	58038
BID	58040
BID	58041
BID	58042
BID	58043
BID	58044
BID	58047
BID	58048
BID	58049
BID	58050
BID	58051
CVE	CVE-2013-0765
CVE	CVE-2013-0772
CVE	CVE-2013-0773
CVE	CVE-2013-0774
CVE	CVE-2013-0775
CVE	CVE-2013-0776
CVE	CVE-2013-0777
CVE	CVE-2013-0778
CVE	CVE-2013-0779
CVE	CVE-2013-0780

CVE	CVE-2013-0781
CVE	CVE-2013-0782
CVE	CVE-2013-0783
CVE	CVE-2013-0784

Plugin Information

Published: 2013/02/20, Modified: 2019/12/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 19.0
```

65806 - Firefox < 20 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 20 and is, therefore, potentially affected by the following vulnerabilities :

- Various memory safety issues exist. (CVE-2013-0788, CVE-2013-0789)

- An out-of-bounds memory read error exists related to 'CERT_DecodeCertPackage' and certificate decoding.
(CVE-2013-0791)

- A memory corruption error exists related to PNG image files when 'gfx.color_management.enablev4' is manually enabled in the application's configuration.
(CVE-2013-0792)

- An error exists related to navigation, history and improper 'baseURI' property values that could allow cross-site scripting attacks. (CVE-2013-0793)

- An error exists related to tab-modal dialog boxes that could be used in phishing attacks. (CVE-2013-0794)

- An error exists related to 'cloneNode' that can allow 'System Only Wrapper' (SOW) to be bypassed, thus violating the same origin policy and possibly leading to privilege escalation and code execution.
(CVE-2013-0795)

- A DLL loading vulnerability exists that could lead to code execution. (CVE-2013-0797)

- A buffer overflow error exists related to the Mozilla Maintenance Service. (CVE-2013-0799)

- An out-of-bounds write error exists related to the Cairo graphics library. (CVE-2013-0800)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2013-30/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-31/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-32/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-34/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-36/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-37/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-38/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-39/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-40/

Solution

Upgrade to Firefox 20 or later.

Risk Factor

Critical

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	58819
BID	58821
BID	58824
BID	58825
BID	58826
BID	58827
BID	58828
BID	58835
BID	58836
BID	58837
CVE	CVE-2013-0788
CVE	CVE-2013-0789
CVE	CVE-2013-0791
CVE	CVE-2013-0792
CVE	CVE-2013-0793
CVE	CVE-2013-0794
CVE	CVE-2013-0795
CVE	CVE-2013-0797
CVE	CVE-2013-0799
CVE	CVE-2013-0800

Plugin Information

Published: 2013/04/04, Modified: 2019/11/27

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
```

```
  Installed version : 3.6.12
  Fixed version     : 20.0
```

66480 - Firefox < 21.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 21.0 and is, therefore, potentially affected by the following vulnerabilities :

- Various memory safety issues exist. (CVE-2013-0801, CVE-2013-1669)

- It is possible to call a content level constructor that allows for the constructor to have chrome privileged access. (CVE-2013-1670)

- An information leakage exists because the file input control has access to the full path. (CVE-2013-1671)

- A local privilege escalation issues exists in the Mozilla Maintenance Service. (CVE-2013-1672)

- The Mozilla Maintenance Service on Windows is vulnerable to a previously fixed privilege escalation attack. Note that new installations of Firefox after version 12 are not affected by this issue. (CVE-2013-1673, CVE-2012-1942)

- A use-after-free vulnerability exists when resizing video while playing. (CVE-2013-1674)

- Some 'DOMSVGZoomEvent' functions are used without being properly initialized, which could lead to information disclosure. (CVE-2013-1675)

- Multiple memory corruption issues exist. (CVE-2013-1676, CVE-2013-1677, CVE-2013-1678, CVE-2013-1679, CVE-2013-1680, CVE-2013-1681)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2013-41/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-42/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-43/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-44/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-45/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-46/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-47/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-48/

Solution

Upgrade to Firefox 21.0 or later.

Risk Factor

Critical

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	53803
BID	59852
BID	59855
BID	59858
BID	59859
BID	59860
BID	59861
BID	59862
BID	59863
BID	59864
BID	59865
BID	59868
BID	59869
BID	59870
BID	59872
BID	59873
CVE	CVE-2012-1942
CVE	CVE-2013-0801
CVE	CVE-2013-1669
CVE	CVE-2013-1670
CVE	CVE-2013-1671
CVE	CVE-2013-1672
CVE	CVE-2013-1673
CVE	CVE-2013-1674
CVE	CVE-2013-1675
CVE	CVE-2013-1676
CVE	CVE-2013-1677
CVE	CVE-2013-1678
CVE	CVE-2013-1679
CVE	CVE-2013-1680
CVE	CVE-2013-1681
XREF	CISA-KNOWN-EXPLOITED:2022/03/24

Plugin Information

Published: 2013/05/16, Modified: 2022/03/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 21.0
```

66993 - Firefox < 22.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 22.0 and is, therefore, potentially affected by the following vulnerabilities :

- Various, unspecified memory safety issues exist.

(CVE-2013-1682, CVE-2013-1683)

- Heap-use-after-free errors exist related to 'LookupMediaElementURITable', 'nsIDocument::GetRootElement' and 'mozilla::ResetDir'.

(CVE-2013-1684, CVE-2013-1685, CVE-2013-1686)

- An error exists related to 'XBL scope', 'System Only Wrappers' (SOW) and chrome-privileged pages that could allow cross-site scripting attacks. (CVE-2013-1687)

- An error exists related to the 'profiler' that could allow arbitrary code execution. (CVE-2013-1688)

- An error related to 'onreadystatechange' and unmapped memory could cause application crashes and allow arbitrary code execution. (CVE-2013-1690)

- The application sends data in the body of XMLHttpRequest (XHR) HEAD requests and could aid in cross-site request forgery attacks. (CVE-2013-1692)

- An error related to the processing of SVG content could allow a timing attack to disclose information across domains. (CVE-2013-1693)

- An error exists related to 'PreserveWrapper' and the 'preserved-wrapper' flag that could cause potentially exploitable application crashes. (CVE-2013-1694)

- An error exists related to '<iframe sandbox>'

restrictions that could allow a bypass of these restrictions. (CVE-2013-1695)

- The 'X-Frame-Options' header is ignored in certain situations and can aid in click-jacking attacks.

(CVE-2013-1696)

- An error exists related to the 'toString' and 'valueOf'

methods that could allow 'XrayWrappers' to be bypassed.

(CVE-2013-1697)

- An error exists related to the 'getUserMedia'

permission dialog that could allow a user to be tricked into giving access to unintended domains.

(CVE-2013-1698)

- Homograph domain spoofing protection is incomplete and certain attacks are still possible using Internationalized Domain Names (IDN). (CVE-2013-1699)

- An error exists related to the 'Mozilla Maintenance Service' on Windows that could allow insecure updates.

(CVE-2013-1700)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2013-49/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-50/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-51/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-52/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-53/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-54/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-55/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-56/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-57/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-58/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-59/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-60/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-61/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-62/

Solution

Upgrade to Firefox 22.0 or later.

Risk Factor

Critical

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	60688
BID	60765
BID	60766
BID	60768
BID	60773
BID	60774
BID	60776

BID	60777
BID	60778
BID	60779
BID	60783
BID	60784
BID	60785
BID	60787
BID	60789
BID	60790
BID	60791
CVE	CVE-2013-1682
CVE	CVE-2013-1683
CVE	CVE-2013-1684
CVE	CVE-2013-1685
CVE	CVE-2013-1686
CVE	CVE-2013-1687
CVE	CVE-2013-1688
CVE	CVE-2013-1690
CVE	CVE-2013-1692
CVE	CVE-2013-1693
CVE	CVE-2013-1694
CVE	CVE-2013-1695
CVE	CVE-2013-1696
CVE	CVE-2013-1697
CVE	CVE-2013-1698
CVE	CVE-2013-1699
CVE	CVE-2013-1700
XREF	CISA-KNOWN-EXPLOITED:2022/04/18
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: 2013/06/26, Modified: 2022/03/29

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 22.0
```

69269 - Firefox < 23.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 23.0 and is, therefore, potentially affected by the following vulnerabilities :

- Various errors exist that could allow memory corruption conditions. (CVE-2013-1701, CVE-2013-1702)

- Use-after-free errors exist related to DOM modification when using 'SetBody' and generating a 'Certificate Request Message'. (CVE-2013-1704, CVE-2013-1705)

- Errors exist related to the update service and 'maintenanceservice.exe' that could allow buffer overflows when handling unexpectedly long path values.

(CVE-2013-1706, CVE-2013-1707)

- An error exists in the function 'nsCString::CharAt'

that could allow application crashes when decoding specially crafted WAV audio files. (CVE-2013-1708)

- Unspecified errors exist related to HTML frames and history handling, 'XrayWrappers', JavaScript URI handling and web workers using 'XMLHttpRequest' that could allow cross-site scripting attacks.

(CVE-2013-1709, CVE-2013-1711, CVE-2013-1713, CVE-2013-1714)

- An unspecified error exists related to generating 'Certificate Request Message Format' (CRMF) requests that could allow cross-site scripting attacks.

(CVE-2013-1710)

- DLL path loading errors exist related to the update service, full installer and the stub installer that could allow execution of arbitrary code.

(CVE-2013-1712, CVE-2013-1715)

- An error exists related to Java applets and 'file:///'

URIs that could allow read-only access to arbitrary files. (CVE-2013-1717)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2013-63/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-64/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-65/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-66/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-67/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-68/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-69/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-70/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-71/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-72/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-73/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-74/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-75/

Solution

Upgrade to Firefox 23.0 or later.

Risk Factor

Critical

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	61864
BID	61867
BID	61869
BID	61871
BID	61872
BID	61873
BID	61874
BID	61875
BID	61876
BID	61877
BID	61878
BID	61882
BID	61883
BID	61896
BID	61900
CVE	CVE-2013-1701
CVE	CVE-2013-1702
CVE	CVE-2013-1704
CVE	CVE-2013-1705
CVE	CVE-2013-1706
CVE	CVE-2013-1707

CVE	CVE-2013-1708
CVE	CVE-2013-1709
CVE	CVE-2013-1710
CVE	CVE-2013-1711
CVE	CVE-2013-1712
CVE	CVE-2013-1713
CVE	CVE-2013-1714
CVE	CVE-2013-1715
CVE	CVE-2013-1717
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: 2013/08/08, Modified: 2019/11/27

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
```

```
    Fixed version     : 23.0
```

69993 - Firefox < 24.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 24.0 and is, therefore, potentially affected by the following vulnerabilities :

- Memory issues exist in the browser engine that could allow for denial of service or arbitrary code execution.

(CVE-2013-1718, CVE-2013-1719)

- The HTML5 Tree Builder does not properly maintain states, which could result in a denial of service or possible arbitrary code execution. (CVE-2013-1720)

- The ANGLE library is vulnerable to an integer overflow, which could result in a denial of service or arbitrary code execution. (CVE-2013-1721)

- Multiple use-after-free problems exist that could result in denial of service attacks or arbitrary code execution. (CVE-2013-1722, CVE-2013-1724, CVE-2013-1735, CVE-2013-1736, CVE-2013-1738)

- The NativeKey widget does not properly terminate key messages, possibly leading to a denial of service attack.

(CVE-2013-1723)

- Incorrect scope handling for JavaScript objects with compartments could result in denial of service or possibly arbitrary code execution. (CVE-2013-1725)

- Local users can gain the same privileges as the Mozilla Updater because the application does not ensure exclusive access to the update file. An attacker could exploit this by inserting a malicious file into the update file. (CVE-2013-1726)

- Sensitive information can be obtained via unspecified vectors because the IonMonkey JavaScript does not properly initialize memory. (CVE-2013-1728)

- A JavaScript compartment mismatch can result in a denial of service or arbitrary code execution. Versions of Firefox 20 or greater are not susceptible to the arbitrary code execution mentioned above.

(CVE-2013-1730)

- A buffer overflow is possible because of an issue with multi-column layouts. (CVE-2013-1732)

- An object is not properly identified during use of user-defined getter methods on DOM proxies. This could result in access restrictions being bypassed.

(CVE-2013-1737)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2013-76/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-77/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-78/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-79/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-80/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-81/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-82/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-83/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-85/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-88/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-89/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-90/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-91/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-92/

Solution

Upgrade to Firefox 24.0 or later.

Risk Factor

Critical

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	62460
BID	62462
BID	62463
BID	62464
BID	62465
BID	62466
BID	62467
BID	62468
BID	62469
BID	62470
BID	62472
BID	62473
BID	62475

BID	62478
BID	62479
BID	62482
CVE	CVE-2013-1718
CVE	CVE-2013-1719
CVE	CVE-2013-1720
CVE	CVE-2013-1721
CVE	CVE-2013-1722
CVE	CVE-2013-1723
CVE	CVE-2013-1724
CVE	CVE-2013-1725
CVE	CVE-2013-1726
CVE	CVE-2013-1728
CVE	CVE-2013-1730
CVE	CVE-2013-1732
CVE	CVE-2013-1735
CVE	CVE-2013-1736
CVE	CVE-2013-1737
CVE	CVE-2013-1738

Plugin Information

Published: 2013/09/19, Modified: 2019/11/27

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 24.0
```

70716 - Firefox < 25.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 25.0 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)

- Arbitrary HTML content can be put into 'select'

elements. This can be used to spoof the displayed address bar, leading to clickjacking and other spoofing attacks. (CVE-2013-5593)

- 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)

- A race condition exists during image collection on large web pages that could result in a denial of service or arbitrary code execution. (CVE-2013-5596)

- 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, CVE-2013-5603)

- Improper handling of the 'IFRAME' element in PDF.js could result in reading arbitrary files and arbitrary JavaScript code execution. (CVE-2013-5598)

- 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/mfsa2013-94/

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/mfsa2013-97/

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

https://www.mozilla.org/en-US/security/advisories/mfsa2013-99/

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

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

https://www.mozilla.org/en-US/security/advisories/mfsa2013-102/

Solution

Upgrade to Firefox 25.0 or later.

Risk Factor

Critical

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	63416
BID	63417
BID	63418
BID	63419
BID	63420
BID	63421
BID	63422
BID	63423
BID	63424
BID	63427
BID	63428
BID	63429
BID	63430
CVE	CVE-2013-1739
CVE	CVE-2013-5590
CVE	CVE-2013-5591
CVE	CVE-2013-5592
CVE	CVE-2013-5593
CVE	CVE-2013-5595
CVE	CVE-2013-5596
CVE	CVE-2013-5597
CVE	CVE-2013-5598
CVE	CVE-2013-5599
CVE	CVE-2013-5600

CVE	CVE-2013-5601
CVE	CVE-2013-5602
CVE	CVE-2013-5603
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 : 3.6.12
Fixed version     : 25.0
```

71347 - Firefox < 26.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 26.0 and is, therefore, potentially affected by the following vulnerabilities :

- Memory issues exist in the browser engine that could result in a denial of service or arbitrary code execution. (CVE-2013-5609, CVE-2013-5610)

- An issue exists where the notification for a Web App installation could persist from one website to another website. This could be used by a malicious website to trick a user into installing an application from one website while making it appear to come from another website. (CVE-2013-5611)

- Cross-site scripting filtering evasion may be possible due to character encodings being inherited from a previously visited website when character set encoding is missing from the current website. (CVE-2013-5612)

- Two use-after-free vulnerabilities exist in the functions for synthetic mouse movement handling.

(CVE-2013-5613)

- Sandbox restrictions may be bypassed because 'iframe sandbox' restrictions are not properly applied to 'object' elements in sandboxed iframes. (CVE-2013-5614)

- An issue exists in which 'GetElementIC' typed array stubs can be generated outside observed typesets. This could lead to unpredictable behavior with a potential security impact. (CVE-2013-5615)

- A use-after-free vulnerability exists when interacting with event listeners from the mListeners array. This could result in a denial of service or arbitrary code execution. (CVE-2013-5616)

- A use-after-free vulnerability exists in the table editing user interface of the editor during garbage collection. This could result in a denial of service or arbitrary code execution. (CVE-2013-5618)

- Memory issues exist in the binary search algorithms in the SpiderMonkey JavaScript engine that could result in a denial of service or arbitrary code execution.

(CVE-2013-5619)

- Issues exist with the JPEG format image processing with Start Of Scan (SOS) and Define Huffman Table (DHT) markers in the 'libjpeg' library. This could allow attackers to read arbitrary memory content as well as cross-domain image theft. (CVE-2013-6629, CVE-2013-6630)

- A memory issue exists when inserting an ordered list into a document through a script that could result in a denial of service or arbitrary code execution.

(CVE-2013-6671)

- Trust settings for built-in root certificates are ignored during extended validation (EV) certificate validation. This removes the ability of users to explicitly untrust root certificates from specific certificate authorities. (CVE-2013-6673)

- An intermediate certificate that is used by a man-in- the-middle (MITM) traffic management device exists in Mozilla's root certificate authorities. Reportedly, this certificate has been misused.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2013-104/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-105/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-106/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-107/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-108/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-109/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-110/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-111/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-113/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-114/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-115/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-116/
https://www.mozilla.org/en-US/security/advisories/mfsa2013-117/

Solution

Upgrade to Firefox 26.0 or later.

Risk Factor

Critical

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	63676
BID	63679
BID	64203
BID	64204
BID	64205
BID	64206
BID	64207
BID	64209
BID	64211
BID	64212

BID	64213
BID	64214
BID	64215
BID	64216
CVE	CVE-2013-5609
CVE	CVE-2013-5610
CVE	CVE-2013-5611
CVE	CVE-2013-5612
CVE	CVE-2013-5613
CVE	CVE-2013-5614
CVE	CVE-2013-5615
CVE	CVE-2013-5616
CVE	CVE-2013-5618
CVE	CVE-2013-5619
CVE	CVE-2013-6629
CVE	CVE-2013-6630
CVE	CVE-2013-6671
CVE	CVE-2013-6673
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: 2013/12/11, Modified: 2019/11/27

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 26.0
```

72331 - Firefox < 27.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 27.0 and is, therefore, potentially affected by the following vulnerabilities :

- Memory issues exist in the browser engine that could result in a denial of service or arbitrary code execution. (CVE-2014-1477, CVE-2014-1478)

- An error exists related to System Only Wrappers (SOW) and the XML Binding Language (XBL) that could allow XUL content to be disclosed. (CVE-2014-1479)

- An error exists related to the 'open file' dialog that could allow users to take unintended actions.

(CVE-2014-1480)

- An error exists related to the JavaScript engine and 'window' object handling that has unspecified impact.

(CVE-2014-1481)

- An error exists related to 'RasterImage' and image decoding that could allow application crashes and possibly arbitrary code execution. (CVE-2014-1482)

- Errors exist related to IFrames, 'document.caretPositionFromPoint' and 'document.elementFromPoint' that could allow cross- origin information disclosure. (CVE-2014-1483)

- An error exists related to the Content Security Policy (CSP) and XSLT stylesheets that could allow unintended script execution. (CVE-2014-1485)

- A use-after-free error exists related to image handling and 'imgRequestProxy' that could allow application crashes and possibly arbitrary code execution.

(CVE-2014-1486)

- An error exists related to 'web workers' that could allow cross-origin information disclosure.

(CVE-2014-1487)

- An error exists related to 'web workers' and 'asm.js'

that could allow application crashes and possibly arbitrary code execution. (CVE-2014-1488)

- An error exists that could allow webpages to access activate content from the 'about:home' page that could lead to data loss. (CVE-2014-1489)

- Network Security Services (NSS) contains a race condition in libssl that occurs during session ticket processing. A remote attacker can exploit this flaw to cause a denial of service. (CVE-2014-1490)

- Network Security Services (NSS) does not properly restrict public values in Diffie-Hellman key exchanges, allowing a remote attacker to bypass cryptographic protection mechanisms. (CVE-2014-1491)

See Also

http://www.zerodayinitiative.com/advisories/ZDI-14-058/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-02/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-03/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-04/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-05/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-07/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-08/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-09/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-10/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-11/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-12/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-13/

Solution

Upgrade to Firefox 27.0 or later.

Risk Factor

Critical

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	65316
BID	65317
BID	65320
BID	65321
BID	65322
BID	65324
BID	65326
BID	65328
BID	65329
BID	65330
BID	65331
BID	65332

BID	65334
BID	65335
CVE	CVE-2014-1477
CVE	CVE-2014-1478
CVE	CVE-2014-1479
CVE	CVE-2014-1480
CVE	CVE-2014-1481
CVE	CVE-2014-1482
CVE	CVE-2014-1483
CVE	CVE-2014-1485
CVE	CVE-2014-1486
CVE	CVE-2014-1487
CVE	CVE-2014-1488
CVE	CVE-2014-1489
CVE	CVE-2014-1490
CVE	CVE-2014-1491

Plugin Information

Published: 2014/02/05, Modified: 2019/11/26

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 27.0
```

73769 - Firefox < 29.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is a version prior to 29.0 and is, therefore, potentially affected by the following vulnerabilities :

- An issue exists in the Network Security (NSS) library due to improper handling of IDNA domain prefixes for wildcard certificates. This issue could allow man-in- the-middle attacks. (CVE-2014-1492)

- Memory issues exist that could lead to arbitrary code execution. (CVE-2014-1518, CVE-2014-1519)

- An issue exists related to the 'Mozilla Maintenance Service' that could lead to privilege escalation due to the creation of a writeable temporary directory during the update process. (CVE-2014-1520)

- An out-of-bounds read issue exists in the Web Audio feature that could lead to information disclosure.

(CVE-2014-1522)

- An out-of-bounds read issue exists when decoding certain JPG images that could lead to a denial of service. (CVE-2014-1523)

- A memory corruption issue exists due to improper validation of XBL objects that could lead to arbitrary code execution. (CVE-2014-1524)

- A use-after-free memory issue exists in the Text Track Manager during HTML video processing that could lead to arbitrary code execution. (CVE-2014-1525)

- An issue exists related to the debugger bypassing XrayWrappers that could lead to privilege escalation.

(CVE-2014-1526)

- An out-of-bounds write issue exists in the Cairo graphics library that could lead to arbitrary code execution.Note that this issue only affects Firefox 28 and SeaMonkey 2.25. (CVE-2014-1528)

- A security bypass issue exists in the Web Notification API that could lead to arbitrary code execution.

(CVE-2014-1529)

- A cross-site scripting issue exists that could allow an attacker to load another website other than the URL for the website that is shown in the address bar.

(CVE-2014-1530)

- A use-after-free issue exists due to an 'imgLoader'

object being freed when being resized. This issue could lead to arbitrary code execution. (CVE-2014-1531)

- A use-after-free issue exists during host resolution that could lead to arbitrary code execution.

(CVE-2014-1532)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2014-34/

https://www.mozilla.org/en-US/security/advisories/mfsa2014-35/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-36/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-37/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-38/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-39/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-41/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-42/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-43/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-44/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-45/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-46/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-47/

Solution

Upgrade to Firefox 29.0 or later.

Risk Factor

Critical

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	66356
BID	67123
BID	67125
BID	67126
BID	67127
BID	67129
BID	67130
BID	67131
BID	67132
BID	67133
BID	67134
BID	67135
BID	67136

BID	67137
CVE	CVE-2014-1492
CVE	CVE-2014-1518
CVE	CVE-2014-1519
CVE	CVE-2014-1520
CVE	CVE-2014-1522
CVE	CVE-2014-1523
CVE	CVE-2014-1524
CVE	CVE-2014-1525
CVE	CVE-2014-1526
CVE	CVE-2014-1528
CVE	CVE-2014-1529
CVE	CVE-2014-1530
CVE	CVE-2014-1531
CVE	CVE-2014-1532
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: 2014/04/29, Modified: 2019/11/26

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 29.0
```

74440 - Firefox < 30.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote host is a version prior to 30.0 and is, therefore, affected by the following vulnerabilities :

- Memory issues exist that could lead to arbitrary code execution. Note that these issues only affect Firefox 29. (CVE-2014-1533, CVE-2014-1534)

- An out-of-bounds read issue exists in 'PropertyProvider::FindJustificationRange'.

(CVE-2014-1536)

- Use-after-free memory issues exist in 'mozilla::dom::workers::WorkerPrivateParent', 'nsTextEditRules::CreateMozBR', and the SMIL Animation Controller that could lead to code execution.

(CVE-2014-1537, CVE-2014-1538, CVE-2014-1541)

- A use-after-free memory issue exists in the event listener manager. Note that this issue only affects Firefox 29. (CVE-2014-1540)

- A buffer overflow issue exists in the Speex resampler for Web Audio that could lead to code execution.

(CVE-2014-1542)

- A buffer overflow issue exists in the Gamepad API that could lead to code execution. Note that this issue only affects Firefox 29 on Windows 8 when a physical or virtual gamepad is attached. (CVE-2014-1543)

See Also

https://www.mozilla.org/security/announce/2014/mfsa2014-48.html

https://www.mozilla.org/security/announce/2014/mfsa2014-49.html

https://www.mozilla.org/security/announce/2014/mfsa2014-51.html

https://www.mozilla.org/security/announce/2014/mfsa2014-52.html

https://www.mozilla.org/security/announce/2014/mfsa2014-53.html

https://www.mozilla.org/security/announce/2014/mfsa2014-54.html

Solution

Upgrade to Firefox 30.0 or later.

Risk Factor

Critical

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	67964
BID	67965
BID	67966
BID	67968
BID	67969
BID	67971
BID	67976
BID	67978
BID	67979
CVE	CVE-2014-1533
CVE	CVE-2014-1534
CVE	CVE-2014-1536
CVE	CVE-2014-1537
CVE	CVE-2014-1538
CVE	CVE-2014-1540
CVE	CVE-2014-1541
CVE	CVE-2014-1542
CVE	CVE-2014-1543

Plugin Information

Published: 2014/06/11, Modified: 2019/11/26

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 30.0
```

76763 - Firefox < 31.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote host is a version prior to 31.0. It is, therefore, affected by the following vulnerabilities :

- When a pair of NSSCertificate structures are added to a trust domain and then one of them is removed during use, a use-after-free error occurs which may cause the application to crash. This crash is potentially exploitable. (CVE-2014-1544)

- There are multiple memory safety hazards within the browser engine. These hazards may lead to memory corruption vulnerabilities, which may allow attackers to execute arbitrary code. (CVE-2014-1547, CVE-2014-1548)

- A buffer overflow exists when interacting with the Web Audio buffer during playback due to an error with the allocation of memory for the buffer. This may lead to a potentially exploitable crash. (CVE-2014-1549)

- A use-after-free exists in Web Audio due to the way control messages are handled. This may lead to a potentially exploitable crash. (CVE-2014-1550)

- There is a potential use-after-free issue in DirectWrite font handling. This may allow an attacker to potentially execute arbitrary code within the context of the user running the application. (CVE-2014-1551)

- There is an issue with the IFRAME sandbox same-origin access policy which allows sandboxed content to access other content from the same origin without approval.

This may lead to a same-origin-bypass vulnerability.

(CVE-2014-1552)

- Triggering the FireOnStateChange event has the potential to crash the application. This may lead to a use-after-free and an exploitable crash.

(CVE-2014-1555)

- When using the Cesium JavaScript library to generate WebGL content, the application may crash. This crash is potentially exploitable. (CVE-2014-1556)

- There is a flaw in the Skia library when scaling images of high quality. If the image data is discarded while being processed, the library may crash. This crash is potentially exploitable. (CVE-2014-1557)

- There are multiple issues with using invalid characters in various certificates. These invalid characters may cause certificates to be parsed incorrectly which may lead to the inability to use valid SSL certificates. (CVE-2014-1558, CVE-2014-1559, CVE-2014-1560)

- It may be possible to spoof drag and drop events in web content. This may allow limited ability to interact with the UI. (CVE-2014-1561)

See Also

https://www.mozilla.org/security/announce/2014/mfsa2014-56.html

https://www.mozilla.org/security/announce/2014/mfsa2014-57.html
https://www.mozilla.org/security/announce/2014/mfsa2014-58.html
https://www.mozilla.org/security/announce/2014/mfsa2014-59.html
https://www.mozilla.org/security/announce/2014/mfsa2014-60.html
https://www.mozilla.org/security/announce/2014/mfsa2014-61.html
https://www.mozilla.org/security/announce/2014/mfsa2014-62.html
https://www.mozilla.org/security/announce/2014/mfsa2014-63.html
https://www.mozilla.org/security/announce/2014/mfsa2014-64.html
https://www.mozilla.org/security/announce/2014/mfsa2014-65.html
https://www.mozilla.org/security/announce/2014/mfsa2014-66.html

Solution

Upgrade to Firefox 31.0 or later.

Risk Factor

Critical

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	68810
BID	68811
BID	68812
BID	68813
BID	68814
BID	68815
BID	68816
BID	68817
BID	68818
BID	68820
BID	68821
BID	68824
BID	68826
CVE	CVE-2014-1544
CVE	CVE-2014-1547

CVE	CVE-2014-1548
CVE	CVE-2014-1549
CVE	CVE-2014-1550
CVE	CVE-2014-1551
CVE	CVE-2014-1552
CVE	CVE-2014-1555
CVE	CVE-2014-1557
CVE	CVE-2014-1558
CVE	CVE-2014-1559
CVE	CVE-2014-1560
CVE	CVE-2014-1561

Plugin Information

Published: 2014/07/24, Modified: 2019/11/26

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 31.0
```

77500 - Firefox < 32.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote host is a version prior to 32.0. It is, therefore, affected by the following vulnerabilities :

- Multiple memory safety flaws exist within the browser engine. Exploiting these, an attacker can cause a denial of service or execute arbitrary code. (CVE-2014-1553, CVE-2014-1554, CVE-2014-1562)

- A use-after-free vulnerability exists due to improper cycle collection when processing animated SVG content.

A remote attacker can exploit this to cause a denial of service or execute arbitrary code. (CVE-2014-1563)

- Memory is not properly initialized during GIF rendering.

Using a specially crafted web script, a remote attacker can exploit this to acquire sensitive information from the process memory. (CVE-2014-1564)

- The Web Audio API contains a flaw where audio timelines are properly created. Using specially crafted API calls, a remote attacker can exploit this to acquire sensitive information from the process memory or cause a denial of service. (CVE-2014-1565)

- A use-after-free vulnerability exists due to improper handling of text layout in directionality resolution.

A remote attacker can exploit this to execute arbitrary code. (CVE-2014-1567)

See Also

http://www.securityfocus.com/archive/1/533357/30/0/threaded

https://www.mozilla.org/security/announce/2014/mfsa2014-67.html

https://www.mozilla.org/security/announce/2014/mfsa2014-68.html

https://www.mozilla.org/security/announce/2014/mfsa2014-69.html

https://www.mozilla.org/security/announce/2014/mfsa2014-70.html

https://www.mozilla.org/en-US/security/advisories/mfsa2014-71/

https://www.mozilla.org/security/announce/2014/mfsa2014-72.html

Solution

Upgrade to Firefox 32.0 or later.

Risk Factor

Critical

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	69519
BID	69520
BID	69521
BID	69523
BID	69524
BID	69525
BID	69526
CVE	CVE-2014-1553
CVE	CVE-2014-1554
CVE	CVE-2014-1562
CVE	CVE-2014-1563
CVE	CVE-2014-1564
CVE	CVE-2014-1565
CVE	CVE-2014-1567

Plugin Information

Published: 2014/09/03, Modified: 2019/11/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 32.0
```

83439 - Firefox < 38.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 38.0. It is, therefore, affected by the following vulnerabilities :

- A privilege escalation vulnerability exists in the Inter-process Communications (IPC) implementation due to a failure to validate the identity of a listener process. (CVE-2011-3079)

- An issue exists in the Mozilla updater in which DLL files in the current working directory or Windows temporary directories will be loaded, allowing the execution of arbitrary code. (CVE-2015-0833 / CVE-2015-2720)

- Multiple memory corruption issues exist within the browser engine. A remote attacker can exploit these to corrupt memory and execute arbitrary code.

(CVE-2015-2708, CVE-2015-2709)

- A buffer overflow condition exists in SVGTextFrame.cpp when rendering SVG graphics that are combined with certain CSS properties due to improper validation of user-supplied input. A remote attacker can exploit this to cause a heap-based buffer overflow, resulting in the execution of arbitrary code. (CVE-2015-2710)

- A security bypass vulnerability exists due to the referrer policy not being enforced in certain situations when opening links (e.g. using the context menu or a middle-clicks by mouse). A remote attacker can exploit this to bypass intended policy settings. (CVE-2015-2711)

- An out-of-bounds read and write issue exists in the CheckHeapLengthCondition() function due to improper JavaScript validation of heap lengths. A remote attacker can exploit this, via a specially crafted web page, to disclose memory contents. (CVE-2015-2712)

- A use-after-free error exists due to improper processing of text when vertical text is enabled. A remote attacker can exploit this to dereference already freed memory.

(CVE-2015-2713)

- A use-after-free error exists in the RegisterCurrentThread() function in nsThreadManager.cpp due to a race condition related to media decoder threads created during the shutdown process. A remote attacker can exploit this to dereference already freed memory.

(CVE-2015-2715)

- A buffer overflow condition exists in the XML_GetBuffer() function in xmlparse.c due to improper validation of user-supplied input when handling compressed XML content. An attacker can exploit this to cause a buffer overflow, resulting in the execution of arbitrary code. (CVE-2015-2716)

- An integer overflow condition exists in the parseChunk() function in MPEG4Extractor.cpp due to improper handling of MP4 video metadata in chunks. A remote attacker can exploit this, via specially crafted media content, to cause a heap-based buffer overflow, resulting in the execution of arbitrary code. (CVE-2015-2717)

- A security bypass vulnerability exists in WebChannel.jsm due to improper handling of message traffic. An untrusted page hosting a trusted page within an iframe can intercept webchannel responses for the trusted page.

This allows a remote attacker, via a specially crafted web page, to bypass origin restrictions, resulting in the disclosure of sensitive information. (CVE-2015-2718)

- Multiple integer overflow conditions exist in the bundled libstagefright component due to improper validation of user-supplied input when processing MPEG4 sample metadata. A remote attacker can exploit this, via specially crafted media content, to execute arbitrary code. (CVE-2015-4496)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-46/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-48/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-49/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-50/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-51/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-53/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-54/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-55/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-56/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-57/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-58/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-93/

Solution

Upgrade to Firefox 38.0 or later.

Risk Factor

Critical

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	53309
BID	72747
BID	74611
BID	74615
BID	76333
CVE	CVE-2011-3079

CVE	CVE-2015-0833
CVE	CVE-2015-2708
CVE	CVE-2015-2709
CVE	CVE-2015-2710
CVE	CVE-2015-2711
CVE	CVE-2015-2712
CVE	CVE-2015-2713
CVE	CVE-2015-2715
CVE	CVE-2015-2716
CVE	CVE-2015-2717
CVE	CVE-2015-2718
CVE	CVE-2015-2720
CVE	CVE-2015-4496

Plugin Information

Published: 2015/05/13, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 38.0
```

84581 - Firefox < 39.0 Multiple Vulnerabilities (Logjam)

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 39.0. It is, therefore, affected by multiple vulnerabilities :

- A security downgrade vulnerability exists due to a flaw in Network Security Services (NSS). When a client allows for a ECDHE_ECDSA exchange, but the server does not send a ServerKeyExchange message, the NSS client will take the EC key from the ECDSA certificate. A remote attacker can exploit this to silently downgrade the exchange to a non-forward secret mixed-ECDH exchange. (CVE-2015-2721)

- Multiple user-after-free errors exist when using an XMLHttpRequest object in concert with either shared or dedicated workers. A remote attacker can exploit this to cause a denial of service condition. (CVE-2015-2722, CVE-2015-2733)

- Multiple memory corruption issues exist that allow an attacker to cause a denial of service condition or potentially execute arbitrary code. (CVE-2015-2724, CVE-2015-2725)

- A security bypass vulnerability exists due to a failure to preserve context restrictions. A remote attacker can exploit this, via a crafted web site that is accessed with unspecified mouse and keyboard actions, to read arbitrary files or execute arbitrary JavaScript code.

(CVE-2015-2727)

- A type confusion flaw exists in the Indexed Database Manager's handling of IDBDatabase. A remote attacker can exploit this to cause a denial of service condition or to execute arbitrary code. (CVE-2015-2728)

- An out-of-bounds read flaw exists in the AudioParamTimeline::AudioNodeInputValue() function when computing oscillator rending ranges. An attacker can exploit this to disclose the contents of four bytes of memory or cause a denial of service condition.

(CVE-2015-2729)

- A signature spoofing vulnerability exists due to a flaw in Network Security Services (NSS) in its Elliptic Curve Digital Signature Algorithm (ECDSA) signature validation. A remote attacker can exploit this to forge signatures. (CVE-2015-2730)

- A use-after-free error exists in the CSPService::ShouldLoad() function when modifying the Document Object Model to remove a DOM object. An attacker can exploit this to dereference already freed memory, potentially resulting in the execution of arbitrary code. (CVE-2015-2731)

- An uninitialized memory use issue exists in the CairoTextureClientD3D9::BorrowDrawTarget() function, the ::d3d11::SetBufferData() function, and the YCbCrImageDataDeserializer::ToDataSourceSurface() function. The impact is unspecified. (CVE-2015-2734, CVE-2015-2737, CVE-2015-2738)

- A memory corruption issue exists in the nsZipArchive::GetDataOffset() function due to improper string length checks. An attacker can exploit this, via a crafted ZIP archive, to potentially execute arbitrary code. (CVE-2015-2735)

- A memory corruption issue exists in the nsZipArchive::BuildFileList() function due to improper validation of user-supplied input. An attacker can exploit this, via a crafted ZIP archive, to potentially execute arbitrary code. (CVE-2015-2736)

- An unspecified memory corruption issue exists in the ArrayBufferBuilder::append() function due to improper validation of user-supplied input. An attacker can exploit this to potentially execute arbitrary code.

(CVE-2015-2739)

- A buffer overflow condition exists in the nsXMLHttpRequest::AppendToResponseText() function due to improper validation of user-supplied input. An attacker can exploit this to potentially execute arbitrary code.

(CVE-2015-2740)

- A security bypass vulnerability exists due to a flaw in certificate pinning checks. Key pinning is not enforced upon encountering an X.509 certificate problem that generates a user dialog. A man-in-the-middle attacker can exploit this to bypass intended access restrictions.

(CVE-2015-2741)

- A privilege escalation vulnerability exists in the PDF viewer (PDF.js) due to internal workers being executed insecurely. An attacker can exploit this, by leveraging a Same Origin Policy bypass, to execute arbitrary code.

(CVE-2015-2743)

- A man-in-the-middle vulnerability, known as Logjam, exists due to a flaw in the SSL/TLS protocol. A remote attacker can exploit this flaw to downgrade connections using ephemeral Diffie-Hellman key exchange to 512-bit export-grade cryptography. (CVE-2015-4000)

See Also

https://www.mozilla.org//en-US/security/advisories/mfsa2015-59/

https://www.mozilla.org//en-US/security/advisories/mfsa2015-60/

https://www.mozilla.org//en-US/security/advisories/mfsa2015-61/

https://www.mozilla.org//en-US/security/advisories/mfsa2015-62/

https://www.mozilla.org//en-US/security/advisories/mfsa2015-63/

https://www.mozilla.org//en-US/security/advisories/mfsa2015-64/

https://www.mozilla.org//en-US/security/advisories/mfsa2015-65/

https://www.mozilla.org//en-US/security/advisories/mfsa2015-66/

https://www.mozilla.org//en-US/security/advisories/mfsa2015-67/

https://www.mozilla.org//en-US/security/advisories/mfsa2015-69/

https://www.mozilla.org//en-US/security/advisories/mfsa2015-70/

https://www.mozilla.org//en-US/security/advisories/mfsa2015-71/

https://weakdh.org/

Solution

Upgrade to Firefox 39.0 or later.

Risk Factor

Critical

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	74733
CVE	CVE-2015-2721
CVE	CVE-2015-2722
CVE	CVE-2015-2724
CVE	CVE-2015-2727
CVE	CVE-2015-2728
CVE	CVE-2015-2729
CVE	CVE-2015-2730
CVE	CVE-2015-2731
CVE	CVE-2015-2733
CVE	CVE-2015-2734
CVE	CVE-2015-2735
CVE	CVE-2015-2736
CVE	CVE-2015-2737
CVE	CVE-2015-2738
CVE	CVE-2015-2739
CVE	CVE-2015-2740
CVE	CVE-2015-2741
CVE	CVE-2015-2743
CVE	CVE-2015-4000

Plugin Information

Published: 2015/07/07, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 39.0
```

85386 - Firefox < 40 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 40. 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)

- 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-2015-4474)

- 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 use-after-free error exists in the Web Audio API during MediaStream playback. A remote attacker can exploit this to dereference already freed memory, resulting in the potential execution of arbitrary code.

(CVE-2015-4477)

- 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 security bypass vulnerability exists due to a flaw in the ShouldLoad() function that occurs during the handling of POST requests to URLs using the 'feed:' URI handler. An attacker can exploit this to bypass the mixed content blocker. (CVE-2015-4483)

- 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 security bypass vulnerability exists due to a discrepancy in the implementation of Content Security Policy and the CSP specification. The specification states that 'blob:', 'data:', and 'filesystem:' URLs should be excluded in case of a wildcard when matching source expressions, but Mozilla's implementation allows these in the case of an asterisk wildcard. A remote attacker can exploit this to bypass restrictions.

(CVE-2015-4490)

- 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/mfsa2015-81/

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/mfsa2015-86/

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/mfsa2015-91/

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

Solution

Upgrade to Firefox 40 or later.

Risk Factor

Critical

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-2015-4474
CVE	CVE-2015-4475
CVE	CVE-2015-4477
CVE	CVE-2015-4478
CVE	CVE-2015-4479
CVE	CVE-2015-4480
CVE	CVE-2015-4481
CVE	CVE-2015-4482
CVE	CVE-2015-4483
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-2015-4490
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 : 3.6.12
Fixed version     : 40
```

85689 - Firefox < 40.0.3 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 40.0.3. 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 40.0.3 or later.

Risk Factor

Critical

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 : 3.6.12
Fixed version     : 40.0.3
```

87476 - Firefox < 43 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 43. 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)

- 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-2015-7202)

- An overflow condition exists in the LoadFontFamilyData() function due to improper validation of user-supplied input. A remote attacker can exploit this to cause a buffer overflow, resulting in the execution of arbitrary code. (CVE-2015-7203)

- A flaw exists in the PropertyWriteNeedsTypeBarrier() function due to improper handling of unboxed objects during JavaScript variable assignments. A remote attacker can exploit this to execute arbitrary code.

(CVE-2015-7204)

- 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 same-origin bypass vulnerability exists that is triggered after a redirect when the function is used alongside an iframe to host a page. An attacker can exploit this to gain access to cross-origin URL information. (CVE-2015-7207)

- The SetCookieInternal() function improperly allows control characters (e.g. ASCII code 11) to be inserted into cookies. An attacker can exploit this to inject cookies. (CVE-2015-7208)

- 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)

- A flaw exists in the ParseURI() function due to improper handling of a hash (#) character in the data: URI. An attacker can exploit this to spoof the URL bar.

(CVE-2015-7211)

- 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 information disclosure vulnerability exists due to improper handling of error events in web workers. An attacker can exploit this to gain access to sensitive cross-origin information. (CVE-2015-7215)

- Multiple integer underflow conditions exist due to improper validation of user-supplied input when handling HTTP2 frames. An attacker can exploit these to crash the application, resulting in a denial of service.

(CVE-2015-7218, CVE-2015-7219)

- An overflow condition exists in the XDRBuffer::grow() function due to improper validation of user-supplied input. An attacker can exploit this to cause a buffer overflow, resulting in the execution of arbitrary code.

(CVE-2015-7220)

- An overflow condition exists in the GrowCapacity() function due to improper validation of user-supplied input. An attacker can exploit this to cause a buffer overflow, resulting in the execution of arbitrary code.

(CVE-2015-7221)

- 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)

- A privilege escalation vulnerability exists in the Extension.jsm script due to a failure to restrict WebExtension APIs from being injected into documents without WebExtension principals. An attacker can exploit this to conduct a cross-site scripting attack, resulting in the execution of arbitrary script code in a user's browser session. (CVE-2015-7223)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-134/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-135/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-136/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-137/

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/mfsa2015-140/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-141/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-142/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-144/

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/mfsa2015-148/

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

Solution

Upgrade to Firefox 43 or later.

Risk Factor

Critical

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	79280
BID	79283
CVE	CVE-2015-7201
CVE	CVE-2015-7202
CVE	CVE-2015-7203
CVE	CVE-2015-7204
CVE	CVE-2015-7205
CVE	CVE-2015-7207
CVE	CVE-2015-7208
CVE	CVE-2015-7210
CVE	CVE-2015-7211
CVE	CVE-2015-7212
CVE	CVE-2015-7213
CVE	CVE-2015-7214
CVE	CVE-2015-7215
CVE	CVE-2015-7218
CVE	CVE-2015-7219
CVE	CVE-2015-7220
CVE	CVE-2015-7221
CVE	CVE-2015-7222
CVE	CVE-2015-7223

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 43
```

88461 - Firefox < 44 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 44. It is, therefore, affected by the following vulnerabilities :

- A cookie injection vulnerability exists due to illegal control characters being stored as cookie values in violation of RFC6265. A remote attacker can exploit this to inject cookies. (CVE-2015-7208)

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

(CVE-2016-1930, CVE-2016-1931)

- An integer overflow condition exists due to improper parsing of GIF images during deinterlacing. A remote attacker can exploit this, via a specially crafted GIF image, to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-1933)

- 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)

- A content spoofing vulnerability exists due to the protocol handler dialog treating double click events as two single click events. A remote attacker can exploit this to spoof content, allowing the attacker to trick a user into performing malicious actions. (CVE-2016-1937)

- A cryptographic weakness exists in Network Security Services (NSS) due to incorrect calculations with 'mp_div' and 'mp_exptmod'. (CVE-2016-1938)

- A cookie injection vulnerability exists due to illegal control characters being permitted in cookie names. A remote attacker can exploit this to inject cookies.

(CVE-2016-1939)

- An URL spoofing vulnerability exists due to a flaw that is triggered during the handling of a URL that invalid for the internal protocol, causing the URL to be pasted into the address bar. A remote attacker can exploit this spoof URLs, allowing the attacker to trick a user into visiting a malicious website. (CVE-2016-1942)

- An unspecified memory corruption issue exists in the ANGLE graphics library implementation. A remote attacker can exploit this to corrupt memory, resulting in the execution of arbitrary code. (CVE-2016-1944)

- A wild pointer flaw exists due to improper handling of ZIP files. A remote attacker can exploit this, via a crafted ZIP file, to have an unspecified impact.

(CVE-2016-1945)

- An integer overflow condition exists in the bundled version of libstagefright due to improper handling of MP4 file metadata. A remote attacker can exploit this to execute arbitrary code. (CVE-2016-1946)

- A flaw exists in the safe browsing feature due to the Application Reputation service being unreachable. A remote attacker can exploit this to convince a user into downloading a malicious executable without being warned. (CVE-2016-1947)

- A use-after-free error exists in Network Security Services (NSS) due to improper handling of failed allocations during DHE and ECDHE handshakes. An attacker can exploit this to dereference already freed memory, resulting in the execution of arbitrary code.

(CVE-2016-1978)

See Also

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

https://www.mozilla.org/en-US/security/advisories/mfsa2016-02/

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

https://www.mozilla.org/en-US/security/advisories/mfsa2016-04/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-06/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-07/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-08/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-09/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-10/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-11/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-15/

Solution

Upgrade to Firefox version 44 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)

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	79280

CVE	CVE-2015-7208
CVE	CVE-2016-1930
CVE	CVE-2016-1931
CVE	CVE-2016-1933
CVE	CVE-2016-1935
CVE	CVE-2016-1937
CVE	CVE-2016-1938
CVE	CVE-2016-1939
CVE	CVE-2016-1942
CVE	CVE-2016-1944
CVE	CVE-2016-1945
CVE	CVE-2016-1946
CVE	CVE-2016-1947
CVE	CVE-2016-1978
XREF	MFSA:2016-01
XREF	MFSA:2016-02
XREF	MFSA:2016-03
XREF	MFSA:2016-04
XREF	MFSA:2016-06
XREF	MFSA:2016-07
XREF	MFSA:2016-08
XREF	MFSA:2016-09
XREF	MFSA:2016-10
XREF	MFSA:2016-11
XREF	MFSA:2016-15

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 44
```

89875 - Firefox < 45 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 45. 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/mfsa2016-18/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-19/
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/mfsa2016-22/
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/mfsa2016-26/
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/mfsa2016-29/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-30/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-31/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-32/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-33/
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/mfsa2016-36/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-37/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-38/

Solution

Upgrade to Firefox version 45 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)

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-2016-1953
CVE	CVE-2016-1954
CVE	CVE-2016-1955
CVE	CVE-2016-1956
CVE	CVE-2016-1957
CVE	CVE-2016-1958
CVE	CVE-2016-1959
CVE	CVE-2016-1960
CVE	CVE-2016-1961
CVE	CVE-2016-1962
CVE	CVE-2016-1963
CVE	CVE-2016-1964
CVE	CVE-2016-1965
CVE	CVE-2016-1966
CVE	CVE-2016-1967
CVE	CVE-2016-1968
CVE	CVE-2016-1969
CVE	CVE-2016-1970
CVE	CVE-2016-1971
CVE	CVE-2016-1972
CVE	CVE-2016-1973
CVE	CVE-2016-1974

CVE	CVE-2016-1975
CVE	CVE-2016-1976
CVE	CVE-2016-1977
CVE	CVE-2016-1979
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:2016-18
XREF	MFSA:2016-19
XREF	MFSA:2016-20
XREF	MFSA:2016-21
XREF	MFSA:2016-22
XREF	MFSA:2016-23
XREF	MFSA:2016-24
XREF	MFSA:2016-25
XREF	MFSA:2016-26
XREF	MFSA:2016-27
XREF	MFSA:2016-28
XREF	MFSA:2016-29
XREF	MFSA:2016-30
XREF	MFSA:2016-31
XREF	MFSA:2016-32
XREF	MFSA:2016-33
XREF	MFSA:2016-34
XREF	MFSA:2016-35
XREF	MFSA:2016-36
XREF	MFSA:2016-37
XREF	MFSA:2016-38

Plugin Information

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

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
  Fixed version     : 45
```

160465 - Mozilla Firefox < 100.0

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 100.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-16 advisory.

- When reusing existing popups Firefox would have allowed them to cover the fullscreen notification UI, which could have enabled browser spoofing attacks. (CVE-2022-29914)

- Documents in deeply-nested cross-origin browsing contexts could have obtained permissions granted to the top-level origin, bypassing the existing prompt and wrongfully inheriting the top-level permissions.

(CVE-2022-29909)

- Firefox behaved slightly differently for already known resources when loading CSS resources involving CSS variables. This could have been used to probe the browser history. (CVE-2022-29916)

- Firefox did not properly protect against top-level navigations for an iframe sandbox with a policy relaxed through a keyword like <code>allow-top-navigation-by-user-activation</code>. (CVE-2022-29911)

- Requests initiated through reader mode did not properly omit cookies with a SameSite attribute.

(CVE-2022-29912)

- When closed or sent to the background, Firefox for Android would not properly record and persist HSTS settings. Note: This issue only affected Firefox for Android. Other operating systems are unaffected.

(CVE-2022-29910)

- The Performance API did not properly hide the fact whether a request cross-origin resource has observed redirects. (CVE-2022-29915)

- Mozilla developers Andrew McCreight, Gabriele Svelto, Tom Ritter and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 99 and Firefox ESR 91.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-29917)

- Mozilla developers Gabriele Svelto, Randell Jesup and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 99. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-29918)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2022-16/

Solution

Upgrade to Mozilla Firefox version 100.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2022-29909
CVE	CVE-2022-29910
CVE	CVE-2022-29911
CVE	CVE-2022-29912
CVE	CVE-2022-29914
CVE	CVE-2022-29915
CVE	CVE-2022-29916
CVE	CVE-2022-29917
CVE	CVE-2022-29918
XREF	IAVA:2022-A-0188

Plugin Information

Published: 2022/05/03, Modified: 2022/05/06

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
```

```
  Fixed version     : 100.0
```

161415 - Mozilla Firefox < 100.0.2

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 100.0.2. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-19 advisory.

- If an attacker was able to corrupt the methods of an Array object in JavaScript via prototype pollution, they could have achieved execution of attacker-controlled JavaScript code in a privileged context.

(CVE-2022-1802)

- An attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process. (CVE-2022-1529)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/

Solution

Upgrade to Mozilla Firefox version 100.0.2 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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-1529
CVE	CVE-2022-1802
XREF	IAVA:2022-A-0217-S

Plugin Information

Published: 2022/05/20, Modified: 2022/06/07

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 100.0.2
```

161716 - Mozilla Firefox < 101.0

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 101.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-20 advisory.

- A malicious website could have learned the size of a cross-origin resource that supported Range requests.

(CVE-2022-31736)

- A malicious webpage could have caused an out-of-bounds write in WebGL, leading to memory corruption and a potentially exploitable crash. (CVE-2022-31737)

- When exiting fullscreen mode, an iframe could have confused the browser about the current state of fullscreen, resulting in potential user confusion or spoofing attacks. (CVE-2022-31738)

- When downloading files on Windows, the % character was not escaped, which could have lead to a download incorrectly being saved to attacker-influenced paths that used variables such as %HOMEPATH% or %APPDATA%.

This bug only affects Firefox for Windows. Other operating systems are unaffected. (CVE-2022-31739)

- On arm64, WASM code could have resulted in incorrect assembly generation leading to a register allocation problem, and a potentially exploitable crash. (CVE-2022-31740)

- A crafted CMS message could have been processed incorrectly, leading to an invalid memory read, and potentially further memory corruption. (CVE-2022-31741)

- An attacker could have exploited a timing attack by sending a large number of allowCredential entries and detecting the difference between invalid key handles and cross-origin key handles. This could have led to cross-origin account linking in violation of WebAuthn goals. (CVE-2022-31742)

- Firefox's HTML parser did not correctly interpret HTML comment tags, resulting in an incongruity with other browsers. This could have been used to escape HTML comments on pages that put user-controlled data in them. (CVE-2022-31743)

- An attacker could have injected CSS into stylesheets accessible via internal URIs, such as resource:, and in doing so bypass a page's Content Security Policy. (CVE-2022-31744)

- If array shift operations are not used, the Garbage Collector may have become confused about valid objects. (CVE-2022-31745)

- An attacker could have caused an uninitialized variable on the stack to be mistakenly freed, causing a potentially exploitable crash. (CVE-2022-1919)

- Mozilla developers Andrew McCreight, Nicolas B. Pierron, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 100 and Firefox ESR 91.9. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-31747)

- Mozilla developers Gabriele Svelto, Timothy Nikkel, Randell Jesup, Jon Coppeard, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 100. Some of these bugs showed evidence of

memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-31748)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/

Solution

Upgrade to Mozilla Firefox version 101.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2022-1919
CVE	CVE-2022-31736
CVE	CVE-2022-31737
CVE	CVE-2022-31738
CVE	CVE-2022-31739
CVE	CVE-2022-31740
CVE	CVE-2022-31741
CVE	CVE-2022-31742

CVE	CVE-2022-31743
CVE	CVE-2022-31744
CVE	CVE-2022-31745
CVE	CVE-2022-31747
CVE	CVE-2022-31748
XREF	IAVA:2022-A-0256
XREF	IAVA:2022-A-0226-S

Plugin Information

Published: 2022/05/31, Modified: 2022/07/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 101.0
```

162602 - Mozilla Firefox < 102.0

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 102.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-24 advisory.

- A malicious website that could create a popup could have resized the popup to overlay the address bar with its own content, resulting in potential user confusion or spoofing attacks. This bug only affects Firefox for Linux. Other operating systems are unaffected. (CVE-2022-34479)

- Navigations between XML documents may have led to a use-after-free and potentially exploitable crash.

(CVE-2022-34470)

- An iframe that was not permitted to run scripts could do so if the user clicked on a <code>javascript:</code> link. (CVE-2022-34468)

- An attacker who could have convinced a user to drag and drop an image to a filesystem could have manipulated the resulting filename to contain an executable extension, and by extension potentially tricked the user into executing malicious code. While very similar, this is a separate issue from CVE-2022-34483. (CVE-2022-34482)

- An attacker who could have convinced a user to drag and drop an image to a filesystem could have manipulated the resulting filename to contain an executable extension, and by extension potentially tricked the user into executing malicious code. While very similar, this is a separate issue from CVE-2022-34482. (CVE-2022-34483)

- ASN.1 parsing of an indefinite SEQUENCE inside an indefinite GROUP could have resulted in the parser accepting malformed ASN.1. (CVE-2022-34476)

- In the <code>nsTArrayImpl::ReplaceElementsAt()</code> function, an integer overflow could have occurred when the number of elements to replace was too large for the container. (CVE-2022-34481)

- Even when an iframe was sandboxed with <code>allow-top-navigation-by-user-activation</code>, if it received a redirect header to an external protocol the browser would process the redirect and prompt the user as appropriate. (CVE-2022-34474)

- When a TLS Certificate error occurs on a domain protected by the HSTS header, the browser should not allow the user to bypass the certificate error. On Firefox for Android, the user was presented with the option to bypass the error; this could only have been done by the user explicitly. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2022-34469)

- When downloading an update for an addon, the downloaded addon update's version was not verified to match the version selected from the manifest. If the manifest had been tampered with on the server, an attacker could trick the browser into downgrading the addon to a prior version. (CVE-2022-34471)

- If there was a PAC URL set and the server that hosts the PAC was not reachable, OCSP requests would have been blocked, resulting in incorrect error pages being shown. (CVE-2022-34472)

- The <code>ms-msdt</code>, <code>search</code>, and <code>search-ms</code> protocols deliver content to Microsoft applications, bypassing the browser, when a user accepts a prompt. These applications have had known vulnerabilities, exploited in the wild (although we know of none exploited

through Firefox), so in this release Firefox has blocked these protocols from prompting the user to open them. This bug only affects Firefox on Windows. Other operating systems are unaffected. (CVE-2022-34478)

- If an object prototype was corrupted by an attacker, they would have been able to set undesired attributes on a JavaScript object, leading to privileged code execution. (CVE-2022-2200)

- Within the <code>lginit()</code> function, if several allocations succeed but then one fails, an uninitialized pointer would have been freed despite never being allocated. (CVE-2022-34480)

- The MediaError message property should be consistent to avoid leaking information about cross-origin resources; however for a same-site cross-origin resource, the message could have leaked information enabling XS-Leaks attacks. (CVE-2022-34477)

- SVG <code><use></code> tags that referenced a same-origin document could have resulted in script execution if attacker input was sanitized via the HTML Sanitizer API. This would have required the attacker to reference a same-origin JavaScript file containing the script to be executed. (CVE-2022-34475)

- The HTML Sanitizer should have sanitized the <code>href</code> attribute of SVG <code><use></code> tags; however it incorrectly did not sanitize <code>xlink:href</code> attributes. (CVE-2022-34473)

- The Mozilla Fuzzing Team reported potential vulnerabilities present in Firefox 101 and Firefox ESR 91.10. Some of these bugs showed evidence of JavaScript prototype or memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-34484)

- Mozilla developers Bryce Seager van Dyk and the Mozilla Fuzzing Team reported potential vulnerabilities present in Firefox 101. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-34485)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2022-24/

Solution

Upgrade to Mozilla Firefox version 102.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2022-2200
CVE	CVE-2022-34468
CVE	CVE-2022-34469
CVE	CVE-2022-34470
CVE	CVE-2022-34471
CVE	CVE-2022-34472
CVE	CVE-2022-34473
CVE	CVE-2022-34474
CVE	CVE-2022-34475
CVE	CVE-2022-34476
CVE	CVE-2022-34477
CVE	CVE-2022-34478
CVE	CVE-2022-34479
CVE	CVE-2022-34480
CVE	CVE-2022-34481
CVE	CVE-2022-34482
CVE	CVE-2022-34483
CVE	CVE-2022-34484
CVE	CVE-2022-34485
XREF	IAVA:2022-A-0256

Plugin Information

Published: 2022/06/29, Modified: 2022/07/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 102.0
```

163497 - Mozilla Firefox < 103.0

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 103.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-28 advisory.

- When combining CSS properties for overflow and transform, the mouse cursor could interact with different coordinates than displayed. (CVE-2022-36319)

- When visiting a website with an overly long URL, the user interface would start to hang. Due to session restore, this could lead to a permanent Denial of Service. This bug only affects Firefox for Android.

Other operating systems are unaffected. (CVE-2022-36317)

- When visiting directory listings for `chrome://` URLs as source text, some parameters were reflected.

(CVE-2022-36318)

- When opening a Windows shortcut from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This bug only affects Firefox for Windows. Other operating systems are unaffected. (CVE-2022-36314)

- When loading a script with Subresource Integrity, attackers with an injection capability could trigger the reuse of previously cached entries with incorrect, different integrity metadata. (CVE-2022-36315)

- When using the Performance API, an attacker was able to notice subtle differences between PerformanceEntries and thus learn whether the target URL had been subject to a redirect. (CVE-2022-36316)

- Mozilla developers and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 102. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-2505, CVE-2022-36320)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2022-28/

Solution

Upgrade to Mozilla Firefox version 103.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2022-2505
CVE	CVE-2022-36314
CVE	CVE-2022-36315
CVE	CVE-2022-36316
CVE	CVE-2022-36317
CVE	CVE-2022-36318
CVE	CVE-2022-36319
CVE	CVE-2022-36320
XREF	IAVA:2022-A-0298

Plugin Information

Published: 2022/07/27, Modified: 2022/07/29

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 103.0
```

117941 - Mozilla Firefox < 49 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 49. It is, therefore, affected by multiple vulnerabilities as noted in Mozilla Firefox stable channel update release notes for 2016/09/20. Please refer to the release notes for additional information. Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?a71b5c71
http://www.nessus.org/u?27887241
http://www.nessus.org/u?4caa1ed8
http://www.nessus.org/u?32eb4c7a
http://www.nessus.org/u?5ef629bf
http://www.nessus.org/u?8865b1d7
http://www.nessus.org/u?160280d4
http://www.nessus.org/u?5dbbf44e
http://www.nessus.org/u?54ac5d09
http://www.nessus.org/u?d3bfda65
http://www.nessus.org/u?5d89bb27
http://www.nessus.org/u?f45fb2ce
http://www.nessus.org/u?47a40c69
http://www.nessus.org/u?0baaaa08
http://www.nessus.org/u?1181d174
http://www.nessus.org/u?2269f975
http://www.nessus.org/u?b74c22ad
http://www.nessus.org/u?7882d62d
http://www.nessus.org/u?0e281edf
http://www.nessus.org/u?117622e5
http://www.nessus.org/u?4b353376
http://www.nessus.org/u?6207b3c0
http://www.nessus.org/u?7e04baf7
http://www.nessus.org/u?527385b7
http://www.nessus.org/u?40b8f022
http://www.nessus.org/u?0d9488e8

http://www.nessus.org/u?c74b0ed3
http://www.nessus.org/u?8e935ffb
http://www.nessus.org/u?d5be7ccc
http://www.nessus.org/u?c34feae8
http://www.nessus.org/u?c773d903
http://www.nessus.org/u?8e86e0c1
http://www.nessus.org/u?8b727e4e

Solution

Upgrade to Mozilla Firefox version 49 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)

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-2016-2827
CVE	CVE-2016-5256
CVE	CVE-2016-5257
CVE	CVE-2016-5270
CVE	CVE-2016-5271
CVE	CVE-2016-5272
CVE	CVE-2016-5273
CVE	CVE-2016-5274
CVE	CVE-2016-5275
CVE	CVE-2016-5276
CVE	CVE-2016-5277
CVE	CVE-2016-5278

CVE	CVE-2016-5279
CVE	CVE-2016-5280
CVE	CVE-2016-5281
CVE	CVE-2016-5282
CVE	CVE-2016-5283
CVE	CVE-2016-5284

Plugin Information

Published: 2018/10/05, Modified: 2019/11/01

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 49
```

93662 - Mozilla Firefox < 49.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 49.0. It is, therefore, affected by multiple vulnerabilities :

- An out-of-bounds read error exists within file dom/security/nsCSPParser.cpp when handling content security policies (CSP) containing empty referrer directives. An unauthenticated, remote attacker can exploit this to cause a denial of service condition.

(CVE-2016-2827)

- Multiple memory safety issues exist that allow an unauthenticated, remote attacker to potentially execute arbitrary code. (CVE-2016-5256, CVE-2016-5257)

- A heap buffer overflow condition exists in the nsCaseTransformTextRunFactory::TransformString() function in layout/generic/nsTextRunTransformations.cpp when converting text containing certain Unicode characters. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-5270)

- An out-of-bounds read error exists in the nsCSSFrameConstructor::GetInsertionPrevSibling() function in file layout/base/nsCSSFrameConstructor.cpp when handling text runs. An unauthenticated, remote attacker can exploit this to disclose memory contents.

(CVE-2016-5271)

- A type confusion error exists within file layout/forms/nsRangeFrame.cpp when handling layout with input elements. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-5272)

- An unspecified flaw exists in the HyperTextAccessible::GetChildOffset() function that allows an unauthenticated, remote attacker to execute arbitrary code. (CVE-2016-5273)

- A use-after-free error exists within file layout/style/nsRuleNode.cpp when handling web animations during restyling. An unauthenticated, remote attacker can exploit this to execute arbitrary code.

(CVE-2016-5274)

- A buffer overflow condition exists in the FilterSupport::ComputeSourceNeededRegions() function when handling empty filters during canvas rendering. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-5275)

- A use-after-free error exists in the DocAccessible::ProcessInvalidationList() function within file accessible/generic/DocAccessible.cpp when setting an aria-owns attribute. An unauthenticated, remote attacker can exploit this to execute arbitrary code.

(CVE-2016-5276)

- A use-after-free error exists in the nsRefreshDriver::Tick() function when handling web animations destroying a timeline. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-5277)

- A buffer overflow condition exists in the nsBMPEncoder::AddImageFrame() function within file dom/base/ImageEncoder.cpp when encoding image frames to images. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-5278)

- A flaw exists that is triggered when handling drag-and-drop events for files. An unauthenticated, remote attacker can exploit this disclose the full local file path. (CVE-2016-5279)

- A use-after-free error exists in the nsTextNodeDirectionalityMap::RemoveElementFromMap() function within file dom/base/DirectionalityUtils.cpp when handling changing of text direction. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-5280)

- A use-after-free error exists when handling SVG format content that is being manipulated through script code.

An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-5281)

- A flaw exists when handling content that requests favicons from non-whitelisted schemes that are using certain URI handlers. An unauthenticated, remote attacker can exploit this to bypass intended restrictions. (CVE-2016-5282)

- A flaw exists that is related to the handling of iframes that allow an unauthenticated, remote attacker to conduct an 'iframe src' fragment timing attack, resulting in disclosure of cross-origin data.

(CVE-2016-5283)

- A flaw exists due to the certificate pinning policy for built-in sites (e.g., addons.mozilla.org) not being honored when pins have expired. A man-in-the-middle (MitM) attacker can exploit this to generate a trusted certificate, which could be used to conduct spoofing attacks. (CVE-2016-5284)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2016-85/

Solution

Upgrade to Mozilla Firefox version 49.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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	93049
BID	93052
CVE	CVE-2016-2827
CVE	CVE-2016-5256
CVE	CVE-2016-5257
CVE	CVE-2016-5270
CVE	CVE-2016-5271
CVE	CVE-2016-5272
CVE	CVE-2016-5273
CVE	CVE-2016-5274
CVE	CVE-2016-5275
CVE	CVE-2016-5276
CVE	CVE-2016-5277
CVE	CVE-2016-5278
CVE	CVE-2016-5279
CVE	CVE-2016-5280
CVE	CVE-2016-5281
CVE	CVE-2016-5282
CVE	CVE-2016-5283
CVE	CVE-2016-5284
XREF	MFSA:2016-85

Plugin Information

Published: 2016/09/22, Modified: 2019/11/14

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 49
```

94960 - Mozilla Firefox < 50.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 50.0. It is, therefore, affected by multiple vulnerabilities, the majority of which are remote code execution vulnerabilities. An unauthenticated, remote attacker can exploit these vulnerabilities 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/mfsa2016-89/

Solution

Upgrade to Mozilla Firefox version 50.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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	94335
BID	94336
BID	94337
BID	94339
BID	94341

CVE	CVE-2016-5289
CVE	CVE-2016-5290
CVE	CVE-2016-5291
CVE	CVE-2016-5292
CVE	CVE-2016-5293
CVE	CVE-2016-5294
CVE	CVE-2016-5295
CVE	CVE-2016-5296
CVE	CVE-2016-5297
CVE	CVE-2016-9063
CVE	CVE-2016-9064
CVE	CVE-2016-9066
CVE	CVE-2016-9067
CVE	CVE-2016-9068
CVE	CVE-2016-9069
CVE	CVE-2016-9070
CVE	CVE-2016-9071
CVE	CVE-2016-9072
CVE	CVE-2016-9073
CVE	CVE-2016-9074
CVE	CVE-2016-9075
CVE	CVE-2016-9076
CVE	CVE-2016-9077
XREF	MFSA:2016-89

Plugin Information

Published: 2016/11/18, Modified: 2019/11/14

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 50
```

95886 - Mozilla Firefox < 50.1 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 50.1. It is, therefore, affected by the following vulnerabilities :

- Multiple memory corruption issues exists when handling style contexts, regular expressions, and clamped gradients that allow an unauthenticated, remote attacker to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-9080)

- Multiple memory corruption issues exists, such as when handling document state changes or HTML5 content, or else due to dereferencing already freed memory or improper validation of user-supplied input. An unauthenticated, remote attacker can exploit these to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-9893)

- A buffer overflow condition exists in SkiaGl, within the GrResourceProvider::createBuffer() function in file gfx/skia/skia/src/gpu/GrResourceProvider.cpp, due to a GrGLBuffer being truncated during allocation. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-9894)

- A security bypass vulnerability exists due to event handlers for marquee elements being executed despite a Content Security Policy (CSP) that disallowed inline JavaScript. An unauthenticated, remote attacker can exploit this to impact integrity. (CVE-2016-9895)

- A use-after-free error exists within WebVR when handling the navigator object. An unauthenticated, remote attacker can exploit this to dereference already freed memory, resulting in the execution of arbitrary code.

(CVE-2016-9896)

- A memory corruption issue exists in libGLES when WebGL functions use a vector constructor with a varying array within libGLES. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-9897)

- A use-after-free error exists in Editor, specifically within file editor/libeditor/HTMLEditor.cpp, when handling DOM subtrees. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code.

(CVE-2016-9898)

- A use-after-free error exists in the nsNodeUtils::CloneAndAdopt() function within file dom/base/nsNodeUtils.cpp, while manipulating DOM events and removing audio elements, due to improper handling of failing node adoption. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code.

(CVE-2016-9899)

- A security bypass vulnerability exists in the nsDataDocumentContentPolicy::ShouldLoad() function within file dom/base/nsDataDocumentContentPolicy.cpp that allows external resources to be inappropriately loaded by SVG images by utilizing 'data:' URLs. An unauthenticated, remote attacker can exploit this to disclose sensitive cross-domain information.

(CVE-2016-9900)

- A flaw exists due to improper sanitization of HTML tags received from the Pocket server. An unauthenticated, remote attacker can exploit this to run JavaScript code in the about:pocket-saved (unprivileged) page, giving it access to Pocket's messaging API through HTML injection.

(CVE-2016-9901)

- A flaw exists in the Pocket toolbar button, specifically in browser/extensions/pocket/content/main.js, due to improper verification of the origin of events fired from its own pages. An unauthenticated, remote attacker can exploit this to inject content and commands from other origins into the Pocket context. Note that this issue does not affect users with e10s enabled. (CVE-2016-9902)

- A universal cross-site scripting (XSS) vulnerability exists in the Add-ons SDK, specifically within files addon-sdk/source/lib/sdk/ui/frame/view.html and addon-sdk/source/lib/sdk/ui/frame/view.js, due to improper validation of input before returning it to users. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to execute arbitrary script code in a user's browser session.

(CVE-2016-9903)

- An information disclosure vulnerability exists that allows an unauthenticated, remote attacker to determine whether an atom is used by another compartment or zone in specific contexts, by utilizing a JavaScript Map/Set timing attack. (CVE-2016-9904)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2016-94/

Solution

Upgrade to Mozilla Firefox version 50.1 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

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

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

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

References

BID	94883

BID	94885
CVE	CVE-2016-9080
CVE	CVE-2016-9893
CVE	CVE-2016-9894
CVE	CVE-2016-9895
CVE	CVE-2016-9896
CVE	CVE-2016-9897
CVE	CVE-2016-9898
CVE	CVE-2016-9899
CVE	CVE-2016-9900
CVE	CVE-2016-9901
CVE	CVE-2016-9902
CVE	CVE-2016-9903
CVE	CVE-2016-9904
XREF	MFSA:2016-94

Exploitable With

Core Impact (true)

Plugin Information

Published: 2016/12/15, Modified: 2019/11/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 50.1
```

96776 - Mozilla Firefox < 51.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 51.0. 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)

- Mozilla developers and community members Gary Kwong, Olli Pettay, Tooru Fujisawa, Carsten Book, Andrew McCreight, Chris Pearce, Ronald Crane, Jan de Mooij, Julian Seward, Nicolas Pierron, Randell Jesup, Esther Monchari, Honza Bambas, and Philipp reported memory safety bugs present in Firefox 50.1. 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-2017-5374)

- 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)

- A memory corruption vulnerability in Skia that can occur when using transforms to make gradients, resulting in a potentially exploitable crash.

(CVE-2017-5377)

- 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)

- Use-after-free vulnerability in Web Animations when interacting with cycle collection found through fuzzing. (CVE-2017-5379)

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

- The 'export' function in the Certificate Viewer can force local filesystem navigation when the 'common name' in a certificate contains slashes, allowing certificate content to be saved in unsafe locations with an arbitrary filename. (CVE-2017-5381)

- Feed preview for RSS feeds can be used to capture errors and exceptions generated by privileged content, allowing for the exposure of internal information not meant to be seen by web content. (CVE-2017-5382)

- 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)

- Proxy Auto-Config (PAC) files can specify a JavaScript function called for all URL requests with the full URL path which exposes more information than would be sent to the proxy itself in the case of HTTPS. Normally

the Proxy Auto-Config file is specified by the user or machine owner and presumed to be non-malicious, but if a user has enabled Web Proxy Auto Detect (WPAD) this file can be served remotely. (CVE-2017-5384)

- Data sent with in multipart channels, such as the multipart/x-mixed-replace MIME type, will ignore the referrer-policy response header, leading to potential information disclosure for sites using this header.

(CVE-2017-5385)

- 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 existence of a specifically requested local file can be found due to the double firing of the 'onerror'

when the 'source' attribute on a <track> tag refers to a file that does not exist if the source page is loaded locally. (CVE-2017-5387)

- A STUN server in conjunction with a large number of 'webkitRTCPeerConnection' objects can be used to send large STUN packets in a short period of time due to a lack of rate limiting being applied on e10s systems, allowing for a denial of service attack. (CVE-2017-5388)

- WebExtensions could use the 'mozAddonManager' API by modifying the CSP headers on sites with the appropriate permissions and then using host requests to redirect script loads to a malicious site. This allows a malicious extension to then install additional extensions without explicit user permission.

(CVE-2017-5389)

- 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)

- Special 'about:' pages used by web content, such as RSS feeds, can load privileged 'about:' pages in an iframe.

If a content-injection bug were found in one of those pages this could allow for potential privilege escalation. (CVE-2017-5391)

- The 'mozAddonManager' allows for the installation of extensions from the CDN for addons.mozilla.org, a publicly accessible site. This could allow malicious extensions to install additional extensions from the CDN in combination with an XSS attack on Mozilla AMO sites.

(CVE-2017-5393)

- 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/mfsa2017-01/

https://bugzilla.mozilla.org/show_bug.cgi?id=1017616

https://bugzilla.mozilla.org/show_bug.cgi?id=1255474

https://bugzilla.mozilla.org/show_bug.cgi?id=1281482
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=1288561
https://bugzilla.mozilla.org/show_bug.cgi?id=1293327
https://bugzilla.mozilla.org/show_bug.cgi?id=1295023
https://bugzilla.mozilla.org/show_bug.cgi?id=1295322
https://bugzilla.mozilla.org/show_bug.cgi?id=1295747
https://bugzilla.mozilla.org/show_bug.cgi?id=1295945
https://bugzilla.mozilla.org/show_bug.cgi?id=1297361
https://bugzilla.mozilla.org/show_bug.cgi?id=1297808
https://bugzilla.mozilla.org/show_bug.cgi?id=1300145
https://bugzilla.mozilla.org/show_bug.cgi?id=1302231
https://bugzilla.mozilla.org/show_bug.cgi?id=1306883
https://bugzilla.mozilla.org/show_bug.cgi?id=1307458
https://bugzilla.mozilla.org/show_bug.cgi?id=1308688
https://bugzilla.mozilla.org/show_bug.cgi?id=1309198
https://bugzilla.mozilla.org/show_bug.cgi?id=1309282
https://bugzilla.mozilla.org/show_bug.cgi?id=1309310
https://bugzilla.mozilla.org/show_bug.cgi?id=1311319
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=1313385
https://bugzilla.mozilla.org/show_bug.cgi?id=1315447
https://bugzilla.mozilla.org/show_bug.cgi?id=1317501
https://bugzilla.mozilla.org/show_bug.cgi?id=1318766
https://bugzilla.mozilla.org/show_bug.cgi?id=1319070
https://bugzilla.mozilla.org/show_bug.cgi?id=1319456
https://bugzilla.mozilla.org/show_bug.cgi?id=1319888
https://bugzilla.mozilla.org/show_bug.cgi?id=1321374
https://bugzilla.mozilla.org/show_bug.cgi?id=1322107
https://bugzilla.mozilla.org/show_bug.cgi?id=1322305
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=1324810
https://bugzilla.mozilla.org/show_bug.cgi?id=1325200

https://bugzilla.mozilla.org/show_bug.cgi?id=1325344
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=1329989
https://bugzilla.mozilla.org/show_bug.cgi?id=1330769
https://bugzilla.mozilla.org/show_bug.cgi?id=1331058
http://www.nessus.org/u?4d11b233

Solution

Upgrade to Mozilla Firefox version 51.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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	95759
BID	95761
BID	95762
BID	95763
BID	95769
CVE	CVE-2017-5373

CVE	CVE-2017-5374
CVE	CVE-2017-5375
CVE	CVE-2017-5376
CVE	CVE-2017-5377
CVE	CVE-2017-5378
CVE	CVE-2017-5379
CVE	CVE-2017-5380
CVE	CVE-2017-5381
CVE	CVE-2017-5382
CVE	CVE-2017-5383
CVE	CVE-2017-5384
CVE	CVE-2017-5385
CVE	CVE-2017-5386
CVE	CVE-2017-5387
CVE	CVE-2017-5388
CVE	CVE-2017-5389
CVE	CVE-2017-5390
CVE	CVE-2017-5391
CVE	CVE-2017-5393
CVE	CVE-2017-5396
XREF	MFSA:2017-01

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 51.0
```

97639 - Mozilla Firefox < 52.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 52.0. 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)

- Mozilla developers and community members Carsten Book, Calixte Denizet, Christian Holler, Andrew McCreight, David Bolter, David Keeler, Jon Coppeard, Tyson Smith, Ronald Crane, Tooru Fujisawa, Ben Kelly, Bob Owen, Jed Davis, Julian Seward, Julian Hector, Philipp, Markus Stange, and Andre Bargull reported memory safety bugs present in Firefox 51. 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-2017-5399)

- 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)

- When adding a range to an object in the DOM, it is possible to use addRange to add the range to an incorrect root object. This triggers a use-after-free, resulting in a potentially exploitable crash.

(CVE-2017-5403)

- 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)

- A segmentation fault can occur in the Skia graphics library during some canvas operations due to issues with mask/clip intersection and empty masks.

(CVE-2017-5406)

- 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)

- A use-after-free can occur during buffer storage operations within the ANGLE graphics library, used for WebGL content. The buffer storage can be freed while still in use in some circumstances, leading to a potentially exploitable crash. Note: This issue is in libGLES, which is only in use on Windows. Other operating systems are not affected. (CVE-2017-5411)

- A buffer overflow read during SVG filter color value operations, resulting in data exposure. (CVE-2017-5412)

- A segmentation fault can occur during some bidirectional layout operations. (CVE-2017-5413)

- The file picker dialog can choose and display the wrong local default directory when instantiated. On some operating systems, this can lead to information disclosure, such as the operating system or the local account name. (CVE-2017-5414)

- An attack can use a blob URL and script to spoof an arbitrary addressbar URL prefaced by blob: as the protocol, leading to user confusion and further spoofing attacks. (CVE-2017-5415)

- In certain circumstances a networking event listener can be prematurely released. This appears to result in a null dereference in practice. (CVE-2017-5416)

- When dragging content from the primary browser pane to the addressbar on a malicious site, it is possible to change the addressbar so that the displayed location following navigation does not match the URL of the newly loaded page. This allows for spoofing attacks.

(CVE-2017-5417)

- An out of bounds read error occurs when parsing some HTTP digest authorization responses, resulting in information leakage through the reading of random memory containing matches to specifically set patterns.

(CVE-2017-5418)

- If a malicious site repeatedly triggers a modal authentication prompt, eventually the browser UI will become non-responsive, requiring shutdown through the operating system. This is a denial of service (DOS) attack. (CVE-2017-5419)

- A javascript: url loaded by a malicious page can obfuscate its location by blanking the URL displayed in the addressbar, allowing for an attacker to spoof an existing page without the malicious page's address being displayed correctly. (CVE-2017-5420)

- A malicious site could spoof the contents of the print preview window if popup windows are enabled, resulting in user confusion of what site is currently loaded.

(CVE-2017-5421)

- If a malicious site uses the view-source: protocol in a series within a single hyperlink, it can trigger a non-exploitable browser crash when the hyperlink is selected. This was fixed by no longer making view-source: linkable. (CVE-2017-5422)

- A non-existent chrome.manifest file will attempt to be loaded during startup from the primary installation directory. If a malicious user with local access puts chrome.manifest and other referenced files in this directory, they will be loaded and activated during startup. This could result in malicious software being added without consent or modification of referenced installed files. (CVE-2017-5427)

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/mfsa2017-05/

Solution

Upgrade to Mozilla Firefox version 52.0 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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	96691
BID	96692
BID	96693
BID	96696

CVE	CVE-2017-5398
CVE	CVE-2017-5399
CVE	CVE-2017-5400
CVE	CVE-2017-5401
CVE	CVE-2017-5402
CVE	CVE-2017-5403
CVE	CVE-2017-5404
CVE	CVE-2017-5405
CVE	CVE-2017-5406
CVE	CVE-2017-5407
CVE	CVE-2017-5408
CVE	CVE-2017-5409
CVE	CVE-2017-5410
CVE	CVE-2017-5411
CVE	CVE-2017-5412
CVE	CVE-2017-5413
CVE	CVE-2017-5414
CVE	CVE-2017-5415
CVE	CVE-2017-5416
CVE	CVE-2017-5417
CVE	CVE-2017-5418
CVE	CVE-2017-5419
CVE	CVE-2017-5420
CVE	CVE-2017-5421
CVE	CVE-2017-5422
CVE	CVE-2017-5427
XREF	MFSA:2017-05

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 52.0
```

99125 - Mozilla Firefox < 52.0.1 CreateImageBitmap RCE

Synopsis

The remote Windows host contains a web browser that is affected by a remote code execution vulnerability.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 52.0.1. It is, therefore, affected by an integer overflow condition in the nsGlobalWindow::CreateImageBitmap() function within file dom/base/nsGlobalWindow.cpp due to improper validation of certain input. An unauthenticated, remote attacker can exploit this to corrupt memory, possibly resulting in the execution of arbitrary code.

Note that this function runs in the content sandbox, requiring a second vulnerability to compromise a user's computer.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2017-08/

Solution

Upgrade to Mozilla Firefox version 52.0.1 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)

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	96959
CVE	CVE-2017-5428

XREF MFSA:2017-08

Plugin Information

Published: 2017/03/31, Modified: 2019/11/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 52.0.1
```

99632 - Mozilla Firefox < 53 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 53. It is, therefore, affected by the following vulnerabilities :

- Multiple buffer overflow conditions exist in the FLEX generated code due to improper validation of certain input. An unauthenticated, remote attacker can exploit these to execute arbitrary code. (CVE-2016-6354, CVE-2017-5469)

- Multiple flaws exist in the Libevent library, within files evdns.c and evutil.c, due to improper validation of input when handling IP address strings, empty base name strings, and DNS packets. An unauthenticated, remote attacker can exploit these to cause a denial of service condition or the execution of arbitrary code.

(CVE-2016-10195, CVE-2016-10196, CVE-2016-10197, CVE-2017-5437)

- Multiple memory corruption issues exist that allow an unauthenticated, remote attacker to execute arbitrary code. (CVE-2017-5429, CVE-2017-5430)

- A use-after-free error exists in input text selection that allows an unauthenticated, remote attacker to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5432)

- A use-after-free error exists in the SMIL animation functions when handling animation elements. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5433)

- A use-after-free error exists when redirecting focus handling that allows an unauthenticated, remote attacker to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5434)

- A use-after-free error exists in design mode interactions when handling transaction processing in the editor. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5435)

- An out-of-bounds write error exists in the Graphite 2 library when handling specially crafted Graphite fonts.

An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5436)

- A use-after-free error exists in the nsAutoPtr() function during XSLT processing due to the result handler being held by a freed handler. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5438)

- A use-after-free error exists in the Length() function in nsTArray when handling template parameters during XSLT processing. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5439)

- A use-after-free error exists in the txExecutionState destructor when processing XSLT content. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5440)

- A use-after-free error exists when holding a selection during scroll events. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code.

(CVE-2017-5441)

- A use-after-free error exists when changing styles in DOM elements that allows an unauthenticated, remote attacker to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5442)

- An out-of-bounds write error exists while decoding improperly formed BinHex format archives that allows an unauthenticated, remote attacker to cause a denial of service condition or the execution of arbitrary code.

(CVE-2017-5443)

- A buffer overflow condition exists while parsing application/http-index-format format content due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via improperly formatted data, to disclose out-of-bounds memory content. (CVE-2017-5444)

- A flaw exists in nsDirIndexParser.cpp when parsing application/http-index-format format content in which uninitialized values are used to create an array. An unauthenticated, remote attacker can exploit this to disclose memory contents. (CVE-2017-5445)

- An out-of-bounds read error exists when handling HTTP/2 DATA connections to a server that sends DATA frames with incorrect content. An unauthenticated, remote attacker can exploit to cause a denial of service condition or the disclosure of memory contents. (CVE-2017-5446)

- An out-of-bounds read error exists when processing glyph widths during text layout. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the disclosure of memory contents.

(CVE-2017-5447)

- An out-of-bounds write error exists in the ClearKeyDecryptor::Decrypt() function within file ClearKeyDecryptionManager.cpp when decrypting Clearkey-encrypted media content. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code.

This vulnerability can only be exploited if a secondary mechanism can be used to escape the Gecko Media Plugin (GMP) sandbox. (CVE-2017-5448)

- A flaw exists when handling bidirectional Unicode text in conjunction with CSS animations that allows an unauthenticated, remote attacker to cause a denial of service condition or the execution or arbitrary code.

(CVE-2017-5449)

- A flaw exists in the handling of specially crafted 'onblur' events. An unauthenticated, remote attacker can exploit this, via a specially crafted event, to spoof the address bar, making the loaded site appear to be different from the one actually loaded. (CVE-2017-5451)

- A flaw exists in the RSS reader preview page due to improper sanitization of URL parameters for a feed's TITLE element. An unauthenticated, remote attacker can exploit this to spoof the TITLE element. However, no scripted content can be run. (CVE-2017-5453)

- A flaw exists in the FileSystemSecurity::Forget() function within file FileSystemSecurity.cpp when using the File Picker due to improper sanitization of input containing path traversal sequences. An unauthenticated, remote attacker can exploit this to bypass file system access protections in the sandbox and read arbitrary files on the local file system. (CVE-2017-5454)

- An unspecified flaw exists in the internal feed reader APIs when handling messages. An unauthenticated, remote attacker can exploit this to escape the sandbox and gain elevated privileges if it can be combined with another vulnerability that allows remote code execution inside the sandboxed process. (CVE-2017-5455)

- A flaw exists in the Entries API when using a file system request constructor through an IPC message. An unauthenticated, remote attacker can exploit this to bypass file system access protections in the sandbox and gain read and write access to the local file system.

(CVE-2017-5456)

- A reflected cross-site scripting (XSS) vulnerability exists when dragging and dropping a 'javascript:' URL into the address bar due to improper validation of input. An unauthenticated, remote attacker can exploit this to execute arbitrary script code in a user's browser session. (CVE-2017-5458)

- A buffer overflow condition exists in WebGL when handling web content due to improper validation of certain input. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5459)

- A use-after-free error exists in frame selection when handling a specially crafted combination of script content and key presses by the user. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code.

(CVE-2017-5460)

- An out-of-bounds write error exists in the Network Security Services (NSS) library during Base64 decoding operations due to insufficient memory being allocated to a buffer. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5461)

- A flaw exists in the Network Security Services (NSS) library during DRBG number generation due to the internal state V not correctly carrying bits over. An unauthenticated, remote attacker can exploit this to potentially cause predictable random number generation.

(CVE-2017-5462)

- A flaw exists when making changes to DOM content in the accessibility tree due to improper validation of certain input, which can lead to the DOM tree becoming out of sync with the accessibility tree. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2017-5464)

- An out-of-bounds read error exists in ConvolvePixel when processing SVG content, which allows for otherwise inaccessible memory being copied into SVG graphic content. An unauthenticated, remote attacker can exploit this to disclose memory contents or cause a denial of service condition. (CVE-2017-5465)

- A cross-site script (XSS) vulnerability exists due to improper handling of data:text/html URL redirects when a reload is triggered, which causes the reloaded data:text/html page to have its origin set incorrectly.

An unauthenticated, remote attacker can exploit this, via a specially crafted request, to execute arbitrary script code in a user's browser session. (CVE-2017-5466)

- A memory corruption issue exists when rendering Skia content outside of the bounds of a clipping region due to improper validation of certain input. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5467)

- A flaw exists in the developer tools due to an incorrect ownership model of privateBrowsing information. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-5468)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2017-10/

Solution

Upgrade to Mozilla Firefox version 53 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)

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

BID	92141
BID	96014
BID	97940
CVE	CVE-2016-6354
CVE	CVE-2016-10195
CVE	CVE-2016-10196
CVE	CVE-2016-10197
CVE	CVE-2017-5429
CVE	CVE-2017-5430
CVE	CVE-2017-5432
CVE	CVE-2017-5433
CVE	CVE-2017-5434
CVE	CVE-2017-5435
CVE	CVE-2017-5436
CVE	CVE-2017-5437
CVE	CVE-2017-5438
CVE	CVE-2017-5439
CVE	CVE-2017-5440
CVE	CVE-2017-5441
CVE	CVE-2017-5442

CVE	CVE-2017-5443
CVE	CVE-2017-5444
CVE	CVE-2017-5445
CVE	CVE-2017-5446
CVE	CVE-2017-5447
CVE	CVE-2017-5448
CVE	CVE-2017-5449
CVE	CVE-2017-5451
CVE	CVE-2017-5453
CVE	CVE-2017-5454
CVE	CVE-2017-5455
CVE	CVE-2017-5456
CVE	CVE-2017-5458
CVE	CVE-2017-5459
CVE	CVE-2017-5460
CVE	CVE-2017-5461
CVE	CVE-2017-5462
CVE	CVE-2017-5464
CVE	CVE-2017-5465
CVE	CVE-2017-5466
CVE	CVE-2017-5467
CVE	CVE-2017-5468
CVE	CVE-2017-5469
XREF	MFSA:2017-10

Plugin Information

Published: 2017/04/24, Modified: 2019/11/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 53
```

100810 - Mozilla Firefox < 54 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 54. It is, therefore, affected by multiple vulnerabilities :

- Multiple memory corruption issues exist that allow an unauthenticated, remote attacker to execute arbitrary code by convincing a user to visit a specially crafted website. (CVE-2017-5470, CVE-2017-5471)

- A use-after-free error exists in the EndUpdate() function in nsCSSFrameConstructor.cpp that is triggered when reconstructing trees during regeneration of CSS layouts. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted website, to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-5472)

- A use-after-free error exists in the Reload() function in nsDocShell.cpp that is triggered when using an incorrect URL during the reload of a docshell. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-7749)

- A use-after-free error exists in the Hide() function in nsDocumentViewer.cpp that is triggered when handling track elements. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-7750)

- A use-after-free error exists in the nsDocumentViewer class in nsDocumentViewer.cpp that is triggered when handling content viewer listeners. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code.

(CVE-2017-7751)

- A use-after-free error exists that is triggered when handling events while specific user interaction occurs with the input method editor (IME). An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code.

(CVE-2017-7752)

- An out-of-bounds read error exists in the IsComplete() function in WebGLTexture.cpp that is triggered when handling textures. An unauthenticated, remote attacker can exploit this to disclose memory contents.

(CVE-2017-7754)

- A privilege escalation vulnerability exists due to improper loading of dynamic-link library (DLL) files. A local attacker can exploit this, via a specially crafted DLL file in the installation path, to inject and execute arbitrary code. (CVE-2017-7755)

- A use-after-free error exists in the SetRequestHead() function in XMLHttpRequestMainThread.cpp that is triggered when logging XML HTTP Requests (XHR). An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-7756)

- A use-after-free error exists in ActorsParent.cpp due to improper handling of objects in memory. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-7757)

- An out-of-bounds read error exists in the AppendAudioSegment() function in TrackEncoder.cpp that is triggered when the number of channels in an audio stream changes while the Opus encoder is in use. An unauthenticated, remote attacker can exploit this to disclose sensitive information. (CVE-2017-7758)

- A flaw exists in the NS_main() function in updater.cpp due to improper validation of input when handling callback file path parameters. A local attacker can exploit this to manipulate files in the installation directory. (CVE-2017-7760)

- A flaw exists in the Maintenance Service helper.exe application that is triggered as permissions for a temporary directory are set to writable by non-privileged users. A local attacker can exploit this to delete arbitrary files on the system. (CVE-2017-7761)

- A flaw exists that is triggered when displaying URLs including authentication sections in reader mode. An unauthenticated, remote attacker can exploit this, via a specially crafted URL, to spoof domains in the address bar. (CVE-2017-7762)

- A flaw exists in the isLabelSafe() function in nsIDNService.cpp that is triggered when handling characters from different unicode blocks. An unauthenticated, remote attacker can exploit this, via a specially crafted IDN domain, to spoof a valid URL and conduct phishing attacks. (CVE-2017-7764)

- A flaw exists that is triggered due to improper parsing of long filenames when handling downloaded files. An unauthenticated, remote attacker can exploit this to cause a file to be downloaded without the 'mark-of-the-web' applied, resulting in security warnings for executables not being displayed.

(CVE-2017-7765)

- A flaw exists in the Mozilla Maintenance Service that is triggered when handling paths for the 'patch', 'install', and 'working' directories. A local attacker can exploit this to execute arbitrary code with elevated privileges. (CVE-2017-7766)

- A flaw exists in the Mozilla Maintenance Service that is triggered when being invoked using the Mozilla Windows Updater. A local attacker can exploit this to overwrite arbitrary files with random data. (CVE-2017-7767)

- A flaw exists in the IsStatusApplying() function in workmonitor.cpp that is triggered when logging the update status. A local attacker can exploit this to read 32 bytes of arbitrary files. (CVE-2017-7768)

- Multiple integer overflow conditions exist in the Graphite component in the decompress() function in Decompressor.cpp due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2017-7772, CVE-2017-7778)

- An out-of-bounds read error exists in the Graphite component in the readGraphite() function in Silf.cpp. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or disclose memory contents. (CVE-2017-7774)

- An assertion flaw exists in the Graphite component when handling zero value sizes. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-7775)

- An out-of-bounds read error exists in the Graphite component in getClassGlyph() function in Silf.cpp due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-7776)

- A flaw exists in the Graphite component in the read_glyph() function in GlyphCache.cpp related to use of uninitialized memory. An unauthenticated, remote attacker can exploit this to have an unspecified impact.

(CVE-2017-7777)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2017-15/

Solution

Upgrade to Mozilla Firefox version 54 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)

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	99040
BID	99041
BID	99042
BID	99047
BID	99057
CVE	CVE-2017-5470
CVE	CVE-2017-5471
CVE	CVE-2017-5472
CVE	CVE-2017-7749
CVE	CVE-2017-7750
CVE	CVE-2017-7751
CVE	CVE-2017-7752
CVE	CVE-2017-7754
CVE	CVE-2017-7755
CVE	CVE-2017-7756
CVE	CVE-2017-7757
CVE	CVE-2017-7758

CVE	CVE-2017-7760
CVE	CVE-2017-7761
CVE	CVE-2017-7762
CVE	CVE-2017-7764
CVE	CVE-2017-7765
CVE	CVE-2017-7766
CVE	CVE-2017-7767
CVE	CVE-2017-7768
CVE	CVE-2017-7772
CVE	CVE-2017-7774
CVE	CVE-2017-7775
CVE	CVE-2017-7776
CVE	CVE-2017-7777
CVE	CVE-2017-7778
XREF	MFSA:2017-15

Plugin Information

Published: 2017/06/15, Modified: 2019/11/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 54
```

102359 - Mozilla Firefox < 55 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 55. It is, therefore, affected by multiple vulnerabilities, some of which allow code execution and potentially exploitable crashes.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2017-18/

Solution

Upgrade to Mozilla Firefox version 55 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)

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	100196
BID	100197
BID	100198
BID	100199
BID	100201
BID	100202

BID	100203
BID	100206
BID	100234
CVE	CVE-2017-7753
CVE	CVE-2017-7779
CVE	CVE-2017-7780
CVE	CVE-2017-7781
CVE	CVE-2017-7782
CVE	CVE-2017-7783
CVE	CVE-2017-7784
CVE	CVE-2017-7785
CVE	CVE-2017-7786
CVE	CVE-2017-7787
CVE	CVE-2017-7788
CVE	CVE-2017-7789
CVE	CVE-2017-7790
CVE	CVE-2017-7791
CVE	CVE-2017-7792
CVE	CVE-2017-7794
CVE	CVE-2017-7796
CVE	CVE-2017-7797
CVE	CVE-2017-7798
CVE	CVE-2017-7799
CVE	CVE-2017-7800
CVE	CVE-2017-7801
CVE	CVE-2017-7802
CVE	CVE-2017-7803
CVE	CVE-2017-7804
CVE	CVE-2017-7806
CVE	CVE-2017-7807
CVE	CVE-2017-7808
CVE	CVE-2017-7809
XREF	MFSA:2017-18

Plugin Information

Published: 2017/08/10, Modified: 2019/11/12

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
```

```
    Fixed version     : 55
```

103680 - Mozilla Firefox < 56 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 56. It is, therefore, affected by multiple vulnerabilities, some of which allow code execution and potentially exploitable crashes.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2017-21/

Solution

Upgrade to Mozilla Firefox version 56 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)

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	101053
BID	101054
BID	101055
BID	101057
CVE	CVE-2017-7793
CVE	CVE-2017-7805

CVE	CVE-2017-7810
CVE	CVE-2017-7811
CVE	CVE-2017-7812
CVE	CVE-2017-7813
CVE	CVE-2017-7814
CVE	CVE-2017-7815
CVE	CVE-2017-7816
CVE	CVE-2017-7817
CVE	CVE-2017-7818
CVE	CVE-2017-7819
CVE	CVE-2017-7820
CVE	CVE-2017-7821
CVE	CVE-2017-7822
CVE	CVE-2017-7823
CVE	CVE-2017-7824
XREF	MFSA:2017-21

Plugin Information

Published: 2017/10/06, Modified: 2019/11/12

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 56
```

104638 - Mozilla Firefox < 57 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 57. It is, therefore, affected by multiple vulnerabilities, some of which allow code execution and potentially exploitable crashes.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2017-24/

Solution

Upgrade to Mozilla Firefox version 57 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)

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	101832
CVE	CVE-2017-7826
CVE	CVE-2017-7827
CVE	CVE-2017-7828
CVE	CVE-2017-7830
CVE	CVE-2017-7831

CVE	CVE-2017-7832
CVE	CVE-2017-7833
CVE	CVE-2017-7834
CVE	CVE-2017-7835
CVE	CVE-2017-7836
CVE	CVE-2017-7837
CVE	CVE-2017-7838
CVE	CVE-2017-7839
CVE	CVE-2017-7840
CVE	CVE-2017-7842
XREF	MFSA:2017-24

Plugin Information

Published: 2017/11/16, Modified: 2019/11/12

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 57
```

106303 - Mozilla Firefox < 58 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 58. It is, therefore, affected by multiple vulnerabilities, some of which allow code execution and potentially exploitable crashes.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2018-02/

Solution

Upgrade to Mozilla Firefox version 58 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)

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	102783
CVE	CVE-2018-5089
CVE	CVE-2018-5090
CVE	CVE-2018-5091
CVE	CVE-2018-5092
CVE	CVE-2018-5093

CVE	CVE-2018-5094
CVE	CVE-2018-5095
CVE	CVE-2018-5097
CVE	CVE-2018-5098
CVE	CVE-2018-5099
CVE	CVE-2018-5100
CVE	CVE-2018-5101
CVE	CVE-2018-5102
CVE	CVE-2018-5103
CVE	CVE-2018-5104
CVE	CVE-2018-5105
CVE	CVE-2018-5106
CVE	CVE-2018-5107
CVE	CVE-2018-5108
CVE	CVE-2018-5109
CVE	CVE-2018-5110
CVE	CVE-2018-5111
CVE	CVE-2018-5112
CVE	CVE-2018-5113
CVE	CVE-2018-5114
CVE	CVE-2018-5115
CVE	CVE-2018-5116
CVE	CVE-2018-5117
CVE	CVE-2018-5118
CVE	CVE-2018-5119
CVE	CVE-2018-5121
CVE	CVE-2018-5122
XREF	MFSA:2018-02

Plugin Information

Published: 2018/01/24, Modified: 2019/11/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 58
```

108377 - Mozilla Firefox < 59 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 59. It is, therefore, affected by multiple vulnerabilities, some of which allow code execution and potentially exploitable crashes.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2018-06/

Solution

Upgrade to Mozilla Firefox version 59 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)

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-2018-5125
CVE	CVE-2018-5126
CVE	CVE-2018-5127
CVE	CVE-2018-5128
CVE	CVE-2018-5129
CVE	CVE-2018-5130

CVE	CVE-2018-5131
CVE	CVE-2018-5132
CVE	CVE-2018-5133
CVE	CVE-2018-5134
CVE	CVE-2018-5135
CVE	CVE-2018-5136
CVE	CVE-2018-5137
CVE	CVE-2018-5138
CVE	CVE-2018-5140
CVE	CVE-2018-5141
CVE	CVE-2018-5142
CVE	CVE-2018-5143
XREF	MFSA:2018-06

Plugin Information

Published: 2018/03/15, Modified: 2019/11/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 59
```

108587 - Mozilla Firefox < 59.0.1 Multiple Code Execution Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 59.0.1. It is, therefore, affected by multiple code execution vulnerabilities. A out-of-bounds write flaw exists in multiple functions of the codebook.c script when decoding Vorbis audio data. A context-dependent attacker could corrupt memory and potentially execute arbitrary code.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2018-08/

Solution

Upgrade to Mozilla Firefox version 59.0.1 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)

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	103432
CVE	CVE-2018-5146
CVE	CVE-2018-5147
XREF	MFSA:2018-08

Plugin Information

Published: 2018/03/23, Modified: 2019/11/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 59.0.1
```

109869 - Mozilla Firefox < 60 Multiple Critical Vulnerabilities

Synopsis

A web browser installed on the remote Windows host is affected by multiple critical and high severity vulnerabilities.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 60. It is, therefore, affected by multiple critical and high severity vulnerabilities.

See Also

http://www.nessus.org/u?6e296858

Solution

Upgrade to Mozilla Firefox version 60.0.0 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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	104136
BID	104139
CVE	CVE-2018-5150
CVE	CVE-2018-5151
CVE	CVE-2018-5152
CVE	CVE-2018-5153

CVE	CVE-2018-5154
CVE	CVE-2018-5155
CVE	CVE-2018-5157
CVE	CVE-2018-5158
CVE	CVE-2018-5159
CVE	CVE-2018-5160
CVE	CVE-2018-5163
CVE	CVE-2018-5164
CVE	CVE-2018-5165
CVE	CVE-2018-5166
CVE	CVE-2018-5167
CVE	CVE-2018-5168
CVE	CVE-2018-5169
CVE	CVE-2018-5172
CVE	CVE-2018-5173
CVE	CVE-2018-5174
CVE	CVE-2018-5175
CVE	CVE-2018-5176
CVE	CVE-2018-5177
CVE	CVE-2018-5180
CVE	CVE-2018-5181
CVE	CVE-2018-5182
XREF	MFSA:2018-11

Plugin Information

Published: 2018/05/17, Modified: 2019/11/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 60.0.0
```

117294 - Mozilla Firefox < 62 Multiple Critical Vulnerabilities

Synopsis

A web browser installed on the remote Windows host is affected by multiple critical and high severity vulnerabilities.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 62. It is, therefore, affected by multiple critical and high severity vulnerabilities.

See Also

http://www.nessus.org/u?8517426b

Solution

Upgrade to Mozilla Firefox version 62.0.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

BID	101665
CVE	CVE-2017-16541
CVE	CVE-2018-12377
CVE	CVE-2018-12378
CVE	CVE-2018-12379
CVE	CVE-2018-12375

CVE	CVE-2018-12376
CVE	CVE-2018-12381
CVE	CVE-2018-12382
CVE	CVE-2018-12383
XREF	MFSA:2018-20

Plugin Information

Published: 2018/09/06, Modified: 2019/04/05

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 62.0.0
```

117921 - Mozilla Firefox < 62.0.3 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 62.0.3. It is, therefore, affected by multiple vulnerabilities as noted in Mozilla Firefox stable channel update release notes for 2018/10/02. Please refer to the release notes for additional information. Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self- reported version number.

See Also

http://www.nessus.org/u?3c59dd1b

http://www.nessus.org/u?b5d12f1e

http://www.nessus.org/u?0b443a0e

Solution

Upgrade to Mozilla Firefox version 62.0.3 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	105460
CVE	CVE-2018-12386

CVE	CVE-2018-12387
XREF	MFSA:2018-24

Plugin Information

Published: 2018/10/04, Modified: 2020/04/27

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 62.0.3
```

119604 - Mozilla Firefox < 64.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is is prior to 64.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2018-29 advisory.

- A buffer overflow occurs when drawing and validating elements with the ANGLE graphics library, used for WebGL content, when working with the VertexBuffer11 module. This results in a potentially exploitable crash. (CVE-2018-12407)

- 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)

- WebExtension content scripts can be loaded into about: pages in some circumstances, in violation of the permissions granted to extensions. This could allow an extension to interfere with the loading and usage of these pages and use capabilities that were intended to be restricted from extensions.

(CVE-2018-18495)

- When the RSS Feed preview about:feeds page is framed within another page, it can be used in concert with scripted content for a clickjacking attack that confuses users into downloading and executing an executable file from a temporary directory. *Note:

This issue only affects Windows operating systems. Other operating systems are not affected.*
(CVE-2018-18496)

- Limitations on the URIs allowed to WebExtensions by the browser.windows.create API can be bypassed when a pipe in the URL field is used within the extension to load multiple pages as a single argument.

This could allow a malicious WebExtension to opened privileged about: or file:

locations. (CVE-2018-18497)

- 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 can lead to an out-of-bounds write.

(CVE-2018-18498)

- The about:crashcontent and about:crashparent pages can be triggered by web content. These pages are used to crash the loaded page or the browser for test purposes. This issue allows for a non-persistent denial of service (DOS) attack by a malicious site which links to these pages.

(CVE-2018-18510)

- Mozilla developers and community members Alex Gaynor, Andr Bargull, Boris Zbarsky, Christian Holler, Jan de Mooij, Jason Kratzer, Philipp, Ronald Crane, Natalia Csoregi, and Paul Theriault reported memory safety bugs present in Firefox 63. 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-2018-12406)

- 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)

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/mfsa2018-29/

https://bugzilla.mozilla.org/show_bug.cgi?id=1422231

https://bugzilla.mozilla.org/show_bug.cgi?id=1427585

https://bugzilla.mozilla.org/show_bug.cgi?id=1434490

https://bugzilla.mozilla.org/show_bug.cgi?id=1456947

https://bugzilla.mozilla.org/show_bug.cgi?id=1458129

https://bugzilla.mozilla.org/show_bug.cgi?id=1475669

https://bugzilla.mozilla.org/show_bug.cgi?id=1481745

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

https://bugzilla.mozilla.org/show_bug.cgi?id=1488180

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

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=1499198

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

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

https://bugzilla.mozilla.org/show_bug.cgi?id=1500064

https://bugzilla.mozilla.org/show_bug.cgi?id=1500310

https://bugzilla.mozilla.org/show_bug.cgi?id=1500696

https://bugzilla.mozilla.org/show_bug.cgi?id=1500759

https://bugzilla.mozilla.org/show_bug.cgi?id=1502013

https://bugzilla.mozilla.org/show_bug.cgi?id=1502886

https://bugzilla.mozilla.org/show_bug.cgi?id=1503082

https://bugzilla.mozilla.org/show_bug.cgi?id=1503326
https://bugzilla.mozilla.org/show_bug.cgi?id=1504365
https://bugzilla.mozilla.org/show_bug.cgi?id=1504452
https://bugzilla.mozilla.org/show_bug.cgi?id=1504816
https://bugzilla.mozilla.org/show_bug.cgi?id=1505181
https://bugzilla.mozilla.org/show_bug.cgi?id=1505973
https://bugzilla.mozilla.org/show_bug.cgi?id=1506640
https://bugzilla.mozilla.org/show_bug.cgi?id=1507702
https://bugzilla.mozilla.org/show_bug.cgi?id=1510471

Solution

Upgrade to Mozilla Firefox version 64.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2018-12406
CVE	CVE-2018-12407
CVE	CVE-2018-17466
CVE	CVE-2018-18492
CVE	CVE-2018-18493
CVE	CVE-2018-18494
CVE	CVE-2018-18495
CVE	CVE-2018-18496

CVE	CVE-2018-18497
CVE	CVE-2018-18498
CVE	CVE-2018-18510
XREF	MFSA:2018-29

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 64.0
```

121512 - Mozilla Firefox < 65.0

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 65.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2019-01 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)

- When JavaScript is used to create and manipulate an audio buffer, a potentially exploitable crash may occur because of a compartment mismatch in some situations.

(CVE-2018-18503)

- A crash and out-of-bounds read can occur when the buffer of a texture client is freed while it is still in use during graphic operations. This results in a potentially exploitable crash and the possibility of reading from the memory of the freed buffers. (CVE-2018-18504)

- 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)

- When proxy auto-detection is enabled, if a web server serves a Proxy Auto-Configuration (PAC) file or if a PAC file is loaded locally, this PAC file can specify that requests to the localhost are to be sent through the proxy to another server. This behavior is disallowed by default when a proxy is manually configured, but when enabled could allow for attacks on services and tools that bind to the localhost for networked behavior if they are accessed through browsing. (CVE-2018-18506)

- Mozilla developers and community members Arthur Iakab, Christoph Diehl, Christian Holler, Kalel, Emilio Cobos Ivarez, Cristina Coroiu, Noemi Erli, Natalia Csoregi, Julian Seward, Gary Kwong, Tyson Smith, Yaron Tausky, and Ronald Crane reported memory safety bugs present in Firefox 64. 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-2018-18502)

- 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/mfsa2019-01/
https://bugzilla.mozilla.org/show_bug.cgi?id=1510114
https://bugzilla.mozilla.org/show_bug.cgi?id=1509442
https://bugzilla.mozilla.org/show_bug.cgi?id=1496413
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=1503393
https://bugzilla.mozilla.org/show_bug.cgi?id=1499426
https://bugzilla.mozilla.org/show_bug.cgi?id=1480090
https://bugzilla.mozilla.org/show_bug.cgi?id=1472990
https://bugzilla.mozilla.org/show_bug.cgi?id=1514762
https://bugzilla.mozilla.org/show_bug.cgi?id=1501482
https://bugzilla.mozilla.org/show_bug.cgi?id=1505887
https://bugzilla.mozilla.org/show_bug.cgi?id=1508102
https://bugzilla.mozilla.org/show_bug.cgi?id=1508618
https://bugzilla.mozilla.org/show_bug.cgi?id=1511580
https://bugzilla.mozilla.org/show_bug.cgi?id=1493497
https://bugzilla.mozilla.org/show_bug.cgi?id=1510145
https://bugzilla.mozilla.org/show_bug.cgi?id=1516289
https://bugzilla.mozilla.org/show_bug.cgi?id=1506798
https://bugzilla.mozilla.org/show_bug.cgi?id=1512758
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 version 65.0 or later.

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 v3.0 Temporal Score

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

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	106773
BID	106781
CVE	CVE-2018-18500
CVE	CVE-2018-18501
CVE	CVE-2018-18502
CVE	CVE-2018-18503
CVE	CVE-2018-18504
CVE	CVE-2018-18505
CVE	CVE-2018-18506
XREF	MFSA:2019-01

Plugin Information

Published: 2019/01/31, Modified: 2022/05/24

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 65.0
```

122948 - Mozilla Firefox < 66.0

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 66.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2019-07 advisory.

- A use-after-free vulnerability can occur when a raw pointer to a DOM element on a page is obtained using JavaScript and the element is then removed while still in use. This results in a potentially exploitable crash.

(CVE-2019-9790)

- The type inference system allows the compilation of functions that can cause type confusions between arbitrary objects when compiled through the IonMonkey just-in-time (JIT) compiler and when the constructor function is entered through on-stack replacement (OSR).

This allows for possible arbitrary reading and writing of objects during an exploitable crash. (CVE-2019-9791)

- The IonMonkey just-in-time (JIT) compiler can leak an internal JSOPTIMIZEDOUT magic value to the running script during a bailout. This magic value can then be used by JavaScript to achieve memory corruption, which results in a potentially exploitable crash.

(CVE-2019-9792)

- A mechanism was discovered that removes some bounds checking for string, array, or typed array accesses if Spectre mitigations have been disabled. This vulnerability could allow an attacker to create an arbitrary value in compiled JavaScript, for which the range analysis will infer a fully controlled, incorrect range in circumstances where users have explicitly disabled Spectre mitigations. Note: Spectre mitigations are currently enabled for all users by default settings. (CVE-2019-9793)

- A vulnerability was discovered where specific command line arguments are not properly discarded during Firefox invocation as a shell handler for URLs. This could be used to retrieve and execute files whose location is supplied through these command line arguments if Firefox is configured as the default URI handler for a given URI scheme in third party applications and these applications insufficiently sanitize URL data. Note: This issue only affects Windows operating systems.

Other operating systems are unaffected. (CVE-2019-9794)

- A vulnerability where type-confusion in the IonMonkey just-in-time (JIT) compiler could potentially be used by malicious JavaScript to trigger a potentially exploitable crash. (CVE-2019-9795)

- A use-after-free vulnerability can occur when the SMIL animation controller incorrectly registers with the refresh driver twice when only a single registration is expected. When a registration is later freed with the removal of the animation controller element, the refresh driver incorrectly leaves a dangling pointer to the driver's observer array. (CVE-2019-9796)

- Cross-origin images can be read in violation of the same-origin policy by exporting an image after using createImageBitmap to read the image and then rendering the resulting bitmap image within a canvas element. (CVE-2019-9797)

- On Android systems, Firefox can load a library from APITRACELIB, which is writable by all users and applications. This could allow malicious third party applications to execute a man-in-the-middle attack if a malicious code was written to that location and loaded.

Note: This issue only affects Android. Other operating systems are unaffected. (CVE-2019-9798)

- Insufficient bounds checking of data during inter- process communication might allow a compromised content process to be able to read memory from the parent process under certain conditions. (CVE-2019-9799)

- Firefox will accept any registered Program ID as an external protocol handler and offer to launch this local application when given a matching URL on Windows operating systems. This should only happen if the program has specifically registered itself as a URL Handler in the Windows registry. Note: This issue only affects Windows operating systems. Other operating systems are unaffected. (CVE-2019-9801)

- If a Sandbox content process is compromised, it can initiate an FTP download which will then use a child process to render the downloaded data. The downloaded data can then be passed to the Chrome process with an arbitrary file length supplied by an attacker, bypassing sandbox protections and allow for a potential memory read of adjacent data from the privileged Chrome process, which may include sensitive data.

(CVE-2019-9802)

- The Upgrade-Insecure-Requests (UIR) specification states that if UIR is enabled through Content Security Policy (CSP), navigation to a same-origin URL must be upgraded to HTTPS. Firefox will incorrectly navigate to an HTTP URL rather than perform the security upgrade requested by the CSP in some circumstances, allowing for potential man-in-the-middle attacks on the linked resources.

(CVE-2019-9803)

- In Firefox Developer Tools it is possible that pasting the result of the 'Copy as cURL' command into a command shell on macOS will cause the execution of unintended additional bash script commands if the URL was maliciously crafted. This is the result of an issue with the native version of Bash on macOS. Note: This issue only affects macOS. Other operating systems are unaffected. (CVE-2019-9804)

- A latent vulnerability exists in the Prio library where data may be read from uninitialized memory for some functions, leading to potential memory corruption.

(CVE-2019-9805)

- A vulnerability exists during authorization prompting for FTP transaction where successive modal prompts are displayed and cannot be immediately dismissed. This allows for a denial of service (DOS) attack.

(CVE-2019-9806)

- When arbitrary text is sent over an FTP connection and a page reload is initiated, it is possible to create a modal alert message with this text as the content. This could potentially be used for social engineering attacks. (CVE-2019-9807)

- If the source for resources on a page is through an FTP connection, it is possible to trigger a series of modal alert messages for these resources through invalid credentials or locations. These messages cannot be immediately dismissed, allowing for a denial of service (DOS) attack. (CVE-2019-9809)

- If WebRTC permission is requested from documents with data: or blob: URLs, the permission notifications do not properly display the originating domain. The notification states Unknown origin as the requestee, leading to user confusion about which site is asking for this permission. (CVE-2019-9808)

- Mozilla developers and community members Dragana Damjanovic, Emilio Cobos lvarez, Henri Sivonen, Narcis Beleuzu, Julian Seward, Marcia Knous, Gary Kwong, Tyson Smith, Yaron Tausky, Ronald Crane, and Andr Bargull reported memory safety bugs present in Firefox 65. 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-2019-9789)

- Mozilla developers and community members Bob Clary, Chun-Min Chang, Aral Yaman, Andreea Pavel, Jonathan Kew, Gary Kwong, Alex Gaynor, Masayuki Nakano, and Anne van Kesteren reported memory safety bugs present in Firefox 65 and Firefox ESR 60.5. 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-2019-9788)

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/mfsa2019-07/

Solution

Upgrade to Mozilla Firefox version 66.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2019-9788
CVE	CVE-2019-9789
CVE	CVE-2019-9790
CVE	CVE-2019-9791
CVE	CVE-2019-9792
CVE	CVE-2019-9793
CVE	CVE-2019-9794
CVE	CVE-2019-9795
CVE	CVE-2019-9796
CVE	CVE-2019-9797

CVE	CVE-2019-9798
CVE	CVE-2019-9799
CVE	CVE-2019-9801
CVE	CVE-2019-9802
CVE	CVE-2019-9803
CVE	CVE-2019-9804
CVE	CVE-2019-9805
CVE	CVE-2019-9806
CVE	CVE-2019-9807
CVE	CVE-2019-9808
CVE	CVE-2019-9809
XREF	MFSA:2019-07

Plugin Information

Published: 2019/03/19, Modified: 2019/05/24

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 66.0
```

125361 - Mozilla Firefox < 67.0

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 67.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2019-13 advisory.

- If hyperthreading is not disabled, a timing attack vulnerability exists, similar to previous Spectre attacks. Apple has shipped macOS 10.14.5 with an option to disable hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker threads. Note: users need to update to macOS 10.14.5 in order to take advantage of this change.

(CVE-2019-9815)

- A possible vulnerability exists where type confusion can occur when manipulating JavaScript objects in object groups, allowing for the bypassing of security checks within these groups. Note: this vulnerability has only been demonstrated with UnboxedObjects, which are disabled by default on all supported releases.

(CVE-2019-9816)

- Images from a different domain can be read using a canvas object in some circumstances. This could be used to steal image data from a different site in violation of same-origin policy. (CVE-2019-9817)

- A race condition is present in the crash generation server used to generate data for the crash reporter.

This issue can lead to a use-after-free in the main process, resulting in a potentially exploitable crash and a sandbox escape. Note: this vulnerability only affects Windows. Other operating systems are unaffected.

(CVE-2019-9818)

- A vulnerability where a JavaScript compartment mismatch can occur while working with the fetch API, resulting in a potentially exploitable crash.

(CVE-2019-9819)

- A use-after-free vulnerability can occur in the chrome event handler when it is freed while still in use. This results in a potentially exploitable crash.

(CVE-2019-9820)

- A use-after-free vulnerability can occur in AssertWorkerThread due to a race condition with shared workers. This results in a potentially exploitable crash. (CVE-2019-9821)

- A use-after-free vulnerability can occur when working with XMLHttpRequest (XHR) in an event loop, causing the XHR main thread to be called after it has been freed. This results in a potentially exploitable crash. (CVE-2019-11691)

- A use-after-free vulnerability can occur when listeners are removed from the event listener manager while still in use, resulting in a potentially exploitable crash.

(CVE-2019-11692)

- The bufferdata function in WebGL is vulnerable to a buffer overflow with specific graphics drivers on Linux. This could result in malicious content freezing a tab or triggering a potentially exploitable crash. Note: this issue only occurs on Linux. Other operating systems are unaffected. (CVE-2019-11693)

- A use-after-free vulnerability was discovered in the pngimagefree function in the libpng library. This could lead to denial of service or a potentially exploitable crash when a malformed image is processed. (CVE-2019-7317)

- A vulnerability exists in the Windows sandbox where an uninitialized value in memory can be leaked to a renderer from a broker when making a call to access an otherwise unavailable file. This results in the potential leaking of information stored at that memory location. Note: this issue only occurs on Windows.

Other operating systems are unaffected. (CVE-2019-11694)

- A custom cursor defined by scripting on a site can position itself over the addressbar to spoof the actual cursor when it should not be allowed outside of the primary web content area. This could be used by a malicious site to trick users into clicking on permission prompts, doorhanger notifications, or other buttons inadvertently if the location is spoofed over the user interface. (CVE-2019-11695)

- Files with the .JNLP extension used for Java web start applications are not treated as executable content for download prompts even though they can be executed if Java is installed on the local system. This could allow users to mistakenly launch an executable binary locally. (CVE-2019-11696)

- If the ALT and a keys are pressed when users receive an extension installation prompt, the extension will be installed without the install prompt delay that keeps the prompt visible in order for users to accept or decline the installation. A malicious web page could use this with spoofing on the page to trick users into installing a malicious extension.

(CVE-2019-11697)

- If a crafted hyperlink is dragged and dropped to the bookmark bar or sidebar and the resulting bookmark is subsequently dragged and dropped into the web content area, an arbitrary query of a user's browser history can be run and transmitted to the content page via drop event data. This allows for the theft of browser history by a malicious site. (CVE-2019-11698)

- A hyperlink using the res: protocol can be used to open local files at a known location in Internet Explorer if a user approves execution when prompted.

Note: this issue only occurs on Windows. Other operating systems are unaffected. (CVE-2019-11700)

- A malicious page can briefly cause the wrong name to be highlighted as the domain name in the addressbar during page navigations. This could result in user confusion of which site is currently loaded for spoofing attacks.

(CVE-2019-11699)

- The default webcal: protocol handler will load a web site vulnerable to cross-site scripting (XSS) attacks. This default was left in place as a legacy feature and has now been removed. Note: this issue only affects users with an account on the vulnerable service. Other users are unaffected. (CVE-2019-11701)

- Mozilla developers and community members Christian Holler, Andrei Ciure, Julien Cristau, Jan de Mooij, Jan Varga, Marcia Knous, Andr Bargull, and Philipp reported memory safety bugs present in Firefox 66. 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-2019-9814)

- Mozilla developers and community members Olli Pettay, Bogdan Tara, Jan de Mooij, Jason Kratzer, Jan Varga, Gary Kwong, Tim Guan-tin Chien, Tyson Smith, Ronald Crane, and Ted Campbell reported memory safety bugs present in Firefox 66 and Firefox ESR 60.6. 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-2019-9800)

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/mfsa2019-13/

Solution

Upgrade to Mozilla Firefox version 67.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

BID	108098
BID	108418
BID	108421
CVE	CVE-2019-7317
CVE	CVE-2019-9800
CVE	CVE-2019-9814
CVE	CVE-2019-9815
CVE	CVE-2019-9816
CVE	CVE-2019-9817
CVE	CVE-2019-9818
CVE	CVE-2019-9819
CVE	CVE-2019-9820
CVE	CVE-2019-9821
CVE	CVE-2019-11691
CVE	CVE-2019-11692
CVE	CVE-2019-11693
CVE	CVE-2019-11694

CVE	CVE-2019-11695
CVE	CVE-2019-11696
CVE	CVE-2019-11697
CVE	CVE-2019-11698
CVE	CVE-2019-11699
CVE	CVE-2019-11700
CVE	CVE-2019-11701
XREF	MFSA:2019-13

Plugin Information

Published: 2019/05/23, Modified: 2019/10/30

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 67.0
```

126072 - Mozilla Firefox < 67.0.4

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 67.0.4. It is, therefore, affected by a vulnerability as referenced in the mfsa2019-19 advisory.

- Insufficient vetting of parameters passed with the Prompt:Open IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities this could result in executing arbitrary code on the user's computer. (CVE-2019-11708)

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/mfsa2019-19/

Solution

Upgrade to Mozilla Firefox version 67.0.4 or later.

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 v3.0 Temporal Score

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

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-2019-11708
XREF	MFSA:2019-19
XREF	CISA-KNOWN-EXPLOITED:2022/06/13

Plugin Information

Published: 2019/06/20, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 67.0.4
```

126622 - Mozilla Firefox < 68.0

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 68.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2019-21 advisory.

- As part of his winning Pwn2Own entry, Niklas Baumstark demonstrated a sandbox escape by installing a malicious language pack and then opening a browser feature that used the compromised translation. (CVE-2019-9811)

- When an inner window is reused, it does not consider the use of document.domain for cross-origin protections. If pages on different subdomains ever cooperatively use document.domain, then either page can abuse this to inject script into arbitrary pages on the other subdomain, even those that did not use document.domain to relax their origin security. (CVE-2019-11711)

- POST requests made by NPAPI plugins, such as Flash, that receive a status 308 redirect response can bypass CORS requirements. This can allow an attacker to perform Cross-Site Request Forgery (CSRF) attacks.

(CVE-2019-11712)

- A use-after-free vulnerability can occur in HTTP/2 when a cached HTTP/2 stream is closed while still in use, resulting in a potentially exploitable crash.

(CVE-2019-11713)

- Necko can access a child on the wrong thread during UDP connections, resulting in a potentially exploitable crash in some instances. (CVE-2019-11714)

- Empty or malformed p256-ECDH public keys may trigger a segmentation fault due values being improperly sanitized before being copied into memory and used.

(CVE-2019-11729)

- Due to an error while parsing page content, it is possible for properly sanitized user input to be misinterpreted and lead to XSS hazards on web sites in certain circumstances. (CVE-2019-11715)

- Until explicitly accessed by script, window.globalThis is not enumerable and, as a result, is not visible to code such as Object.getOwnPropertyNames(window). Sites that deploy a sandboxing that depends on enumerating and freezing access to the window object may miss this, allowing their sandboxes to be bypassed.

(CVE-2019-11716)

- A vulnerability exists where the caret (^) character is improperly escaped constructing some URIs due to it being used as a separator, allowing for possible spoofing of origin attributes. (CVE-2019-11717)

- Activity Stream can display content from sent from the Snippet Service website. This content is written to innerHTML on the Activity Stream page without sanitization, allowing for a potential access to other information available to the Activity Stream, such as browsing history, if the Snipper Service were compromised. (CVE-2019-11718)

- When importing a curve25519 private key in PKCS#8format with leading 0x00 bytes, it is possible to trigger an out-of-bounds read in the Network Security Services (NSS) library. This could lead to information disclosure. (CVE-2019-11719)

- Some unicode characters are incorrectly treated as whitespace during the parsing of web content instead of triggering parsing errors. This allows malicious code to then be processed, evading cross-site scripting (XSS) filtering. (CVE-2019-11720)

- The unicode latin 'kra' character can be used to spoof a standard 'k' character in the addressbar. This allows for domain spoofing attacks as do not display as punycode text, allowing for user confusion.

(CVE-2019-11721)

- A vulnerability exists where if a user opens a locally saved HTML file, this file can use file:

URIs to access other files in the same directory or sub- directories if the names are known or guessed. The Fetch API can then be used to read the contents of any files stored in these directories and they may uploaded to a server. Luigi Gubello demonstrated that in combination with a popular Android messaging app, if a malicious HTML attachment is sent to a user and they opened that attachment in Firefox, due to that app's predictable pattern for locally-saved file names, it is possible to read attachments the victim received from other correspondents. (CVE-2019-11730)

- A vulnerability exists during the installation of add- ons where the initial fetch ignored the origin attributes of the browsing context. This could leak cookies in private browsing mode or across different containers for people who use the Firefox Multi- Account Containers Web Extension. (CVE-2019-11723)

- Application permissions give additional remote troubleshooting permission to the site input.mozilla.org, which has been retired and now redirects to another site. This additional permission is unnecessary and is a potential vector for malicious attacks. (CVE-2019-11724)

- When a user navigates to site marked as unsafe by the Safebrowsing API, warning messages are displayed and navigation is interrupted but resources from the same site loaded through websockets are not blocked, leading to the loading of unsafe resources and bypassing safebrowsing protections. (CVE-2019-11725)

- A vulnerability exists where it possible to force Network Security Services (NSS) to sign CertificateVerify with PKCS#1 v1.5 signatures when those are the only ones advertised by server in CertificateRequest in TLS 1.3.

PKCS#1 v1.5 signatures should not be used for TLS 1.3 messages. (CVE-2019-11727)

- The HTTP Alternative Services header, Alt- Svc, can be used by a malicious site to scan all TCP ports of any host that the accessible to a user when web content is loaded. (CVE-2019-11728)

- Mozilla developers and community members Andr Bargull, Christian Holler, Natalia Csoregi, Raul Gurzau, Daniel Varga, Jon Coppeard, Marcia Knous, Gary Kwong, Randell Jesup, David Bolter, Jeff Gilbert, and Deian Stefan reported memory safety bugs present in Firefox 67. 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-2019-11710)

- Mozilla developers and community members Andreea Pavel, Christian Holler, Honza Bambas, Jason Kratzer, and Jeff Gilbert reported memory safety bugs present in Firefox 67 and Firefox ESR 60.7. 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-2019-11709)

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/mfsa2019-21/

Solution

Upgrade to Mozilla Firefox version 68.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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	109081
BID	109083
BID	109084
BID	109085
BID	109086
BID	109087
CVE	CVE-2019-9811
CVE	CVE-2019-11709
CVE	CVE-2019-11710
CVE	CVE-2019-11711
CVE	CVE-2019-11712
CVE	CVE-2019-11713
CVE	CVE-2019-11714
CVE	CVE-2019-11715
CVE	CVE-2019-11716
CVE	CVE-2019-11717
CVE	CVE-2019-11718

CVE	CVE-2019-11719
CVE	CVE-2019-11720
CVE	CVE-2019-11721
CVE	CVE-2019-11723
CVE	CVE-2019-11724
CVE	CVE-2019-11725
CVE	CVE-2019-11727
CVE	CVE-2019-11728
CVE	CVE-2019-11729
CVE	CVE-2019-11730
XREF	MFSA:2019-21

Plugin Information

Published: 2019/07/11, Modified: 2022/05/19

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 68.0
```

128061 - Mozilla Firefox < 68.0.2

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 68.0.2. It is, therefore, affected by a vulnerability as referenced in the mfsa2019-24 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/mfsa2019-24/

Solution

Upgrade to Mozilla Firefox version 68.0.2 or later.

Risk Factor

Medium

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2019-11733
XREF	MFSA:2019-24

Plugin Information

Published: 2019/08/22, Modified: 2020/04/27

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 68.0.2
```

128525 - Mozilla Firefox < 69.0

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 69.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2019-25 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/mfsa2019-25/

Solution

Upgrade to Mozilla Firefox version 69.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2019-5849
CVE	CVE-2019-9812
CVE	CVE-2019-11734
CVE	CVE-2019-11735

CVE	CVE-2019-11736
CVE	CVE-2019-11737
CVE	CVE-2019-11738
CVE	CVE-2019-11740
CVE	CVE-2019-11741
CVE	CVE-2019-11742
CVE	CVE-2019-11743
CVE	CVE-2019-11744
CVE	CVE-2019-11746
CVE	CVE-2019-11747
CVE	CVE-2019-11748
CVE	CVE-2019-11749
CVE	CVE-2019-11750
CVE	CVE-2019-11751
CVE	CVE-2019-11752
CVE	CVE-2019-11753
XREF	MFSA:2019-25

Plugin Information

Published: 2019/09/05, Modified: 2022/05/19

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 69.0
```

134405 - Mozilla Firefox < 74.0 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 74.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-08 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/mfsa2020-08/

Solution

Upgrade to Mozilla Firefox version 74.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2020-6808
CVE	CVE-2020-6809

CVE	CVE-2020-6810
CVE	CVE-2020-6811
CVE	CVE-2020-6812
CVE	CVE-2020-6813
CVE	CVE-2020-6814
CVE	CVE-2020-6815
XREF	MFSA:2020-08

Plugin Information

Published: 2020/03/11, Modified: 2020/05/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 74.0
```

135276 - Mozilla Firefox < 75.0 (mfsa2020-12)

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 75.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-12 advisory.

- Mozilla developers and community members Tyson Smith and Christian Holler reported memory safety bugs present in Firefox 74 and Firefox ESR 68.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2020-6825)

- When reading from areas partially or fully outside the source resource with WebGL's copyTexSubImage method, the specification requires the returned values be zero. Previously, this memory was uninitialized, leading to potentially sensitive data disclosure. (CVE-2020-6821)

- On 32-bit builds, an out of bounds write could have occurred when processing an image larger than 4 GB in GMPDecodeData. It is possible that with enough effort this could have been exploited to run arbitrary code. (CVE-2020-6822)

- A malicious extension could have called browser.identity.launchWebAuthFlow, controlling the redirect_uri, and through the Promise returned, obtain the Auth code and gain access to the user's account at the service provider. (CVE-2020-6823)

- Initially, a user opens a Private Browsing Window and generates a password for a site, then closes the Private Browsing Window but leaves Firefox open. Subsequently, if the user had opened a new Private Browsing Window, revisited the same site, and generated a new password - the generated passwords would have been identical, rather than independent. (CVE-2020-6824)

- Mozilla developers Tyson Smith, Bob Clary, and Alexandru Michis reported memory safety bugs present in Firefox 74. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2020-6826)

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/mfsa2020-12/

Solution

Upgrade to Mozilla Firefox version 75.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2020-6821
CVE	CVE-2020-6822
CVE	CVE-2020-6823
CVE	CVE-2020-6824
CVE	CVE-2020-6825
CVE	CVE-2020-6826
XREF	MFSA:2020-12

Plugin Information

Published: 2020/04/07, Modified: 2020/04/09

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 75.0
```

136404 - Mozilla Firefox < 76.0

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 76.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-16 advisory.

- A race condition when running shutdown code for Web Worker led to a use-after-free vulnerability. This resulted in a potentially exploitable crash.

(CVE-2020-12387)

- The Firefox content processes did not sufficiently lockdown access control which could result in a sandbox escape.Note: this issue only affects Firefox on Windows operating systems. (CVE-2020-12388, CVE-2020-12389)

- A buffer overflow could occur when parsing and validating SCTP chunks in WebRTC. This could have led to memory corruption and a potentially exploitable crash.

(CVE-2020-6831)

- Incorrect origin serialization of URLs with IPv6 addresses could lead to incorrect security checks (CVE-2020-12390)

- Documents formed using data: URLs in an object element failed to inherit the CSP of the creating context. This allowed the execution of scripts that should have been blocked, albeit with a unique opaque origin. (CVE-2020-12391)

- The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP POST data of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in the disclosure of local files. (CVE-2020-12392)

- The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in command injection and arbitrary command execution.Note: this issue only affects Firefox on Windows operating systems.

(CVE-2020-12393)

- A logic flaw in our location bar implementation could have allowed a local attacker to spoof the current location by selecting a different origin and removing focus from the input element. (CVE-2020-12394)

- Mozilla developers and community members Alexandru Michis, Jason Kratzer, philipp, Ted Campbell, Bas Schouten, Andr Bargull, and Karl Tomlinson reported memory safety bugs present in Firefox 75 and Firefox ESR 68.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2020-12395)

- Mozilla developers and community members Frederik Braun, Andrew McCreight, C.M.Chang, and Dan Minor reported memory safety bugs present in Firefox 75. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2020-12396)

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/mfsa2020-16/

Solution

Upgrade to Mozilla Firefox version 76.0 or later.

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 v3.0 Temporal Score

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

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

II

References

CVE	CVE-2020-6831
CVE	CVE-2020-12387
CVE	CVE-2020-12388
CVE	CVE-2020-12389
CVE	CVE-2020-12390
CVE	CVE-2020-12391
CVE	CVE-2020-12392
CVE	CVE-2020-12393
CVE	CVE-2020-12394
CVE	CVE-2020-12395
CVE	CVE-2020-12396
XREF	MFSA:2020-16
XREF	IAVA:2020-A-0190-S

Plugin Information

Published: 2020/05/07, Modified: 2022/05/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 76.0
```

141571 - Mozilla Firefox < 82.0

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 82.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-45 advisory.

- Crossbeam is a set of tools for concurrent programming. In crossbeam-channel before version 0.4.4, the bounded channel incorrectly assumes that `Vec::from_iter` has allocated capacity that same as the number of iterator elements. `Vec::from_iter` does not actually guarantee that and may allocate extra memory. The destructor of the `bounded` channel reconstructs `Vec` from the raw pointer based on the incorrect assumes described above. This is unsound and causing deallocation with the incorrect capacity when `Vec::from_iter` has allocated different sizes with the number of iterator elements. This has been fixed in crossbeam-channel 0.4.4. (CVE-2020-15254)

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/mfsa2020-45/

Solution

Upgrade to Mozilla Firefox version 82.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2020-15254
CVE	CVE-2020-15680
CVE	CVE-2020-15681
CVE	CVE-2020-15682
CVE	CVE-2020-15683
CVE	CVE-2020-15684
CVE	CVE-2020-15969
XREF	MFSA:2020-45
XREF	IAVA:2020-A-0472-S

Plugin Information

Published: 2020/10/20, Modified: 2020/11/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 82.0
```

144282 - Mozilla Firefox < 84.0

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 84.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-54 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/mfsa2020-54/

Solution

Upgrade to Mozilla Firefox version 84.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2020-16042
CVE	CVE-2020-26971

CVE	CVE-2020-26972
CVE	CVE-2020-26973
CVE	CVE-2020-26974
CVE	CVE-2020-26975
CVE	CVE-2020-26976
CVE	CVE-2020-26977
CVE	CVE-2020-26978
CVE	CVE-2020-26979
CVE	CVE-2020-35111
CVE	CVE-2020-35112
CVE	CVE-2020-35113
CVE	CVE-2020-35114
XREF	MFSA:2020-54
XREF	IAVA:2020-A-0575-S
XREF	IAVA:2021-A-0051-S

Plugin Information

Published: 2020/12/15, Modified: 2021/02/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 84.0
```

151571 - Mozilla Firefox < 90.0

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 90.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-28 advisory.

- A malicious webpage could have triggered a use-after-free, memory corruption, and a potentially exploitable crash. This bug only affected Firefox when accessibility was enabled. (CVE-2021-29970)

- If a user had granted a permission to a webpage and saved that grant, any webpage running on the same host

- irrespective of scheme or port - would be granted that permission.This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29971)

- An out of bounds write in ANGLE could have allowed an attacker to corrupt memory leading to a potentially exploitable crash. (CVE-2021-30547)

- A user-after-free vulnerability was found via testing, and traced to an out-of-date Cairo library.

Updating the library resolved the issue, and may have remediated other, unknown security vulnerabilities as well. (CVE-2021-29972)

- Password autofill was enabled without user interaction on insecure websites on Firefox for Android. This was corrected to require user interaction with the page before a user's password would be entered by the browser's autofill functionality.This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29973)

- When network partitioning was enabled, e.g. as a result of Enhanced Tracking Protection settings, a TLS error page would allow the user to override an error on a domain which had specified HTTP Strict Transport Security (which implies that the error should not be override-able.) This issue did not affect the network connections, and they were correctly upgraded to HTTPS automatically. (CVE-2021-29974)

- Through a series of DOM manipulations, a message, over which the attacker had control of the text but not HTML or formatting, could be overlaid on top of another domain (with the new domain correctly shown in the address bar) resulting in possible user confusion. (CVE-2021-29975)

- Mozilla developers Emil Ghitta, Tyson Smith, Valentin Gosu, Olli Pettay, and Randell Jesup reported memory safety bugs present in Firefox 89 and Firefox ESR 78.11. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29976)

- Mozilla developers Andrew McCreight, Tyson Smith, Christian Holler, and Gabriele Svelto reported memory safety bugs present in Firefox 89. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29977)

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/mfsa2021-28/

Solution

Upgrade to Mozilla Firefox version 90.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2021-29970
CVE	CVE-2021-29971
CVE	CVE-2021-29972
CVE	CVE-2021-29973
CVE	CVE-2021-29974
CVE	CVE-2021-29975
CVE	CVE-2021-29976
CVE	CVE-2021-29977
CVE	CVE-2021-30547
XREF	IAVA:2021-A-0293-S
XREF	IAVA:2021-A-0309-S

Plugin Information

Published: 2021/07/13, Modified: 2021/08/12

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
  Fixed version     : 90.0
```

153881 - Mozilla Firefox < 93.0

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 93.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-43 advisory.

- During operations on MessageTasks, a task may have been removed while it was still scheduled, resulting in memory corruption and a potentially exploitable crash. (CVE-2021-38496)

- Through use of reportValidity() and window.open(), a plain-text validation message could have been overlaid on another origin, leading to possible user confusion and spoofing attacks. (CVE-2021-38497)

- During process shutdown, a document could have caused a use-after-free of a languages service object, leading to memory corruption and a potentially exploitable crash. (CVE-2021-38498)

- In the crossbeam crate, one or more tasks in the worker queue could have been be popped twice instead of other tasks that are forgotten and never popped. If tasks are allocated on the heap, this could have caused a double free and a memory leak. (CVE-2021-32810)

- Mozilla developers and community members Andreas Pehrson and Christian Holler reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.

(CVE-2021-38500)

- Mozilla developers and community members Kevin Brosnan, Mihai Alexandru Michis, and Christian Holler reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-38501)

- Mozilla developers and community members Julien Cristau, Christian Holler reported memory safety bugs present in Firefox 92. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-38499)

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/mfsa2021-43/

Solution

Upgrade to Mozilla Firefox version 93.0 or later.

Risk Factor

Medium

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)

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-2021-32810
CVE	CVE-2021-38496
CVE	CVE-2021-38497
CVE	CVE-2021-38498
CVE	CVE-2021-38499
CVE	CVE-2021-38500
CVE	CVE-2021-38501
CVE	CVE-2021-43535
XREF	IAVA:2021-A-0461-S
XREF	IAVA:2021-A-0450-S

Plugin Information

Published: 2021/10/05, Modified: 2022/05/09

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 93.0
```

154819 - Mozilla Firefox < 94.0

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 94.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-48 advisory.

- The iframe sandbox rules were not correctly applied to XSLT stylesheets, allowing an iframe to bypass restrictions such as executing scripts or navigating the top-level frame. (CVE-2021-38503)

- When interacting with an HTML input element's file picker dialog with <code>webkitdirectory</code> set, a use-after-free could have resulted, leading to memory corruption and a potentially exploitable crash.

(CVE-2021-38504)

- Microsoft introduced a new feature in Windows 10 known as Cloud Clipboard which, if enabled, will record data copied to the clipboard to the cloud, and make it available on other computers in certain scenarios.

Applications that wish to prevent copied data from being recorded in Cloud History must use specific clipboard formats; and Firefox before versions 94 and ESR 91.3 did not implement them. This could have caused sensitive data to be recorded to a user's Microsoft account. This bug only affects Firefox for Windows 10+ with Cloud Clipboard enabled. Other operating systems are unaffected. (CVE-2021-38505)

- Through a series of navigations, Firefox could have entered fullscreen mode without notification or warning to the user. This could lead to spoofing attacks on the browser UI including phishing.

(CVE-2021-38506)

- The Opportunistic Encryption feature of HTTP2 (RFC 8164) allows a connection to be transparently upgraded to TLS while retaining the visual properties of an HTTP connection, including being same-origin with unencrypted connections on port 80. However, if a second encrypted port on the same IP address (e.g. port 8443) did not opt-in to opportunistic encryption; a network attacker could forward a connection from the browser to port 443 to port 8443, causing the browser to treat the content of port 8443 as same-origin with HTTP. This was resolved by disabling the Opportunistic Encryption feature, which had low usage.

(CVE-2021-38507)

- By displaying a form validity message in the correct location at the same time as a permission prompt (such as for geolocation), the validity message could have obscured the prompt, resulting in the user potentially being tricked into granting the permission. (CVE-2021-38508)

- Due to an unusual sequence of attacker-controlled events, a Javascript <code>alert()</code> dialog with arbitrary (although unstyled) contents could be displayed over top an uncontrolled webpage of the attacker's choosing. (CVE-2021-38509)

- The executable file warning was not presented when downloading .inetloc files, which can run commands on a user's computer. Note: This issue only affected Mac OS operating systems. Other operating systems are unaffected. (CVE-2021-38510)

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/mfsa2021-48/

Solution

Upgrade to Mozilla Firefox version 94.0 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

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

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-2021-38503
CVE	CVE-2021-38504
CVE	CVE-2021-38505
CVE	CVE-2021-38506
CVE	CVE-2021-38507
CVE	CVE-2021-38508
CVE	CVE-2021-38509
CVE	CVE-2021-38510
XREF	IAVA:2021-A-0527-S

Plugin Information

Published: 2021/11/02, Modified: 2022/03/17

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
  Fixed version     : 94.0
```

156606 - Mozilla Firefox < 96.0

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 96.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-01 advisory.

- A race condition could have allowed bypassing the fullscreen notification which could have lead to a fullscreen window spoof being unnoticed. This bug only affects Firefox for Windows. Other operating systems are unaffected. (CVE-2022-22746)

- When navigating from inside an iframe while requesting fullscreen access, an attacker-controlled tab could have made the browser unable to leave fullscreen mode. (CVE-2022-22743)

- When inserting text while in edit mode, some characters might have lead to out-of-bounds memory access causing a potentially exploitable crash. (CVE-2022-22742)

- When resizing a popup while requesting fullscreen access, the popup would have become unable to leave fullscreen mode. (CVE-2022-22741)

- Certain network request objects were freed too early when releasing a network request handle. This could have lead to a use-after-free causing a potentially exploitable crash. (CVE-2022-22740)

- Applying a CSS filter effect could have accessed out of bounds memory. This could have lead to a heap-buffer-overflow causing a potentially exploitable crash. (CVE-2022-22738)

- Constructing audio sinks could have lead to a race condition when playing audio files and closing windows.

This could have lead to a use-after-free causing a potentially exploitable crash. (CVE-2022-22737)

- It was possible to construct specific XSLT markup that would be able to bypass an iframe sandbox.

(CVE-2021-4140)

- By generally accepting and passing resource handles across processes, a compromised content process might have confused higher privileged processes to interact with handles that the unprivileged process should not have access to. This bug only affects Firefox for Windows and MacOS. Other operating systems are unaffected. (CVE-2022-22750)

- When scanning QR codes, Firefox for Android would have allowed navigation to some URLs that do not point to web content. This bug only affects Firefox for Android. Other operating systems are unaffected.

(CVE-2022-22749)

- Malicious websites could have confused Firefox into showing the wrong origin when asking to launch a program and handling an external URL protocol. (CVE-2022-22748)

- Securitypolicyviolation events could have leaked cross-origin information for frame-ancestors violations (CVE-2022-22745)

- The constructed curl command from the Copy as curl feature in DevTools was not properly escaped for PowerShell. This could have lead to command injection if pasted into a Powershell prompt. This bug only affects Firefox for Windows. Other operating systems are unaffected. (CVE-2022-22744)

- After accepting an untrusted certificate, handling an empty pkcs7 sequence as part of the certificate data could have lead to a crash. This crash is believed to be unexploitable. (CVE-2022-22747)

- If Firefox was installed to a world-writable directory, a local privilege escalation could occur when Firefox searched the current directory for system libraries. However the install directory is not world- writable by default. This bug only affects Firefox for Windows in a non-default installation. Other operating systems are unaffected. (CVE-2022-22736)

- Malicious websites could have tricked users into accepting launching a program to handle an external URL protocol. (CVE-2022-22739)

- Mozilla developers Calixte Denizet, Kershaw Chang, Christian Holler, Jason Kratzer, Gabriele Svelto, Tyson Smith, Simon Giesecke, and Steve Fink reported memory safety bugs present in Firefox 95 and Firefox ESR 91.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-22751)

- Mozilla developers Christian Holler and Jason Kratzer reported memory safety bugs present in Firefox 95.

Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-22752)

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/mfsa2022-01/

Solution

Upgrade to Mozilla Firefox version 96.0 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2021-4140
CVE	CVE-2022-22736
CVE	CVE-2022-22737
CVE	CVE-2022-22738
CVE	CVE-2022-22739
CVE	CVE-2022-22740
CVE	CVE-2022-22741
CVE	CVE-2022-22742
CVE	CVE-2022-22743
CVE	CVE-2022-22744
CVE	CVE-2022-22745
CVE	CVE-2022-22746
CVE	CVE-2022-22747
CVE	CVE-2022-22748
CVE	CVE-2022-22749
CVE	CVE-2022-22750
CVE	CVE-2022-22751
CVE	CVE-2022-22752
CVE	CVE-2022-22763
XREF	IAVA:2022-A-0017-S
XREF	IAVA:2022-A-0079-S

Plugin Information

Published: 2022/01/11, Modified: 2022/05/06

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 96.0
```

157443 - Mozilla Firefox < 97.0

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 97.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-04 advisory.

- A Time-of-Check Time-of-Use bug existed in the Maintenance (Updater) Service that could be abused to grant Users write access to an arbitrary directory. This could have been used to escalate to SYSTEM access. This bug only affects Firefox on Windows. Other operating systems are unaffected. (CVE-2022-22753)

- If a user installed an extension of a particular type, the extension could have auto-updated itself and while doing so, bypass the prompt which grants the new version the new requested permissions.

(CVE-2022-22754)

- By using XSL Transforms, a malicious webserver could have served a user an XSL document that would continue to execute JavaScript (within the bounds of the same-origin policy) even after the tab was closed. (CVE-2022-22755)

- If a user was convinced to drag and drop an image to their desktop or other folder, the resulting object could have been changed into an executable script which would have run arbitrary code after the user clicked on it. (CVE-2022-22756)

- Remote Agent, used in WebDriver, did not validate the Host or Origin headers. This could have allowed websites to connect back locally to the user's browser to control it. This bug only affected Firefox when WebDriver was enabled, which is not the default configuration. (CVE-2022-22757)

- When clicking on a tel: link, USSD codes, specified after a <code></code> character, would be included in the phone number. On certain phones, or on certain carriers, if the number was dialed this could perform actions on a user's account, similar to a cross-site request forgery attack. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2022-22758)

- If a document created a sandboxed iframe without <code>allow-scripts</code>, and subsequently appended an element to the iframe's document that e.g. had a JavaScript event handler - the event handler would have run despite the iframe's sandbox. (CVE-2022-22759)

- When importing resources using Web Workers, error messages would distinguish the difference between <code>application/javascript</code> responses and non-script responses. This could have been abused to learn information cross-origin. (CVE-2022-22760)

- Web-accessible extension pages (pages with a moz-extension:// scheme) were not correctly enforcing the frame-ancestors directive when it was used in the Web Extension's Content Security Policy.

(CVE-2022-22761)

- Under certain circumstances, a JavaScript alert (or prompt) could have been shown while another website was displayed underneath it. This could have been abused to trick the user. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2022-22762)

- Mozilla developers Paul Adenot and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 96 and Firefox ESR 91.5. Some of these bugs showed evidence of memory corruption and

we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-22764)

- Mozilla developers and community members Gabriele Svelto, Sebastian Hengst, Randell Jesup, Luan Herrera, Lars T Hansen, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 96. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-0511)

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/mfsa2022-04/

Solution

Upgrade to Mozilla Firefox version 97.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2022-0511
CVE	CVE-2022-22753
CVE	CVE-2022-22754
CVE	CVE-2022-22755
CVE	CVE-2022-22756

CVE	CVE-2022-22757
CVE	CVE-2022-22758
CVE	CVE-2022-22759
CVE	CVE-2022-22760
CVE	CVE-2022-22761
CVE	CVE-2022-22762
CVE	CVE-2022-22764
XREF	IAVA:2022-A-0079-S

Plugin Information

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

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 97.0
```

158654 - Mozilla Firefox < 97.0.2

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 97.0.2. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-09 advisory.

- Removing an XSLT parameter during processing could have lead to an exploitable use-after-free. We have had reports of attacks in the wild abusing this flaw. (CVE-2022-26485)

- An unexpected message in the WebGPU IPC framework could lead to a use-after-free and exploitable sandbox escape. We have had reports of attacks in the wild abusing this flaw. (CVE-2022-26486)

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/mfsa2022-09/

Solution

Upgrade to Mozilla Firefox version 97.0.2 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)

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)

STIG Severity

I

References

CVE	CVE-2022-26485
CVE	CVE-2022-26486
XREF	CISA-KNOWN-EXPLOITED:2022/03/21
XREF	IAVA:2022-A-0103-S

Plugin Information

Published: 2022/03/07, Modified: 2022/04/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 97.0.2
```

158694 - Mozilla Firefox < 98.0

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 98.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-10 advisory.

- When resizing a popup after requesting fullscreen access, the popup would not display the fullscreen notification. (CVE-2022-26383)

- If an attacker could control the contents of an iframe sandboxed with <code>allow-popups</code> but not <code>allow-scripts</code>, they were able to craft a link that, when clicked, would lead to JavaScript execution in violation of the sandbox. (CVE-2022-26384)

- When installing an add-on, Firefox verified the signature before prompting the user; but while the user was confirming the prompt, the underlying add-on file could have been modified and Firefox would not have noticed. (CVE-2022-26387)

- An attacker could have caused a use-after-free by forcing a text reflow in an SVG object leading to a potentially exploitable crash. (CVE-2022-26381)

- While the text displayed in Autofill tooltips cannot be directly read by JavaScript, the text was rendered using page fonts. Side-channel attacks on the text by using specially crafted fonts could have lead to this text being inferred by the webpage. (CVE-2022-26382)

- In unusual circumstances, an individual thread may outlive the thread's manager during shutdown. This could have led to a use-after-free causing a potentially exploitable crash. (CVE-2022-26385)

- Mozilla developers Kershaw Chang, Ryan VanderMeulen, and Randell Jesup reported memory safety bugs present in Firefox 97. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-0843)

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/mfsa2022-10/

Solution

Upgrade to Mozilla Firefox version 98.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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-2022-0843
CVE	CVE-2022-26381
CVE	CVE-2022-26382
CVE	CVE-2022-26383
CVE	CVE-2022-26384
CVE	CVE-2022-26385
CVE	CVE-2022-26387
XREF	IAVA:2022-A-0103-S

Plugin Information

Published: 2022/03/08, Modified: 2022/04/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 98.0
```

108756 - Mozilla Firefox ESR < 59.0.2 Denial of Service Vulnerability

Synopsis

A web browser installed on the remote Windows host is affected by a Denial of Service vulnerability.

Description

The version of Mozilla Firefox ESR installed on the remote Windows host is prior to 59.0.2. It is, therefore, affected by a use-after-free error that causes a denial of service vulnerability.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2018-10/

Solution

Upgrade to Mozilla Firefox ESR version 59.0.2 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)

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	103506
CVE	CVE-2018-5148
XREF	MFSA:2018-10

Plugin Information

Published: 2018/03/30, Modified: 2019/11/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 59.0.2
```

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: 2022/06/08

Plugin Output

tcp/445/cifs

```
Product           : Mozilla Firefox
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Latest version    : 103.0.0
EOL URL           : https://www.mozilla.org/en-US/security/known-vulnerabilities/firefox-3.6/
```

51121 - Firefox 3.6 < 3.6.13 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox 3.6 is earlier than 3.6.13. Such versions are potentially affected by multiple vulnerabilities :

- Multiple memory corruption issues could lead to arbitrary code execution. (MFSA 2010-74)

- On the Windows platform, when 'document.write()' is called with a very long string, a buffer overflow could be triggered. (MFSA 2010-75)

- A privilege escalation vulnerability exists with 'window.open' and the '<isindex>' element. (MFSA 2010-76)

- Arbitrary code execution is possible when using HTML tags inside a XUL tree. (MFSA 2010-77)

- Downloadable fonts could expose vulnerabilities in the underlying OS font code. (MFSA 2010-78)

- A Java security bypass vulnerability exists when LiveConnect is loaded via a 'data:' URL meta refresh. (MFSA 2010-79)

- A use-after-free error exists with nsDOMAttribute MutationObserver. (MFSA 2010-80)

- An integer overflow exists in NewIdArray. (MFSA 2010-81)

- It is possible to circumvent the fix for CVE-2010-0179.

(MFSA 2010-82)

- It is possible to spoof SSL in the location bar using the network error page. (MFSA 2010-83)

- A cross-site scripting hazard exists in multiple character encodings. (MFSA 2010-84)

See Also

http://www.nessus.org/u?de9e67fa

https://www.mozilla.org/en-US/security/advisories/mfsa2010-74/

https://www.mozilla.org/en-US/security/advisories/mfsa2010-75/

https://www.mozilla.org/en-US/security/advisories/mfsa2010-76/

https://www.mozilla.org/en-US/security/advisories/mfsa2010-77/

https://www.mozilla.org/en-US/security/advisories/mfsa2010-78/

https://www.mozilla.org/en-US/security/advisories/mfsa2010-79/

https://www.mozilla.org/en-US/security/advisories/mfsa2010-80/

https://www.mozilla.org/en-US/security/advisories/mfsa2010-81/

https://www.mozilla.org/en-US/security/advisories/mfsa2010-82/

https://www.mozilla.org/en-US/security/advisories/mfsa2010-83/

https://www.mozilla.org/en-US/security/advisories/mfsa2010-84/

http://www.nessus.org/u?4c81664e

Solution

Upgrade to Firefox 3.6.13 or later.

Risk Factor

High

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

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

References

BID	45314
BID	45324
BID	45326
BID	45345
BID	45346
BID	45347
BID	45348
BID	45351
BID	45352
BID	45353
BID	45354
BID	45355
CVE	CVE-2010-3766
CVE	CVE-2010-3767
CVE	CVE-2010-3768
CVE	CVE-2010-3769
CVE	CVE-2010-3770
CVE	CVE-2010-3771
CVE	CVE-2010-3772
CVE	CVE-2010-3773
CVE	CVE-2010-3774
CVE	CVE-2010-3775
CVE	CVE-2010-3776
CVE	CVE-2010-3777
XREF	Secunia:42517

Plugin Information

Published: 2010/12/10, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.13
```

52531 - Firefox 3.6 < 3.6.14 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox 3.6 is earlier than 3.6.14. Such versions are potentially affected by multiple vulnerabilities :

- Multiple memory corruption errors exist and may lead to arbitrary code execution. (MFSA 2011-01)

- An error exists in the processing of recursive calls to 'eval()' when the call is wrapped in a try/catch statement. This error causes dialog boxes to be displayed with no content and non-functioning buttons.

Closing the dialog results in default acceptance of the dialog. (MFSA 2011-02)

- A use-after-free error exists in a method used by 'JSON.stringify' and can allow arbitrary code execution. (MFSA 2011-03)

- A buffer overflow vulnerability exists in the JavaScript engine's internal memory mapping of non-local variables and may lead to code execution. (MFSA 2011-04)

- A buffer overflow vulnerability exists in the JavaScript engine's internal mapping of string values and may lead to code execution. (MFSA 2011-05)

- A use-after-free error exists such that a JavaScript 'Worker' can be used to keep a reference to an object which can be freed during garbage collection. This vulnerability may lead to arbitrary code execution.

(MFSA 2011-06)

- A buffer overflow error exists related to the creation very long strings and the insertion of those strings into an HTML document. This vulnerability may lead to arbitrary code execution. (MFSA 2011-07)

- An input validation error exists in the class, 'ParanoidFragmentSink', which allows inline JavaScript and 'javascript:' URLs in a chrome document. Note that no unsafe usage occurs in Mozilla products, however community generated extensions could.(MFSA 2011-08)

- A buffer overflow exists related to JPEG decoding and may lead to arbitrary code execution. (MFSA 2011-09)

- A cross-site request forgery (CSRF) vulnerability exists when an HTTP 307 redirect is received in response to a plugin's request. The request is forwarded to the new location without the plugin's knowledge and with custom headers intact, even across origins. (MFSA 2011-10)

See Also

https://seclists.org/bugtraq/2010/Apr/202

https://www.mozilla.org/en-US/security/advisories/mfsa2011-01/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-02/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-03/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-04/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-05/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-06/
https://www.mozilla.org/en-US/security/advisories/mfsa2011-07/
https://www.mozilla.org/en-US/security/advisories/mfsa2011-08/
https://www.mozilla.org/en-US/security/advisories/mfsa2011-09/
https://www.mozilla.org/en-US/security/advisories/mfsa2011-10/
http://www.nessus.org/u?2f087a83

Solution

Upgrade to Firefox 3.6.14 or later.

Risk Factor

High

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	46368
BID	46643
BID	46645
BID	46647
BID	46648
BID	46650
BID	46651
BID	46652
BID	46660
BID	46661
BID	46663
CVE	CVE-2010-1585
CVE	CVE-2011-0051
CVE	CVE-2011-0053
CVE	CVE-2011-0054
CVE	CVE-2011-0055
CVE	CVE-2011-0056
CVE	CVE-2011-0057
CVE	CVE-2011-0058
CVE	CVE-2011-0059

CVE	CVE-2011-0061
CVE	CVE-2011-0062
XREF	Secunia:43550

Plugin Information

Published: 2011/03/03, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.14
```

53594 - Firefox 3.6 < 3.6.17 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox 3.6 is earlier than 3.6.17. Such versions are potentially affected by the following security issues :

- Multiple use-after-free errors exist in the handling of the object attributes 'mChannel', 'mObserverList' and 'nsTreeRange'. (CVE-2011-0065, CVE-2011-0066, CVE-2011-0073)

- An error exists in the handling of Java applets that can allow sensitive form history data to be accessed. (CVE-2011-0067)

- An error in the resource protocol can allow directory traversal. (CVE-2011-0071)

- Multiple memory safety issues can lead to application crashes and possibly remote code execution. (CVE-2011-0069, CVE-2011-0070, CVE-2011-0072, CVE-2011-0074, CVE-2011-0075, CVE-2011-0077, CVE-2011-0078, CVE-2011-0080, CVE-2011-0081)

- An information disclosure vulnerability exists in the 'xsltGenerateIdFunction' function in the included libxslt library. (CVE-2011-1202)

See Also

https://www.zerodayinitiative.com/advisories/ZDI-11-157/

https://www.zerodayinitiative.com/advisories/ZDI-11-158/

https://www.zerodayinitiative.com/advisories/ZDI-11-159/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-12/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-13/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-14/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-16/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-18/

http://www.nessus.org/u?7cbff22e

Solution

Upgrade to Firefox 3.6.17 or later.

Risk Factor

High

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	47641
BID	47646
BID	47647
BID	47648
BID	47651
BID	47653
BID	47654
BID	47655
BID	47656
BID	47657
BID	47659
BID	47660
BID	47662
BID	47663
BID	47667
BID	47668
CVE	CVE-2011-0065
CVE	CVE-2011-0066
CVE	CVE-2011-0067
CVE	CVE-2011-0069
CVE	CVE-2011-0070
CVE	CVE-2011-0071
CVE	CVE-2011-0072
CVE	CVE-2011-0073
CVE	CVE-2011-0074
CVE	CVE-2011-0075
CVE	CVE-2011-0077
CVE	CVE-2011-0078
CVE	CVE-2011-0080
CVE	CVE-2011-0081
CVE	CVE-2011-1202
XREF	EDB-ID:17419
XREF	EDB-ID:17520
XREF	EDB-ID:17612
XREF	EDB-ID:17650
XREF	EDB-ID:17672

XREF	EDB-ID:18377
XREF	Secunia:44357

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2011/04/29, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.17
```

55287 - Firefox 3.6 < 3.6.18 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox 3.6 is earlier than 3.6.18. Such versions are potentially affected by the following security issues :

- Multiple memory safety issues can lead to application crashes and possibly remote code execution.
(CVE-2011-2374, CVE-2011-2376, CVE-2011-2364, CVE-2011-2365)

- A use-after-free issue when viewing XUL documents with scripts disabled could lead to code execution.
(CVE-2011-2373)

- A memory corruption issue due to multipart / x-mixed-replace images could lead to memory corruption.
(CVE-2011-2377)

- When a JavaScript Array object has its length set to an extremely large value, the iteration of array elements that occurs when its reduceRight method is called could result in code execution due to an invalid index value being used. (CVE-2011-2371)

- Multiple dangling pointer vulnerabilities could lead to code execution. (CVE-2011-0083, CVE-2011-2363, CVE-2011-0085)

- An error in the way cookies are handled could lead to information disclosure. (CVE-2011-2362)

See Also

http://www.nessus.org/u?5694f54a

https://www.mozilla.org/en-US/security/advisories/mfsa2011-19/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-20/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-21/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-22/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-23/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-24/

http://www.zerodayinitiative.com/advisories/ZDI-11-223/

http://www.zerodayinitiative.com/advisories/ZDI-11-224/

http://www.zerodayinitiative.com/advisories/ZDI-11-225/

Solution

Upgrade to Firefox 3.6.18 or later.

Risk Factor

High

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	48357
BID	48358
BID	48360
BID	48361
BID	48365
BID	48366
BID	48367
BID	48368
BID	48369
BID	48372
BID	48373
BID	48376
CVE	CVE-2011-0083
CVE	CVE-2011-0085
CVE	CVE-2011-2362
CVE	CVE-2011-2363
CVE	CVE-2011-2364
CVE	CVE-2011-2365
CVE	CVE-2011-2371
CVE	CVE-2011-2373
CVE	CVE-2011-2374
CVE	CVE-2011-2376
CVE	CVE-2011-2377
XREF	EDB-ID:17974
XREF	EDB-ID:17976
XREF	EDB-ID:18531
XREF	Secunia:44982

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2011/06/21, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.18
```

55901 - Firefox 3.6 < 3.6.20 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox 3.6 is earlier than 3.6.20. As such, it is potentially affected by the following security issues :

- A dangling pointer vulnerability exists in an SVG text manipulation routine. (CVE-2011-0084)

- A DOM accounting error exists in the 'appendChild' JavaScript function that can allow an invalid pointer to be dereferenced. (CVE-2011-2378)

- An error exists in 'ThinkPadSensor::Startup' that can allow malicious DLLs to be loaded. (CVE-2011-2980)

- An error exists in the event management code that can allow JavaScript to execute in the context of a different website and possibly in the chrome-privileged context. (CVE-2011-2981)

- Various unspecified memory safety issues exist. (CVE-2011-2982)

- A cross-domain information disclosure vulnerability exists if the configuration option 'RegExp.input' is set. (CVE-2011-2983)

- A privilege escalation vulnerability exists if web content is registered to handle 'drop' events and a browser tab is dropped in that element's area. This can allow the web content to execute with browser chrome privileges. (CVE-2011-2984)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2011-30/

https://www.zerodayinitiative.com/advisories/ZDI-11-270/

https://www.zerodayinitiative.com/advisories/ZDI-11-271/

Solution

Upgrade to Firefox 3.6.20 or later.

Risk Factor

High

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	49213
BID	49214
BID	49216
BID	49217
BID	49218
BID	49219
BID	49223
CVE	CVE-2011-0084
CVE	CVE-2011-2378
CVE	CVE-2011-2980
CVE	CVE-2011-2981
CVE	CVE-2011-2982
CVE	CVE-2011-2983
CVE	CVE-2011-2984

Exploitable With

(true)

Plugin Information

Published: 2011/08/18, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.20
```

56334 - Firefox 3.6.x < 3.6.23 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox 3.6.x is earlier than 3.6.23 and is affected by the following vulnerabilities:

- An integer underflow exists when handling a large JavaScript 'RegExp' expression that can allow a potentially exploitable crash. (CVE-2011-2998)

- If an attacker could trick a user into holding down the 'Enter' key, via a malicious game, for example, a malicious application or extension could be downloaded and executed. (CVE-2011-2372)

- Unspecified errors exist that can be exploited to corrupt memory. No additional information is available at this time. (CVE-2011-2995, CVE-2011-2996)

- There is an error in the implementation of the 'window.location' JavaScript object when creating named frames. This can be exploited to bypass the same-origin policy and potentially conduct cross-site scripting attacks. (CVE-2011-2999)

- A weakness exists when handling the 'Location' header. This can lead to response splitting attacks when visiting a vulnerable web server. The same fix has been applied to the headers 'Content-Length' and 'Content-Disposition'. (CVE-2011-3000)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2011-36/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-37/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-38/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-39/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-40/

Solution

Upgrade to Firefox 3.6.23 or later.

Risk Factor

High

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	49809
BID	49810
BID	49811
BID	49845
BID	49848
BID	49849
CVE	CVE-2011-2372
CVE	CVE-2011-2995
CVE	CVE-2011-2996
CVE	CVE-2011-2998
CVE	CVE-2011-2999
CVE	CVE-2011-3000

Plugin Information

Published: 2011/09/29, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.23
```

56750 - Firefox 3.6.x < 3.6.24 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox 3.6.x is earlier than 3.6.24 and is potentially affected by the following vulnerabilities:

- There is an error within the JSSubScriptLoader that incorrectly unwraps 'XPCNativeWrappers'. By tricking a user into installing a malicious plug-in, an attacker could exploit this issue to execute arbitrary code.

(CVE-2011-3647)

- Certain invalid sequences are not handled properly in 'Shift-JIS' encoding and can allow cross-site scripting attacks. (CVE-2011-3648)

- Profiling JavaScript files with many functions can cause the application to crash. It may be possible to trigger this behavior even when the debugging APIs are not being used. (CVE-2011-3650)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2011-46/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-47/

https://www.mozilla.org/en-US/security/advisories/mfsa2011-49/

Solution

Upgrade to Firefox 3.6.24 or later.

Risk Factor

High

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	50589
BID	50593
BID	50595

CVE	CVE-2011-3647
CVE	CVE-2011-3648
CVE	CVE-2011-3650

Plugin Information

Published: 2011/11/09, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.24
```

57769 - Firefox 3.6.x < 3.6.26 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox 3.6.x is earlier than 3.6.26 and is, therefore, potentially affected by the following security issues :

- A use-after-free error exists related to removed nsDOMAttribute child nodes.(CVE-2011-3659)

- The IPv6 literal syntax in web addresses is not being properly enforced. (CVE-2011-3670)

- Various memory safety issues exist. (CVE-2012-0442)

- Memory corruption errors exist related to the decoding of Ogg Vorbis files and processing of malformed XSLT stylesheets. (CVE-2012-0444, CVE-2012-0449)

See Also

https://www.zerodayinitiative.com/advisories/ZDI-12-059/

http://www.zerodayinitiative.com/advisories/ZDI-12-110/

http://www.ietf.org/rfc/rfc3986.txt

https://www.mozilla.org/en-US/security/advisories/mfsa2012-01/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-02/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-04/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-07/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-08/

Solution

Upgrade to Firefox 3.6.26 or later.

Risk Factor

High

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	51753
BID	51754
BID	51755
BID	51756
BID	51786
CVE	CVE-2011-3659
CVE	CVE-2011-3670
CVE	CVE-2012-0442
CVE	CVE-2012-0444
CVE	CVE-2012-0449

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2012/02/01, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.26
```

58006 - Firefox 3.6.x < 3.6.27 '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 3.6.x is earlier than 3.6.27 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 3.6.27 or later.

Risk Factor

High

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 : 3.6.12
Fixed version     : 3.6.27
```

58349 - Firefox 3.6.x < 3.6.28 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox 3.6.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-2012-0457, CVE-2012-0461, CVE-2012-0463, CVE-2012-0464)

- 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)

See Also

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/mfsa2012-16/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-19/

Solution

Upgrade to Firefox 3.6.28 or later.

Risk Factor

High

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	52458

BID	52459
BID	52460
BID	52461
BID	52464
BID	52465
BID	52466
CVE	CVE-2012-0455
CVE	CVE-2012-0456
CVE	CVE-2012-0457
CVE	CVE-2012-0458
CVE	CVE-2012-0461
CVE	CVE-2012-0463
CVE	CVE-2012-0464

Plugin Information

Published: 2012/03/15, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.28
```

57768 - Firefox < 10.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 10.0 and thus, is potentially affected by the following security issues :

- A use-after-free error exists related to removed nsDOMAttribute child nodes.(CVE-2011-3659)

- Various memory safety issues exist. (CVE-2012-0442, CVE-2012-0443)

- Memory corruption errors exist related to the decoding of Ogg Vorbis files and processing of malformed XSLT stylesheets. (CVE-2012-0444, CVE-2012-0449)

- The HTML5 frame navigation policy can be violated by allowing an attacker to replace a sub-frame in another domain's document. (CVE-2012-0445)

- Scripts in frames are able to bypass security restrictions in XPConnect. This bypass can allow malicious websites to carry out cross-site scripting attacks. (CVE-2012-0446)

- An information disclosure issue exists when uninitialized memory is used as padding when encoding icon images. (CVE-2012-0447)

See Also

https://www.zerodayinitiative.com/advisories/ZDI-12-059/

http://www.zerodayinitiative.com/advisories/ZDI-12-110/

http://dev.w3.org/html5/spec/browsers.html#security-nav

https://www.mozilla.org/en-US/security/advisories/mfsa2012-01/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-03/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-04/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-05/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-06/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-07/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-08/

Solution

Upgrade to Firefox 10.0 or later.

Risk Factor

High

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	51752
BID	51753
BID	51754
BID	51755
BID	51756
BID	51757
BID	51765
CVE	CVE-2011-3659
CVE	CVE-2012-0442
CVE	CVE-2012-0443
CVE	CVE-2012-0444
CVE	CVE-2012-0445
CVE	CVE-2012-0446
CVE	CVE-2012-0447
CVE	CVE-2012-0449
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

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2012/02/01, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 10.0
```

58898 - Firefox < 12.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 12.0 and thus, is potentially affected by the following security issues :

- An error exists with handling JavaScript errors that could lead to information disclosure. (CVE-2011-1187)

- An off-by-one error exists in the 'OpenType Sanitizer'

that could 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, CVE-2012-0468)

- 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 could 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)

- IPv6 addresses and cross-site 'XHR' or 'WebSocket'

connections on non-standard ports could allow this application to send ambiguous origin headers.

(CVE-2012-0475)

- 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/mfsa2012-28/
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/mfsa2012-32/
https://www.mozilla.org/en-US/security/advisories/mfsa2012-33/

Solution

Upgrade to Firefox 12.0 or later.

Risk Factor

High

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	53221
BID	53222
BID	53223
BID	53224
BID	53225
BID	53227
BID	53228
BID	53229
BID	53230

BID	53231
CVE	CVE-2011-1187
CVE	CVE-2011-3062
CVE	CVE-2012-0467
CVE	CVE-2012-0468
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-2012-0475
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 : 3.6.12
Fixed version     : 12.0
```

59407 - Firefox < 13.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 13.0 and thus, 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-2012-1938)

- 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)

- Two arbitrary DLL load issues exist related to the application update and update service functionality.
(CVE-2012-1942, CVE-2012-1943)

- 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)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2012-34/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-35/

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/

https://www.mozilla.org/en-US/security/advisories/mfsa2012-54/

Solution

Upgrade to Firefox 13.0 or later.

Risk Factor

High

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	53796
BID	53798
BID	53800
BID	53801
BID	53803
BID	53807
BID	54581
CVE	CVE-2012-0441
CVE	CVE-2012-1937
CVE	CVE-2012-1938
CVE	CVE-2012-1940
CVE	CVE-2012-1941
CVE	CVE-2012-1942
CVE	CVE-2012-1943
CVE	CVE-2012-1944
CVE	CVE-2012-1946
CVE	CVE-2012-1947
CVE	CVE-2012-1964
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 : 3.6.12
Fixed version     : 13.0
```

65131 - Firefox < 19.0.2 nsHTMLEditor Use-After-Free

Synopsis

The remote Windows host contains a web browser that is potentially affected by a use-after-free vulnerability.

Description

The installed version of Firefox is earlier than 19.0.2, and thus, is potentially affected by a use-after-free vulnerability.

An error exists in the HTML editor (nsHTMLEditor) related to content script and the calling of the function 'document.execCommand' while internal editor operations are running. The previously freed memory can be dereferenced and could lead to arbitrary code execution.

See Also

http://www.securityfocus.com/archive/1/526050/30/0/threaded

http://www.zerodayinitiative.com/advisories/ZDI-13-090/

https://www.mozilla.org/en-US/security/advisories/mfsa2013-29/

Solution

Upgrade to Firefox 19.0.2 or later.

Risk Factor

High

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	58391
CVE	CVE-2013-0787

Plugin Information

Published: 2013/03/08, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 19.0.2
```

70949 - Firefox < 25.0.1 NSS and NSPR Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is a version prior to 25.0.1 and is, therefore, potentially affected by the following vulnerabilities :

- An error exists related to handling input greater than half the maximum size of the 'PRUint32' value.

(CVE-2013-1741)

- An error exists in the 'Null_Cipher' function in the file 'ssl/ssl3con.c' related to handling invalid handshake packets that could allow arbitrary code execution. (CVE-2013-5605)

- An error exists in the 'CERT_VerifyCert' function in the file 'lib/certhigh/certvfy.c' that could allow invalid certificates to be treated as valid.

(CVE-2013-5606)

- An integer truncation error exists in the function 'PL_ArenaAllocate' in the Netscape Portable Runtime (NSPR) library. (CVE-2013-5607)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2013-103/

https://www.mozilla.org/en-US/firefox/25.0.1/releasenotes/

https://developer.mozilla.org/en-US/docs/NSS/NSS_3.15.3_release_notes

Solution

Upgrade to Firefox 25.0.1 or later.

Risk Factor

High

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	63736

BID	63737
BID	63738
BID	63802
CVE	CVE-2013-1741
CVE	CVE-2013-5605
CVE	CVE-2013-5606
CVE	CVE-2013-5607

Plugin Information

Published: 2013/11/18, Modified: 2019/11/27

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 25.0.1
```

73099 - Firefox < 28.0 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is a version prior to 28.0 and is, therefore, potentially affected by the following vulnerabilities :

- Memory issues exist that could lead to arbitrary code execution. (CVE-2014-1493, CVE-2014-1494)

- An issue exists where extracted files for updates are not read-only while updating. An attacker may be able to modify these extracted files resulting in privilege escalation. (CVE-2014-1496)

- An out-of-bounds read error exists when decoding WAV format audio files that could lead to a denial of service attack or information disclosure.

(CVE-2014-1497)

- An issue exists in the 'crypto.generateCRFMRequest'

method due to improper validation of the KeyParams argument when generating 'ec-dual-use' requests. This could lead to a denial of service attack.

(CVE-2014-1498)

- An issue exists that could allow for spoofing attacks to occur during a WebRTC session. Exploitation of this issue could allow an attacker to gain access to the user's webcam or microphone. (CVE-2014-1499)

- An issue exists with JavaScript 'onbeforeunload' events that could lead to denial of service attacks.

(CVE-2014-1500)

- An issue exists where WebGL context from one website can be injected into the WebGL context of another website that could result in arbitrary content being rendered from the second website. (CVE-2014-1502)

- A cross-site scripting issue exists due to the Content Security Policy (CSP) of 'data:' documents not being saved for a session restore. Under certain circumstances, an attacker may be able to evade the CSP of a remote website resulting in a cross-scripting attack. (CVE-2014-1504)

- An out-of-bounds read error exists when polygons are rendered in 'MathML' that could lead to information disclosure. (CVE-2014-1508)

- A memory corruption issue exists in the Cairo graphics library when rendering a PDF file that could lead to arbitrary code execution or a denial of service attack.

(CVE-2014-1509)

- An issue exists in the SVG filters and the feDisplacementMap element that could lead to information disclosure via timing attacks.

(CVE-2014-1505)

- An issue exists that could allow malicious websites to load chrome-privileged pages when JavaScript implemented WebIDL calls the 'window.open()' function, which could result in arbitrary code execution.

(CVE-2014-1510)

- An issue exists that could allow a malicious website to bypass the pop-up blocker. (CVE-2014-1511)

- A use-after-free memory issue exists in 'TypeObjects'
in the JavaScript engine during Garbage Collection that could lead to arbitrary code execution.
(CVE-2014-1512)

- An out-of-bounds write error exists due to 'TypedArrayObject' improperly handling 'ArrayBuffer'
objects that could result in arbitrary code execution.
(CVE-2014-1513)

- An out-of-bounds write error exists when copying values from one array to another that could result in arbitrary code execution. (CVE-2014-1514)

See Also

http://www.securityfocus.com/archive/1/531617/30/0/threaded
https://www.mozilla.org/en-US/security/advisories/mfsa2014-15/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-16/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-17/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-18/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-19/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-15/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-16/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-17/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-18/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-19/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-20/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-22/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-23/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-26/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-27/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-28/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-29/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-30/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-31/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-32/

Solution

Upgrade to Firefox 28.0 or later.

Risk Factor

High

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	66203
BID	66206
BID	66207
BID	66209
BID	66240
BID	66412
BID	66416
BID	66417
BID	66418
BID	66419
BID	66421
BID	66422
BID	66423
BID	66425
BID	66426
BID	66428
BID	66429
CVE	CVE-2014-1493
CVE	CVE-2014-1494
CVE	CVE-2014-1496
CVE	CVE-2014-1497
CVE	CVE-2014-1498
CVE	CVE-2014-1499
CVE	CVE-2014-1500
CVE	CVE-2014-1502
CVE	CVE-2014-1504
CVE	CVE-2014-1505
CVE	CVE-2014-1508
CVE	CVE-2014-1509
CVE	CVE-2014-1510
CVE	CVE-2014-1511
CVE	CVE-2014-1512
CVE	CVE-2014-1513
CVE	CVE-2014-1514

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: 2014/03/19, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 28.0
```

77906 - Firefox < 32.0.3 NSS Signature Verification Vulnerability

Synopsis

The remote Windows host contains a web browser that is affected by a signature forgery vulnerability.

Description

The version of Firefox installed on the remote host is prior to 32.0.3. It is, therefore, affected by a flaw in the Network Security Services (NSS) library, which is due to lenient parsing of ASN.1 values involved in a signature and can lead to the forgery of RSA signatures, such as SSL certificates.

See Also

https://www.mozilla.org/security/announce/2014/mfsa2014-73.html

Solution

Upgrade to Firefox 32.0.3 or later.

Risk Factor

High

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	70116
CVE	CVE-2014-1568
XREF	CERT:772676

Plugin Information

Published: 2014/09/26, Modified: 2019/11/25

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
```

```
  Installed version : 3.6.12
  Fixed version     : 32.0.3
```

78473 - Firefox < 33.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is a version prior to 33.0. It is, therefore, affected by the following vulnerabilities :

- Multiple memory safety flaws exist within the browser engine. Exploiting these, an attacker can cause a denial of service or execute arbitrary code. (CVE-2014-1574, CVE-2014-1575)

- A buffer overflow vulnerability exists when capitalization style changes occur during CSS parsing.

(CVE-2014-1576)

- An out-of-bounds read error exists in the Web Audio component when invalid values are used in custom waveforms that leads to a denial of service or information disclosure. (CVE-2014-1577)

- An out-of-bounds write error exists when processing invalid tile sizes in 'WebM' format videos that result in arbitrary code execution. (CVE-2014-1578)

- Memory is not properly initialized during GIF rendering within a '<canvas>' element. Using a specially crafted web script, a remote attacker can exploit this to acquire sensitive information from the process memory.

(CVE-2014-1580)

- A use-after-free error exists in the 'DirectionalityUtils' component when text direction is used in the text layout that results in arbitrary code execution. (CVE-2014-1581)

- Multiple security bypass vulnerabilities exist related to key pinning, a method to prevent man-in-the-middle attacks by verifying certificates. An attacker can use SPDY or HTTP/2 connection coalescing to bypass key pinning on websites that use a domain name that resolve to the same IP address. Another issue exists in which key pinning verification is not performed due to an issue verifying the issuer of an SSL certificate. These issues could result in man-in-the-middle attacks. Note that key pinning was introduced in Firefox 32.

(CVE-2014-1582, CVE-2014-1584)

- An error exists that could allow a malicious app to use 'AlarmAPI' to read cross-origin references and possibly allow for the same-origin policy to be bypassed.

(CVE-2014-1583)

- Multiple issues exist in WebRTC when the session is running within an 'iframe' element that will allow the session to be accessible even when sharing is stopped and when returning to the website. This could lead to video inadvertently being shared. (CVE-2014-1585, CVE-2014-1586)

See Also

https://www.mozilla.org/security/announce/2014/mfsa2014-74.html

https://www.mozilla.org/security/announce/2014/mfsa2014-75.html

https://www.mozilla.org/security/announce/2014/mfsa2014-76.html

https://www.mozilla.org/security/announce/2014/mfsa2014-77.html
https://www.mozilla.org/security/announce/2014/mfsa2014-78.html
https://www.mozilla.org/security/announce/2014/mfsa2014-79.html
https://www.mozilla.org/security/announce/2014/mfsa2014-80.html
https://www.mozilla.org/security/announce/2014/mfsa2014-81.html
https://www.mozilla.org/security/announce/2014/mfsa2014-82.html

Solution

Upgrade to Firefox 33.0 or later.

Risk Factor

High

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

BID	70424
BID	70425
BID	70426
BID	70427
BID	70428
BID	70430
BID	70431
BID	70432
BID	70434
BID	70436
BID	70439
BID	70440
CVE	CVE-2014-1574
CVE	CVE-2014-1575
CVE	CVE-2014-1576
CVE	CVE-2014-1577
CVE	CVE-2014-1578
CVE	CVE-2014-1580
CVE	CVE-2014-1581
CVE	CVE-2014-1582

CVE	CVE-2014-1583
CVE	CVE-2014-1584
CVE	CVE-2014-1585
CVE	CVE-2014-1586

Plugin Information

Published: 2014/10/15, Modified: 2019/11/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 33.0
```

79665 - Firefox < 34.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is a version prior to 34.0. It is, therefore, affected by the following vulnerabilities :

- A security bypass vulnerability exists due to the 'XrayWrappers' filter not properly validating object properties. This allows a remote attacker to bypass security protection mechanisms to access protected objects. (CVE-2014-8631)

- A security bypass vulnerability exists due to Chrome Object Wrappers (COW) being passed as native interfaces.

This allows a remote attacker to access normally protected objects. (CVE-2014-8632)

- A remote code execution vulnerability exists in Mozilla Network Security Services (NSS) due to a flaw in 'quickder.c' that is triggered when handling PKCS#1 signatures during the decoding of ASN.1 DER.

(CVE-2014-1569)

- Multiple memory safety flaws exist within the browser engine. Exploiting these, an attacker can cause a denial of service or execute arbitrary code. (CVE-2014-1587, CVE-2014-1588)

- A security bypass vulnerability exists due improper declaration of chrome accessible CSS primary namespaces allowing for XML Binding Language (XBL) bindings to be triggered remotely. (CVE-2014-1589)

- A denial of service vulnerability exists due to improper parsing of a JavaScript object to the XMLHttpRequest API which can result in a crash.

(CVE-2014-1590)

- An information disclosure vulnerability exists due to Content Security Policy (CSP) violation reports triggered by a redirect not properly removing path information which can reveal sensitive information.

Note that this only affects Firefox 33. (CVE-2014-1591)

- A use-after-free error exists due the creation of a second XML root element when parsing HTML written to a document created with 'document.open()' function which can result in arbitrary code execution. (CVE-2014-1592)

- A buffer overflow vulnerability exists in the 'mozilla::FileBlockCache::Read' function when parsing media which can result in arbitrary code execution.

(CVE-2014-1593)

- A casting error exists when casting from the 'BasicThebesLayer' layer to the 'BasicContainerLayer'

layer which can result in arbitrary code execution.

(CVE-2014-1594)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2014-83/

https://www.mozilla.org/en-US/security/advisories/mfsa2014-84/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-85/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-86/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-87/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-88/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-89/
https://www.mozilla.org/en-US/security/advisories/mfsa2014-91/

Solution

Upgrade to Firefox 34.0 or later.

Risk Factor

High

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	71391
BID	71392
BID	71393
BID	71395
BID	71396
BID	71397
BID	71398
BID	71399
BID	71556
BID	71560
BID	71675
CVE	CVE-2014-1569
CVE	CVE-2014-1587
CVE	CVE-2014-1588
CVE	CVE-2014-1589
CVE	CVE-2014-1590
CVE	CVE-2014-1591
CVE	CVE-2014-1592
CVE	CVE-2014-1593

CVE	CVE-2014-1594
CVE	CVE-2014-8631
CVE	CVE-2014-8632

Plugin Information

Published: 2014/12/02, Modified: 2019/11/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 34.0
```

80523 - Firefox < 35 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 35.0. It is, therefore, affected by the following vulnerabilities :

- Multiple unspecified memory safety issues exist within the browser engine. (CVE-2014-8634, CVE-2014-8635)

- A flaw exists where DOM objects with some specific properties can bypass XrayWrappers. This can allow web content to confuse privileged code, potentially enabling privilege escalation. (CVE-2014-8636)

- A flaw exists in the rendering of bitmap images. When rending a malformed bitmap image, memory may not always be properly initialized, which can result in a leakage of data to web content. (CVE-2014-8637)

- A flaw exists in 'navigator.sendBeacon()' in which it does not follow the cross-origin resource sharing specification. This results in requests from 'sendBeacon()' lacking an 'origin' header, which allows malicious sites to perform XSRF attacks. (CVE-2014-8638)

- A flaw exists when receiving 407 Proxy Authentication responses with a 'set-cookie' header. This can allow a session-fixation attack. (CVE-2014-8639)

- A flaw exists in Web Audio that cam allow a small block of memory to be read. (CVE-2014-8640)

- A read-after-free flaw exists in WebRTC due to the way tracks are handled, which can result in a potentially exploitable crash or incorrect WebRTC behavior.

(CVE-2014-8641)

- A flaw exists where delegated Online Certificate Status Protocol responder certificates fail to recognize the id-pkix-ocsp-nocheck extension. This can result in a user connecting to a site with a revoked certificate.

(CVE-2014-8642)

- A flaw exists in the Gecko Media Plugin which can allow an attacker to break out of the sandbox. (CVE-2014-8643)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-01/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-02/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-03/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-04/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-05/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-06/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-07/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-08/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-09/

Solution

Upgrade to Firefox 35.0 or later.

Risk Factor

High

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	72041
BID	72042
BID	72043
BID	72044
BID	72045
BID	72046
BID	72047
BID	72048
BID	72049
BID	72050
CVE	CVE-2014-8634
CVE	CVE-2014-8635
CVE	CVE-2014-8636
CVE	CVE-2014-8637
CVE	CVE-2014-8638
CVE	CVE-2014-8639
CVE	CVE-2014-8640
CVE	CVE-2014-8641
CVE	CVE-2014-8642
CVE	CVE-2014-8643
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: 2015/01/14, Modified: 2019/11/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 35
```

81521 - Firefox < 36 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 36.0. It is, therefore, affected by the following vulnerabilities :

- An issue exists that allows whitelisted Mozilla domains to make 'UITour' API calls while UI Tour pages are present in background tabs. This allows an attacker, via a compromised Mozilla domain, to engage in spoofing and clickjacking in any foreground tab. (CVE-2015-0819)

- An issue exists related to sandbox libraries, including the Caja Compiler, which allows JavaScript objects to be marked as extensible even though the objects were initially marked as non-extensible. (CVE-2015-0820)

- An issue exists when opening hyperlinks on a page with the mouse and specific keyboard key combinations that allows a Chrome privileged URL to be opened without context restrictions being preserved. Additionally, the issue allows the opening of local files and resources from a known location to be opened with local privileges, bypassing security protections.

(CVE-2015-0821)

- An information disclosure vulnerability exists related to the autocomplete feature that allows an attacker to read arbitrary files. (CVE-2015-0822)

- A use-after-free error exists with the OpenType Sanitiser (OTS) when expanding macros. (CVE-2015-0823)

- An issue exists in the DrawTarget() function of the Cairo graphics library that allows an attacker cause a segmentation fault, resulting in a denial of service.

(CVE-2015-0824)

- A buffer underflow issue exists during audio playback of invalid MP3 audio files. (CVE-2015-0825)

- An out-of-bounds read issue exists while restyling and reflowing changes of web content with CSS, resulting in a denial of service condition or arbitrary code execution. (CVE-2015-0826)

- An out-of-bounds read and write issue exists when processing invalid SVG graphic files. This allows an attacker to disclose sensitive information.

(CVE-2015-0827)

- A double-free issue exists when sending a zero-length XmlHttpRequest (XHR) object due to errors in memory allocation when using different memory allocator libraries than 'jemalloc'. This allows an attacker to crash the application. (CVE-2015-0828)

- A buffer overflow issue exists in the 'libstagefright'

library when processing invalid MP4 video files, resulting in a denial of service condition or arbitrary code execution. (CVE-2015-0829)

- An unspecified issue exists that allows an attacker, via specially crafted WebGL content, to cause a denial of service condition. (CVE-2015-0830)

- A use-after-free issue exists when running specific web content with 'IndexedDB' to create an index, resulting in a denial of service condition or arbitrary code execution. (CVE-2015-0831)

- An issue exists when a period is appended to a hostname that results in a bypass of the Public Key Pinning Extension for HTTP (HPKP) and HTTP Strict Transport Security (HSTS) when certificate pinning is set to strict mode. An attacker can exploit this issue to perform man-in-the-middle attacks if the attacker has a security certificate for a domain with the added period.

(CVE-2015-0832)

- An issue exists in the Mozilla updater in which DLL files in the current working directory or Windows temporary directories will be loaded, allowing the execution of arbitrary code. Note that hosts are only affected if the updater is not run by the Mozilla Maintenance Service. (CVE-2015-0833)

- An information disclosure vulnerability exists due to the lack of TLS support for connections to TURN and STUN servers, resulting in cleartext connections.

(CVE-2015-0834)

- Multiple unspecified memory safety issues exist within the browser engine. (CVE-2015-0835, CVE-2015-0836)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-11/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-12/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-13/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-14/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-15/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-16/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-17/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-18/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-19/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-20/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-21/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-22/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-23/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-24/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-25/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-26/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-27/

Solution

Upgrade to Firefox 36.0 or later.

Risk Factor

High

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	72741
BID	72742
BID	72743
BID	72744
BID	72745
BID	72746
BID	72747
BID	72748
BID	72750
BID	72751
BID	72752
BID	72753
BID	72754
BID	72755
BID	72756
BID	72757
BID	72758
BID	72759
CVE	CVE-2015-0819
CVE	CVE-2015-0820
CVE	CVE-2015-0821
CVE	CVE-2015-0822
CVE	CVE-2015-0823
CVE	CVE-2015-0824
CVE	CVE-2015-0825
CVE	CVE-2015-0826
CVE	CVE-2015-0827
CVE	CVE-2015-0828
CVE	CVE-2015-0829
CVE	CVE-2015-0830
CVE	CVE-2015-0831
CVE	CVE-2015-0832
CVE	CVE-2015-0833
CVE	CVE-2015-0834

CVE	CVE-2015-0835
CVE	CVE-2015-0836

Plugin Information

Published: 2015/02/25, Modified: 2019/11/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 36
```

82041 - Firefox < 36.0.4 SVG Bypass Privilege Escalation

Synopsis

The remote Windows host contains a web browser that is affected by a privilege escalation vulnerability.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 36.0.4. It is, therefore, affected by a privilege escalation vulnerability due to a flaw within 'docshell/base/nsDocShell.cpp', which relates to SVG format content navigation. A remote attacker can exploit this to bypass same-origin policy protections, allowing a possible execution of arbitrary scripts in a privileged context.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-28/

Solution

Upgrade to Firefox 36.0.4 or later.

Risk Factor

High

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	73265
CVE	CVE-2015-0818

Plugin Information

Published: 2015/03/24, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
```

```
    Fixed version     : 36.0.4
```

82503 - Firefox < 37.0 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 37.0. It is, therefore, affected by the following vulnerabilities :

- A privilege escalation vulnerability exists which relates to anchor navigation. A remote attacker can exploit this to bypass same-origin policy protections, allowing a possible execution of arbitrary scripts in a privileged context. Note that this is a variant of CVE-2015-0818 that was fixed in Firefox 36.0.4.

(CVE-2015-0801)

- Access to certain privileged internal methods is retained when navigating from windows created to contain privileged UI content to unprivileged pages. An attacker can exploit this to execute arbitrary JavaScript with elevated privileges. (CVE-2015-0802)

- Multiple type confusion issues exist that can lead to use-after-free errors, which a remote attacker can exploit to execute arbitrary code or cause a denial of service. (CVE-2015-0803, CVE-2015-0804)

- Multiple memory corruption issues exist related to Off Main Thread Compositing when rendering 2D graphics, which a remote attacker can exploit to execute arbitrary code or cause a denial of service. (CVE-2015-0805, CVE-2015-0806)

- A cross-site request forgery (XSRF) vulnerability exists in the sendBeacon() function due to cross-origin resource sharing (CORS) requests following 30x redirections. (CVE-2015-0807)

- An issue exists in WebRTC related to memory management for simple-style arrays, which may be used by a remote attacker to cause a denial of service. (CVE-2015-0808)

- An out-of-bounds read issue exists in the QCMS color management library that could lead to an information disclosure. (CVE-2015-0811)

- An issue exists that can allow a man-in-the-middle attacker to bypass user-confirmation and install a Firefox lightweight theme by spoofing a Mozilla sub-domain. (CVE-2015-0812)

- Multiple memory safety issues exist within the browser engine. A remote attacker can exploit these to corrupt memory and possibly execute arbitrary code.

(CVE-2015-0814, CVE-2015-0815)

- A privilege escalation vulnerability exists related to documents loaded through a 'resource:' URL. An attacker can exploit this to load pages and execute JavaScript with elevated privileges. (CVE-2015-0816)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-30/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-32/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-33/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-34/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-36/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-37/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-38/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-39/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-40/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-42/

Solution

Upgrade to Firefox 37.0 or later.

Risk Factor

High

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	73454
BID	73455
BID	73457
BID	73458
BID	73460
BID	73461
BID	73462
BID	73464
BID	73465
BID	73466
BID	73467
CVE	CVE-2015-0801
CVE	CVE-2015-0802
CVE	CVE-2015-0803
CVE	CVE-2015-0804
CVE	CVE-2015-0805
CVE	CVE-2015-0806
CVE	CVE-2015-0807
CVE	CVE-2015-0808
CVE	CVE-2015-0811
CVE	CVE-2015-0812

CVE	CVE-2015-0814
CVE	CVE-2015-0815
CVE	CVE-2015-0816

Exploitable With

Metasploit (true)

Plugin Information

Published: 2015/04/01, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 37.0
```

86071 - Firefox < 41 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 41. 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 that allows scripted proxies to access the inner window. (CVE-2015-4502)

- An out-of-bounds read issue exists in TCPSocket.js related to the sending of strings over TCPSocket. A remote attacker can exploit this disclose memory contents. (CVE-2015-4503)

- An out-of-bounds read error exists in the QCMS color management library that is triggered when manipulating an image with specific attributes in its ICC V4 profile.

A remote attacker can exploit this to cause a denial of service condition or to disclose sensitive information.

(CVE-2015-4504)

- 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 flaw exists in the debugger API that is triggered when using the debugger with SavedStacks in JavaScript. An attacker can exploit this to cause a denial of service condition. (CVE-2015-4507)

- A flaw exists in reader mode that allows an attacker to spoof the URL displayed in the address bar.

(CVE-2015-4508)

- 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 use-after-free error exists when using a shared worker with IndexedDB due to a race condition with the worker.

A remote attacker can exploit this, via specially crafted content, to cause a denial of service condition.

(CVE-2015-4510)

- 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)

- An out-of-bounds read error exists during 2D canvas rendering due to an issue in the cairo graphics library.

An attacker can exploit this to read random memory, resulting in the disclosure of sensitive information.

(CVE-2015-4512)

- A security bypass vulnerability exists due to a flaw in Gecko's implementation of the ECMAScript 5 API. An attacker can exploit this to run web content in a privileged context, resulting in the execution of arbitrary code. (CVE-2015-4516)

- 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)

- An unspecified flaw exists in the nsPerformance::Now() function in dom/base/nsPerformance.cpp that allows an attacker to use a side-channel attack to disclose sensitive information. (CVE-2015-7327)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-96/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-98/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-97/
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/mfsa2015-102/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-103/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-104/
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/mfsa2015-107/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-108/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-109/
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/
https://www.mozilla.org/en-US/security/advisories/mfsa2015-114/

Solution

Upgrade to Firefox 41 or later.

Risk Factor

High

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-2015-4500
CVE	CVE-2015-4501
CVE	CVE-2015-4502
CVE	CVE-2015-4503

CVE	CVE-2015-4504
CVE	CVE-2015-4505
CVE	CVE-2015-4506
CVE	CVE-2015-4507
CVE	CVE-2015-4508
CVE	CVE-2015-4509
CVE	CVE-2015-4510
CVE	CVE-2015-4511
CVE	CVE-2015-4512
CVE	CVE-2015-4516
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
CVE	CVE-2015-7327

Plugin Information

Published: 2015/09/22, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 41
```

86764 - Firefox < 42 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 42. 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 information disclosure vulnerability exists when handling type 3 messages as part of the NTLM authentication exchange. A remote attacker can exploit this, via a specially crafted web page that sends an NTLM request, to disclose system hostname and windows domain information. (CVE-2015-4515)

- A security bypass vulnerability exists due to the whitelist used by Reader View to disable scripts for rendered pages being too permissive. A remote attacker can exploit this, via specially crafted web page, to bypass Content Security Policy (CSP) protections.

(CVE-2015-4518)

- 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 security bypass vulnerability exists due to a failure to enforce settings when disabling scripts in the Add-on SDK panel. A remote attacker can exploit this, via a crafted web page, to bypass security restrictions and conduct a cross-site scripting attack. (CVE-2015-7187)

- 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)

- An information disclosure vulnerability exists due to improper parsing of escaped characters in the hostname of location headers. A remote attacker can exploit this to gain access to arbitrary site-specific token information. (CVE-2015-7195)

- 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/mfsa2015-117/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-118/

https://www.mozilla.org/en-US/security/advisories/mfsa2015-121/

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/mfsa2015-129/

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 42 or later.

Risk Factor

High

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	77412
BID	77415
BID	77416
CVE	CVE-2015-4513
CVE	CVE-2015-4514
CVE	CVE-2015-4515
CVE	CVE-2015-4518
CVE	CVE-2015-7181
CVE	CVE-2015-7182
CVE	CVE-2015-7183
CVE	CVE-2015-7187
CVE	CVE-2015-7188
CVE	CVE-2015-7189
CVE	CVE-2015-7193
CVE	CVE-2015-7194
CVE	CVE-2015-7195
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 : 3.6.12
Fixed version     : 42
```

88754 - Firefox < 44.0.2 Service Workers Security Bypass

Synopsis

The remote Windows host contains a web browser that is affected by a security bypass vulnerability.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 44.0.2. It is, therefore, affected by a security bypass vulnerability due to improper restriction of interaction between service workers and plugins. An unauthenticated, remote attacker can exploit this, via a crafted web site that triggers spoofed responses to requests that use NPAPI, to bypass the same-origin policy.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2016-13/

Solution

Upgrade to Mozilla Firefox version 44.0.2 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)

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-2016-1949
XREF	MFSA:2016-13

Plugin Information

Published: 2016/02/16, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 44.0.2
```

90793 - Firefox < 46 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 46. 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-2016-2804, CVE-2016-2806, 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 local privilege escalation vulnerability exists in the Maintenance Service updater due to improper handling of long log file paths. A local attacker can exploit this to delete arbitrary files and gain elevated privileges.

(CVE-2016-2809)

- A remote code execution vulnerability exists due to a use-after-free error in the BeginReading() function. A context-dependent attacker can exploit this to dereference already freed memory, resulting in the execution of arbitrary code. (CVE-2016-2811)

- A remote code execution vulnerability exists due to a race condition in ServiceWorkerManager in the get() function. A context-dependent attacker can exploit this to execute arbitrary code. (CVE-2016-2812)

- 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)

- A security bypass vulnerability exists due to the Content Security Policy (CSP) not being properly applied to web content sent with the 'multipart/x-mixed-replace'

MIME-type. A context-dependent attacker can exploit this to bypass CSP protection. (CVE-2016-2816)

- A cross-site scripting (XSS) vulnerability exists due to improper restriction of unprivileged 'javascript: URL'

navigation. A context-dependent attacker can exploit this, via a specially crafted request, to execute arbitrary script code in the context of a user's browser session. (CVE-2016-2817)

- A flaw exists in the Firefox Health Report that is triggered when it accepts any content document events that are presented in its iframe. A context-dependent attacker can exploit this to manipulate sharing preferences. (CVE-2016-2820)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2016-39/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-40/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-42/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-44/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-45/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-46/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-47/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-48/

Solution

Upgrade to Firefox version 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)

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-2016-2804
CVE	CVE-2016-2806
CVE	CVE-2016-2807
CVE	CVE-2016-2808
CVE	CVE-2016-2809
CVE	CVE-2016-2811
CVE	CVE-2016-2812
CVE	CVE-2016-2814
CVE	CVE-2016-2816
CVE	CVE-2016-2817
CVE	CVE-2016-2820
XREF	MFSA:2016-39
XREF	MFSA:2016-40

XREF	MFSA:2016-42
XREF	MFSA:2016-44
XREF	MFSA:2016-45
XREF	MFSA:2016-46
XREF	MFSA:2016-47
XREF	MFSA:2016-48

Plugin Information

Published: 2016/04/29, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 46
```

91547 - Firefox < 47 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 47. It is, therefore, affected by multiple vulnerabilities :

- Multiple memory corruption issues exist that allow an unauthenticated, remote attacker to execute arbitrary code. (CVE-2016-2815, CVE-2016-2818)

- An overflow condition exists that is triggered when handling HTML5 fragments in foreign contexts (e.g., under <svg> nodes). An unauthenticated, remote attacker can exploit this to cause a heap-based buffer overflow, resulting in the execution of arbitrary code.

(CVE-2016-2819)

- A use-after-free error exists that is triggered when deleting DOM table elements in 'contenteditable' mode.

An unauthenticated, remote attacker can exploit this to dereference already freed memory, resulting in the execution of arbitrary code. (CVE-2016-2821)

- A spoofing vulnerability exists due to improper handling of SELECT elements. An unauthenticated, remote attacker can exploit this to spoof the contents of the address bar. (CVE-2016-2822)

- An out-of-bounds write error exists in the ANGLE graphics library due to improper size checking while writing to an array during WebGL shader operations. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-2824)

- A same-origin bypass vulnerability exists that is triggered when handling location.host property values set after the creation of invalid 'data:' URIs. An unauthenticated, remote attacker can exploit this to partially bypass same-origin policy protections.

(CVE-2016-2825)

- A privilege escalation vulnerability exists in the Windows updater utility due to improper extraction of files from MAR archives. A local attacker can exploit this to replace the extracted files, allowing the attacker to gain elevated privileges. (CVE-2016-2826)

- A use-after-free error exists that is triggered when destroying the recycle pool of a texture used during the processing of WebGL content. An unauthenticated, remote attacker can exploit this to dereference already freed memory, resulting in the execution of arbitrary code.

(CVE-2016-2828)

- A flaw exists in browser/modules/webrtcUI.jsm that is triggered when handling a large number of permission requests over a small period of time. An unauthenticated, remote attacker can exploit this to cause the incorrect icon to be displayed in a given permission request, potentially resulting in a user approving unintended permission requests.

(CVE-2016-2829)

- A flaw exists that is triggered when handling paired fullscreen and pointerlock requests in combination with closing windows. An unauthenticated, remote attacker can exploit this to create an unauthorized pointerlock, resulting in a denial of service condition.

Additionally, an attacker can exploit this to conduct spoofing and clickjacking attacks. (CVE-2016-2831)

- An information disclosure vulnerability exists that is triggered when handling CSS pseudo-classes. An unauthenticated, remote attacker can exploit this disclose a list of installed plugins. (CVE-2016-2832)

- A Content Security Policy (CSP) bypass exists that is triggered when handling specially crafted cross-domain Java applets. An unauthenticated, remote attacker can exploit this to bypass the CSP and conduct cross-site scripting attacks. (CVE-2016-2833)

- Multiple unspecified flaws exist in the Mozilla Network Security Services (NSS) component that allow an attacker to have an unspecified impact. (CVE-2016-2834)

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2016-49/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-50/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-51/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-52/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-53/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-54/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-55/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-56/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-57/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-58/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-59/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-60/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-61/

Solution

Upgrade to Firefox version 47 or later.

Risk Factor

High

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)

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	91072
BID	91074
BID	91075
CVE	CVE-2016-2815
CVE	CVE-2016-2818
CVE	CVE-2016-2819
CVE	CVE-2016-2821
CVE	CVE-2016-2822
CVE	CVE-2016-2824
CVE	CVE-2016-2825
CVE	CVE-2016-2826
CVE	CVE-2016-2828
CVE	CVE-2016-2829
CVE	CVE-2016-2831
CVE	CVE-2016-2832
CVE	CVE-2016-2833
CVE	CVE-2016-2834
XREF	MFSA:2016-49
XREF	MFSA:2016-50
XREF	MFSA:2016-51
XREF	MFSA:2016-52
XREF	MFSA:2016-53
XREF	MFSA:2016-54
XREF	MFSA:2016-55
XREF	MFSA:2016-56
XREF	MFSA:2016-57
XREF	MFSA:2016-58
XREF	MFSA:2016-59
XREF	MFSA:2016-60
XREF	MFSA:2016-61

Plugin Information

Published: 2016/06/09, Modified: 2019/11/19

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 47
```

92755 - Firefox < 48 Multiple Vulnerabilities

Synopsis

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

Description

The version of Firefox installed on the remote Windows host is prior to 48. It is, therefore, affected by multiple vulnerabilities :

- An overflow condition exists in the expat XML parser due to improper validation of user-supplied input when handling malformed input documents. An attacker can exploit this to cause a buffer overflow, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2016-0718)

- An information disclosure vulnerability exists due to a failure to close connections after requesting favicons.

An attacker can exploit this to continue to send requests to the user's browser and disclose sensitive information.(CVE-2016-2830)

- Multiple memory corruption issues exist due to improper validation of user-supplied input. An attacker can exploit these issues to cause a denial of service condition or the execution of arbitrary code.

(CVE-2016-2835, CVE-2016-2836)

- An overflow condition exists in the ClearKey Content Decryption Module (CDM) used by the Encrypted Media Extensions (EME) API due to improper validation of user-supplied input. An attacker can exploit this to cause a buffer overflow, resulting in a denial of service condition or the execution of arbitrary code.

(CVE-2016-2837)

- An overflow condition exists in the ProcessPDI() function in layout/base/nsBidi.cpp due to improper validation of user-supplied input. An 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-2016-2838)

- A flaw exists in the Resource Timing API during page navigation. An attacker can exploit this to disclose sensitive information. (CVE-2016-5250)

- A flaw exists that is triggered when decoding url-encoded values in 'data:' URLs. An attacker can exploit this, via non-ASCII or emoji characters, to spoof the address in the address bar. (CVE-2016-5251)

- An underflow condition exists in the BasePoint4d() function in gfx/2d/Matrix.h due to improper validation of user-supplied input when calculating clipping regions in 2D graphics. A remote attacker can exploit this to cause a stack-based buffer underflow, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2016-5252)

- A flaw in the updater service exists when launched using the callback application path parameter that allows an attacker to escalate privileges. (CVE-2016-5253)

- A use-after-free error exists in the KeyDown() function in layout/xul/nsXULPopupManager.cpp when using the alt key in conjunction with top level menu items. An attacker can exploit this to dereference already freed memory, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2016-5254)

- A use-after-free error exists in the sweep() function that is triggered when handling objects and pointers during incremental garbage collection. An attacker can exploit this to dereference already freed memory, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2016-5255)

- A use-after-free error exists in WebRTC that is triggered when handling DTLS objects. An attacker can exploit this to dereference already freed memory, resulting in a denial of service condition or the execution of arbitrary code. (CVE-2016-5258)

- A use-after-free error exists in the DestroySyncLoop() function in dom/workers/WorkerPrivate.cpp that is triggered when handling nested sync event loops in Service Workers. An attacker can exploit this to dereference already freed memory, resulting in a denial of service condition or the execution of arbitrary code.

(CVE-2016-5259)

- An information disclosure vulnerability exists in the restorableFormNodes() function in XPathGenerator.jsm due to persistently storing passwords in plaintext in session restore data. An attacker can exploit this to disclose password information. (CVE-2016-5260)

- An integer overflow condition exists in the ProcessInput() function in WebSocketChannel.cpp due to improper validation of user-supplied input when handling specially crafted WebSocketChannel packets. An attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-5261)

- A security bypass vulnerability exists due to event handler attributes on a <marquee> tag being executed inside a sandboxed iframe that does not have the allow-scripts flag set. An attacker can exploit this to bypass cross-site scripting protection mechanisms.

(CVE-2016-5262)

- A type confusion flaw exists in the HitTest() function in nsDisplayList.cpp when handling display transformations. An attacker can exploit this to execute arbitrary code. (CVE-2016-5263)

- A use-after-free error exists in the NativeAnonymousChildListChange() function when applying effects to SVG elements. An attacker can exploit this to dereference already freed memory, resulting in a denial of service condition or the execution of arbitrary code.

(CVE-2016-5264)

- A flaw exists in the Redirect() function in nsBaseChannel.cpp that is triggered when a malicious shortcut is called from the same directory as a local HTML file. An attacker can exploit this to bypass the same-origin policy. (CVE-2016-5265)

- A flaw exists due to a failure to properly filter file URIs dragged from a web page to a different piece of software. An attacker can exploit this to disclose sensitive information. (CVE-2016-5266)

- A flaw exists that is triggered when handling certain specific 'about:' URLs that allows an attacker to spoof the contents of system information or error messages (CVE-2016-5268)

- A flaw exists in woff2 that is triggered during the handling of TTC detection. An attacker can exploit this to have an unspecified impact.

- Multiple unspecified flaws exist in woff2 that allow an attacker to cause a denial of service condition.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2016-62/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-63/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-64/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-66/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-67/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-68/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-69/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-70/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-71/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-72/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-73/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-74/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-75/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-76/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-77/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-78/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-79/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-80/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-81/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-83/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-84/

Solution

Upgrade to Firefox version 48 or later.

Risk Factor

High

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)

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	90729

BID	92258
BID	92260
BID	92261
CVE	CVE-2016-0718
CVE	CVE-2016-2830
CVE	CVE-2016-2835
CVE	CVE-2016-2836
CVE	CVE-2016-2837
CVE	CVE-2016-2838
CVE	CVE-2016-5250
CVE	CVE-2016-5251
CVE	CVE-2016-5252
CVE	CVE-2016-5253
CVE	CVE-2016-5254
CVE	CVE-2016-5255
CVE	CVE-2016-5258
CVE	CVE-2016-5259
CVE	CVE-2016-5260
CVE	CVE-2016-5261
CVE	CVE-2016-5262
CVE	CVE-2016-5263
CVE	CVE-2016-5264
CVE	CVE-2016-5265
CVE	CVE-2016-5266
CVE	CVE-2016-5268
XREF	MFSA:2016-62
XREF	MFSA:2016-63
XREF	MFSA:2016-64
XREF	MFSA:2016-66
XREF	MFSA:2016-67
XREF	MFSA:2016-68
XREF	MFSA:2016-69
XREF	MFSA:2016-70
XREF	MFSA:2016-71
XREF	MFSA:2016-72
XREF	MFSA:2016-73
XREF	MFSA:2016-74
XREF	MFSA:2016-75
XREF	MFSA:2016-76
XREF	MFSA:2016-77
XREF	MFSA:2016-78
XREF	MFSA:2016-79
XREF	MFSA:2016-80

XREF	MFSA:2016-81
XREF	MFSA:2016-83
XREF	MFSA:2016-84

Plugin Information

Published: 2016/08/05, Modified: 2019/11/14

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 48
```

95475 - Mozilla Firefox < 50.0.2 nsSMILTimeContainer.cpp SVG Animation RCE

Synopsis

The remote Windows host contains a web browser that is affected by a remote code execution vulnerability.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 50.0.2. It is, therefore, affected by a use-after-free error in dom/smil/nsSMILTimeContainer.cpp when handling SVG animations. An unauthenticated, remote attacker can exploit this issue, via a specially crafted web page, to deference already freed memory, resulting in the execution of arbitrary code.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2016-92/

Solution

Upgrade to Mozilla Firefox version 50.0.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	94591
CVE	CVE-2016-9079
XREF	MFSA:2016-92
XREF	CERT:791496

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2016/12/02, Modified: 2019/11/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 50.0.2
```

100127 - Mozilla Firefox < 53.0.2 ANGLE Graphics Library RCE

Synopsis

The remote Windows host contains a web browser that is affected by a remote code execution vulnerability.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 53.0.2. It is, therefore, affected by a use-after-free error in libANGLE/renderer/d3d/d3d11/Buffer11.cpp within the ANGLE graphics library (libGLES) when handling Buffer11 API calls. An unauthenticated, remote attacker can exploit this, by convincing a user to visit a specially crafted web page, to dereference already freed memory, resulting in a crash or potentially the execution of arbitrary code.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2017-14/

Solution

Upgrade to Mozilla Firefox version 53.0.2 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)

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	98326
CVE	CVE-2017-5031
XREF	MFSA:2017-14

Plugin Information

Published: 2017/05/11, Modified: 2019/11/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 53.0.2
```

105040 - Mozilla Firefox < 57.0.1 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 57.0.1. It is, therefore, affected by multiple vulnerabilities.

Note: CVE-2017-7844 only affects version 57. Earlier releases are not affected.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2017-27/

Solution

Upgrade to Mozilla Firefox version 57.0.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	102039
CVE	CVE-2017-7843
CVE	CVE-2017-7844

Plugin Information

Published: 2017/12/06, Modified: 2019/11/12

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 57.0.1
```

105213 - Mozilla Firefox < 57.0.2 ANGLE Graphics Library RCE

Synopsis

A web browser installed on the remote Windows host is affected by a remote code execution vulnerability.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 57.0.2. It is, therefore, affected by a flaw related to handling Direct 3D 9 drawing and validating elements with the ANGLE graphics library that could allow buffer overflows and potentially code execution.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2017-29/

Solution

Upgrade to Mozilla Firefox version 57.0.2 or later.

Risk Factor

High

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)

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	102115
CVE	CVE-2017-7845
XREF	MFSA:2017-29

Plugin Information

Published: 2017/12/13, Modified: 2018/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 57.0.2
```

110811 - Mozilla Firefox < 61 Multiple Critical Vulnerabilities

Synopsis

A web browser installed on the remote Windows host is affected by multiple critical and high severity vulnerabilities.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 61. It is, therefore, affected by multiple critical and high severity vulnerabilities.

See Also

http://www.nessus.org/u?cf08db1a

Solution

Upgrade to Mozilla Firefox version 61.0.0 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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	104246
BID	104555
BID	104556
BID	104557
BID	104558
BID	104560

BID	104561
BID	104562
CVE	CVE-2018-5156
CVE	CVE-2018-5186
CVE	CVE-2018-5187
CVE	CVE-2018-5188
CVE	CVE-2018-12358
CVE	CVE-2018-12359
CVE	CVE-2018-12360
CVE	CVE-2018-12361
CVE	CVE-2018-12362
CVE	CVE-2018-12363
CVE	CVE-2018-12364
CVE	CVE-2018-12365
CVE	CVE-2018-12366
CVE	CVE-2018-12367
CVE	CVE-2018-12368
CVE	CVE-2018-12369
CVE	CVE-2018-12370
CVE	CVE-2018-12371
XREF	MFSA:2018-15

Plugin Information

Published: 2018/06/29, Modified: 2019/11/04

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 61.0.0
```

117668 - Mozilla Firefox < 62.0.2 Vulnerability

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 62.0.2. It is, therefore, affected by a vulnerability as noted in Mozilla Firefox stable channel update release notes for 2018/09/21. Please refer to the release notes for additional information. Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?c7fa8df5

http://www.nessus.org/u?a35eec72

Solution

Upgrade to Mozilla Firefox version 62.0.2 or later.

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)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2018-12385

Plugin Information

Published: 2018/09/24, Modified: 2019/11/01

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 62.0.2
```

118397 - Mozilla Firefox < 63 Multiple Vulnerabilities

Synopsis

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

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 63. It is, therefore, affected by multiple vulnerabilities :

- During HTTP Live Stream playback on Firefox for Android, audio data can be accessed across origins in violation of security policies. Because the problem is in the underlying Android service, this issue is addressed by treating all HLS streams as cross-origin and opaque to access. *Note: this issue only affects Firefox for Android. Desktop versions of Firefox are unaffected.* (CVE-2018-12391)

- When manipulating user events in nested loops while opening a document through script, it is possible to trigger a potentially exploitable crash due to poor event handling. (CVE-2018-12392)

- A potential vulnerability was found in 32-bit builds where an integer overflow during the conversion of scripts to an internal UTF-16 representation could result in allocating a buffer too small for the conversion. This leads to a possible out-of-bounds write. *Note: 64-bit builds are not vulnerable to this issue.* (CVE-2018-12393)

- By rewriting the Host request headers using the webRequest API, a WebExtension can bypass domain restrictions through domain fronting. This would allow access to domains that share a host that are otherwise restricted. (CVE-2018-12395)

- A vulnerability where a WebExtension can run content scripts in disallowed contexts following navigation or other events. This allows for potential privilege escalation by the WebExtension on sites where content scripts should not be run. (CVE-2018-12396)

- A WebExtension can request access to local files without the warning prompt stating that the extension will 'Access your data for all websites' being displayed to the user. This allows extensions to run content scripts in local pages without permission warnings when a local file is opened. (CVE-2018-12397)

- By using the reflected URL in some special resource URIs, such as chrome:, it is possible to inject stylesheets and bypass Content Security Policy (CSP). (CVE-2018-12398)

- When a new protocol handler is registered, the API accepts a title argument which can be used to mislead users about which domain is registering the new protocol. This may result in the user approving a protocol handler that they otherwise would not have.

(CVE-2018-12399)

- In private browsing mode on Firefox for Android, favicons are cached in the cache/icons folder as they are in non-private mode.

This allows information leakage of sites visited during private browsing sessions. *Note: this issue only affects Firefox for Android. Desktop versions of Firefox are unaffected.* (CVE-2018-12400)

- Some special resource URIs will cause a non-exploitable crash if loaded with optional parameters following a '?' in the parsed string. This could lead to denial of service (DOS) attacks.

(CVE-2018-12401)

- SameSite cookies are sent on cross-origin requests when the 'Save Page As...' menu item is selected to save a page, violating cookie policy. This can result in saving the wrong version of resources based on those cookies. (CVE-2018-12402)

- If a site is loaded over a HTTPS connection but loads a favicon resource over HTTP, the mixed content warning is not displayed to users. (CVE-2018-12403)

- Mozilla developers and community members Christian Holler, Dana Keeler, Ronald Crane, Marcia Knous, Tyson Smith, Daniel Veditz, and Steve Fink reported memory safety bugs present in Firefox 62.

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-2018-12388)

- Mozilla developers and community members Christian Holler, Bob Owen, Boris Zbarsky, Calixte Denizet, Jason Kratzer, Jed Davis, Taegeon Lee, Philipp, Ronald Crane, Raul Gurzau, Gary Kwong, Tyson Smith, Raymond Forbes, and Bogdan Tara reported memory safety bugs present in Firefox 62 and Firefox ESR 60.2. 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-2018-12390)

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

See Also

http://www.nessus.org/u?dc2c2cb7

http://www.nessus.org/u?1c645d5e

http://www.nessus.org/u?62d886c6

http://www.nessus.org/u?614520ad

http://www.nessus.org/u?99f950cc

http://www.nessus.org/u?9811edbe

http://www.nessus.org/u?a6969f4f

http://www.nessus.org/u?4146eabd

http://www.nessus.org/u?ec6f6183

http://www.nessus.org/u?8089c07f

http://www.nessus.org/u?dd1081d2

http://www.nessus.org/u?cf41751c

http://www.nessus.org/u?a30fef4e

http://www.nessus.org/u?75a288c2

http://www.nessus.org/u?ca6d9c31

http://www.nessus.org/u?a5c1931e

http://www.nessus.org/u?56a8a5aa

http://www.nessus.org/u?10a58f5f

http://www.nessus.org/u?ce604af2

http://www.nessus.org/u?56bedc2c

http://www.nessus.org/u?0940e1a6

http://www.nessus.org/u?16df5cdc

http://www.nessus.org/u?2fa35353
http://www.nessus.org/u?984d8e82
http://www.nessus.org/u?9ce74e28
http://www.nessus.org/u?6af37c5b
http://www.nessus.org/u?5a6c0ca4
http://www.nessus.org/u?55d351a5
http://www.nessus.org/u?82482803
http://www.nessus.org/u?e7bb037e
http://www.nessus.org/u?a6a9565b
http://www.nessus.org/u?5daf782e
http://www.nessus.org/u?166aa054
http://www.nessus.org/u?a933cb35
http://www.nessus.org/u?39935a02
http://www.nessus.org/u?c5b58d2f
http://www.nessus.org/u?f6925998
http://www.nessus.org/u?a31d3226
http://www.nessus.org/u?b3a7cc16
http://www.nessus.org/u?ef389f56
http://www.nessus.org/u?6eea10ba

Solution

Upgrade to Mozilla Firefox version 63 or later.

Risk Factor

High

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)

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-2018-12388
CVE	CVE-2018-12390
CVE	CVE-2018-12391
CVE	CVE-2018-12392
CVE	CVE-2018-12393
CVE	CVE-2018-12395
CVE	CVE-2018-12396
CVE	CVE-2018-12397
CVE	CVE-2018-12398
CVE	CVE-2018-12399
CVE	CVE-2018-12400
CVE	CVE-2018-12401
CVE	CVE-2018-12402
CVE	CVE-2018-12403

Plugin Information

Published: 2018/10/25, Modified: 2019/11/01

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 63.0.0
```

122233 - Mozilla Firefox < 65.0.1

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 65.0.1. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2019-04 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)

- Cross-origin images can be read from a canvas element in violation of the same- origin policy using the transferFromImageBitmap method. *Note:

This only affects Firefox 65. Previous versions are unaffected.* (CVE-2018-18511)

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/mfsa2019-04/

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=1526218

Solution

Upgrade to Mozilla Firefox version 65.0.1 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)

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-2018-18356
CVE	CVE-2018-18511
CVE	CVE-2019-5785
XREF	MFSA:2019-04

Plugin Information

Published: 2019/02/15, Modified: 2019/10/31

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 65.0.1
```

123012 - Mozilla Firefox < 66.0.1

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 66.0.1. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2019-09 advisory.

- Incorrect alias information in IonMonkey JIT compiler for Array.prototype.slice method may lead to missing bounds check and a buffer overflow. (CVE-2019-9810)

- Incorrect handling of __proto__ mutations may lead to type confusion in IonMonkey JIT code and can be leveraged for arbitrary memory read and write.

(CVE-2019-9813)

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/mfsa2019-09/

Solution

Upgrade to Mozilla Firefox version 66.0.1 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

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

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-2019-9810
CVE	CVE-2019-9813
XREF	MFSA:2019-09

Plugin Information

Published: 2019/03/22, Modified: 2020/01/31

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 66.0.1
```

126002 - Mozilla Firefox < 67.0.3

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 67.0.3. It is, therefore, affected by a vulnerability as referenced in the mfsa2019-18 advisory.

- A type confusion vulnerability can occur when manipulating JavaScript objects due to issues in Array.pop. This can allow for an exploitable crash. We are aware of targeted attacks in the wild abusing this flaw. (CVE-2019-11707)

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/mfsa2019-18/

Solution

Upgrade to Mozilla Firefox version 67.0.3 or later.

Risk Factor

High

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)

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-2019-11707

XREF	MFSA:2019-18
XREF	CISA-KNOWN-EXPLOITED:2022/06/13

Plugin Information

Published: 2019/06/18, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 67.0.3
```

130170 - Mozilla Firefox < 70.0 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 70.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2019-34 advisory, including the following:

- Incorrect derivation of a packet length in WebRTC in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file. (CVE-2018-6156)

- In libexpat before 2.2.8, crafted XML input could fool the parser into changing from DTD parsing to document parsing too early; a consecutive call to XML_GetCurrentLineNumber (or XML_GetCurrentColumnNumber) then resulted in a heap-based buffer over-read. (CVE-2019-15903)

- When storing a value in IndexedDB, the value's prototype chain is followed and it was possible to retain a reference to a locale, delete it, and subsequently reference it. This resulted in a use-after-free and a potentially exploitable crash. (CVE-2019-11757)

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/mfsa2019-34/

Solution

Upgrade to Mozilla Firefox version 70.0 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)

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

II

References

BID	104887
CVE	CVE-2018-6156
CVE	CVE-2019-11757
CVE	CVE-2019-11759
CVE	CVE-2019-11760
CVE	CVE-2019-11761
CVE	CVE-2019-11762
CVE	CVE-2019-11763
CVE	CVE-2019-11764
CVE	CVE-2019-11765
CVE	CVE-2019-15903
CVE	CVE-2019-17000
CVE	CVE-2019-17001
CVE	CVE-2019-17002
XREF	MFSA:2019-34
XREF	IAVA:2019-A-0395-S

Plugin Information

Published: 2019/10/24, Modified: 2021/06/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 70.0
```

131773 - Mozilla Firefox < 71.0

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 71.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2019-36 advisory.

- When encrypting with a block cipher, if a call to NSC_EncryptUpdate was made with data smaller than the block size, a small out of bounds write could occur. This could have caused heap corruption and a potentially exploitable crash. (CVE-2019-11745)

- Improper refcounting of soft token session objects could cause a use-after-free and crash (likely limited to a denial of service). (CVE-2019-11756)

- When setting a thread name on Windows in WebRTC, an incorrect number of arguments could have been supplied, leading to stack corruption and a potentially exploitable crash.

Note: this issue only occurs on Windows. Other operating systems are unaffected. (CVE-2019-13722)

- When using nested workers, a use-after-free could occur during worker destruction. This resulted in a potentially exploitable crash. (CVE-2019-17008)

- When running, the updater service wrote status and log files to an unrestricted location; potentially allowing an unprivileged process to locate and exploit a vulnerability in file handling in the updater service.

- Note: This attack requires local system access and only affects Windows. Other operating systems are not affected.

(CVE-2019-17009)

- Under certain conditions, when checking the Resist Fingerprinting preference during device orientation checks, a race condition could have caused a use-after-free and a potentially exploitable crash. (CVE-2019-17010)

- Under certain conditions, when retrieving a document from a DocShell in the antitracking code, a race condition could cause a use-after-free condition and a potentially exploitable crash. (CVE-2019-17011)

- Mozilla developers Christoph Diehl, Nathan Froyd, Jason Kratzer, Christian Holler, Karl Tomlinson, Tyson Smith reported memory safety bugs present in Firefox 70 and Firefox ESR 68.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.

(CVE-2019-17012)

- Mozilla developers and community members Philipp, Diego Calleja, Mikhail Gavrilov, Jason Kratzer, Christian Holler, Markus Stange, Tyson Smith reported memory safety bugs present in Firefox 70. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2019-17013)

- If an image had not loaded correctly (such as when it is not actually an image), it could be dragged and dropped cross-domain, resulting in a cross-origin information leak.

(CVE-2019-17014) 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/mfsa2019-36/

Solution

Upgrade to Mozilla Firefox version 71.0 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)

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-2019-11745
CVE	CVE-2019-11756
CVE	CVE-2019-13722
CVE	CVE-2019-17005
CVE	CVE-2019-17008
CVE	CVE-2019-17009
CVE	CVE-2019-17010
CVE	CVE-2019-17011
CVE	CVE-2019-17012
CVE	CVE-2019-17013
CVE	CVE-2019-17014
XREF	MFSA:2019-36

Plugin Information

Published: 2019/12/06, Modified: 2020/01/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 71.0
```

132709 - Mozilla Firefox < 72.0 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 72.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-01 advisory, including the following:

- During the initialization of a new content process, a pointer offset can be manipulated leading to memory corruption and a potentially exploitable crash in the parent process. (CVE-2019-17015)

- When pasting a <style> tag from the clipboard into a rich text editor, the CSS sanitizer incorrectly rewrites a @namespace rule. This could allow for injection into certain types of websites resulting in data exfiltration. (CVE-2019-17016)

- Due to a missing case handling object types, a type confusion vulnerability could occur, resulting in a crash. We presume that with enough effort that it could be exploited to run arbitrary code.

(CVE-2019-17017)

- When in Private Browsing Mode on Windows 10, the Windows keyboard may retain word suggestions to improve the accuracy of the keyboard. (CVE-2019-17018)

- When Python was installed on Windows, a python file being served with the MIME type of text/plain could be executed by Python instead of being opened as a text file when the Open option was selected upon download. (CVE-2019-17019)

- If an XML file is served with a Content Security Policy and the XML file includes an XSL stylesheet, the Content Security Policy will not be applied to the contents of the XSL stylesheet. If the XSL sheet e.g.

includes JavaScript, it would bypass any of the restrictions of the Content Security Policy applied to the XML document. (CVE-2019-17020)

- During the initialization of a new content process, a race condition occurs that can allow a content process to disclose heap addresses from the parent process. (CVE-2019-17021)

- When pasting a <style> tag from the clipboard into a rich text editor, the CSS sanitizer does not escape < and > characters. Because the resulting string is pasted directly into the text node of the element this does not result in a direct injection into the webpage; however, if a webpage subsequently copies the node's innerHTML, assigning it to another innerHTML, this would result in an XSS vulnerability. Two WYSIWYG editors were identified with this behavior, more may exist. (CVE-2019-17022)

- After a HelloRetryRequest has been sent, the client may negotiate a lower protocol that TLS 1.3, resulting in an invalid state transition in the TLS State Machine. If the client gets into this state, incoming Application Data records will be ignored. (CVE-2019-17023)

- Mozilla developers Jason Kratzer, Christian Holler, and Bob Clary reported memory safety bugs present in Firefox 71 and Firefox ESR 68.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2019-17024)

- Mozilla developers Karl Tomlinson, Jason Kratzer, Tyson Smith, Jon Coppeard, and Christian Holler reported memory safety bugs present in Firefox 71. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2019-17025)

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/mfsa2020-01/

Solution

Upgrade to Mozilla Firefox version 72.0 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)

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-2019-17015
CVE	CVE-2019-17016
CVE	CVE-2019-17017
CVE	CVE-2019-17018
CVE	CVE-2019-17019
CVE	CVE-2019-17020
CVE	CVE-2019-17021
CVE	CVE-2019-17022
CVE	CVE-2019-17023
CVE	CVE-2019-17024
CVE	CVE-2019-17025
XREF	MFSA:2020-01

Plugin Information

Published: 2020/01/08, Modified: 2020/02/14

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 72.0
```

132715 - Mozilla Firefox < 72.0.1

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 72.0.1.

It is, therefore, affected by the vulnerability as referenced in the mfsa2020-03 advisory.

- Incorrect alias information in IonMonkey JIT compiler for setting array elements could lead to a type confusion. We are aware of targeted attacks in the wild abusing this flaw. (CVE-2019-17026)

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/mfsa2020-03/

Solution

Upgrade to Mozilla Firefox version 72.0.1 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

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

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-2019-17026
XREF	MFSA:2020-03

XREF CISA-KNOWN-EXPLOITED:2022/05/03

Plugin Information

Published: 2020/01/08, Modified: 2021/11/30

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 72.0.1
```

133693 - Mozilla Firefox < 73.0

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 73.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-05 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/mfsa2020-05/

Solution

Upgrade to Mozilla Firefox version 73.0 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)

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
CVE	CVE-2020-6801
XREF	MFSA:2020-05
XREF	IAVA:2020-A-0072-S

Plugin Information

Published: 2020/02/14, Modified: 2020/05/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 73.0
```

135202 - Mozilla Firefox < 74.0.1

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 74.0.1. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-11 advisory.

- Under certain conditions, when running the nsDocShell destructor, a race condition can cause a use-after-free.

We are aware of targeted attacks in the wild abusing this flaw. (CVE-2020-6819)

- Under certain conditions, when handling a ReadableStream, a race condition can cause a use-after- free. We are aware of targeted attacks in the wild abusing this flaw. (CVE-2020-6820)

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/mfsa2020-11/

Solution

Upgrade to Mozilla Firefox version 74.0.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

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

II

References

CVE	CVE-2020-6819
CVE	CVE-2020-6820
XREF	MFSA:2020-11
XREF	IAVA:2020-A-0128-S
XREF	CISA-KNOWN-EXPLOITED:2022/05/03

Plugin Information

Published: 2020/04/06, Modified: 2022/01/24

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 74.0.1
```

137049 - Mozilla Firefox < 77.0

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 77.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-20 advisory.

- NSS has shown timing differences when performing DSA signatures, which was exploitable and could eventually leak private keys. (CVE-2020-12399)

- When browsing a malicious page, a race condition in our SharedWorkerService could occur and lead to a potentially exploitable crash. (CVE-2020-12405)

- Mozilla Developer Iain Ireland discovered a missing type check during unboxed objects removal, resulting in a crash. We presume that with enough effort that it could be exploited to run arbitrary code. (CVE-2020-12406)

- Mozilla Developer Nicolas Silva found that when using WebRender, Firefox would under certain conditions leak arbitrary GPU memory to the visible screen. The leaked memory content was visible to the user, but not observable from web content. (CVE-2020-12407)

- When browsing a document hosted on an IP address, an attacker could insert certain characters to flip domain and path information in the address bar.

(CVE-2020-12408)

- Mozilla developers Tom Tung and Karl Tomlinson reported memory safety bugs present in Firefox 76 and Firefox ESR 68.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2020-12409)

- Mozilla developers :Gijs (he/him), Randell Jesup reported memory safety bugs present in Firefox 76. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.

(CVE-2020-12411)

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/mfsa2020-20/

Solution

Upgrade to Mozilla Firefox version 77.0 or later.

Risk Factor

High

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)

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)

STIG Severity

I

References

CVE	CVE-2020-12399
CVE	CVE-2020-12405
CVE	CVE-2020-12406
CVE	CVE-2020-12407
CVE	CVE-2020-12408
CVE	CVE-2020-12409
CVE	CVE-2020-12411
XREF	MFSA:2020-20
XREF	IAVA:2020-A-0238-S

Plugin Information

Published: 2020/06/02, Modified: 2020/07/13

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 77.0
```

138085 - Mozilla Firefox < 78.0

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 78.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-24 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/mfsa2020-24/

Solution

Upgrade to Mozilla Firefox version 78.0 or later.

Risk Factor

High

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)

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)

STIG Severity

I

References

CVE	CVE-2020-12402
CVE	CVE-2020-12415

CVE	CVE-2020-12416
CVE	CVE-2020-12417
CVE	CVE-2020-12418
CVE	CVE-2020-12419
CVE	CVE-2020-12420
CVE	CVE-2020-12421
CVE	CVE-2020-12422
CVE	CVE-2020-12423
CVE	CVE-2020-12424
CVE	CVE-2020-12425
CVE	CVE-2020-12426
XREF	MFSA:2020-24
XREF	IAVA:2020-A-0287-S

Plugin Information

Published: 2020/07/02, Modified: 2020/07/31

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 78.0
```

139040 - Mozilla Firefox < 79.0

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 79.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-30 advisory.

- Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to potentially exploit heap corruption via a crafted SCTP stream. (CVE-2020-6514)

- Use after free in ANGLE in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

(CVE-2020-6463)

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/mfsa2020-30/

Solution

Upgrade to Mozilla Firefox version 79.0 or later.

Risk Factor

High

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)

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)

STIG Severity

I

References

CVE	CVE-2020-6463
CVE	CVE-2020-6514
CVE	CVE-2020-15652
CVE	CVE-2020-15653
CVE	CVE-2020-15654
CVE	CVE-2020-15655
CVE	CVE-2020-15656
CVE	CVE-2020-15657
CVE	CVE-2020-15658
CVE	CVE-2020-15659
XREF	MFSA:2020-30
XREF	IAVA:2020-A-0344-S

Plugin Information

Published: 2020/07/28, Modified: 2020/08/28

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 79.0
```

139789 - Mozilla Firefox < 80.0

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 80.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-36 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/mfsa2020-36/

Solution

Upgrade to Mozilla Firefox version 80.0 or later.

Risk Factor

High

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)

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)

STIG Severity

I

References

CVE	CVE-2020-6829
CVE	CVE-2020-12400

CVE	CVE-2020-12401
CVE	CVE-2020-15663
CVE	CVE-2020-15664
CVE	CVE-2020-15665
CVE	CVE-2020-15666
CVE	CVE-2020-15667
CVE	CVE-2020-15668
CVE	CVE-2020-15670
XREF	MFSA:2020-36
XREF	IAVA:2020-A-0391-S

Plugin Information

Published: 2020/08/25, Modified: 2020/10/14

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 80.0
```

140732 - Mozilla Firefox < 81.0

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 81.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-42 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/mfsa2020-42/

Solution

Upgrade to Mozilla Firefox version 81.0 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)

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-2020-15673
CVE	CVE-2020-15674

CVE	CVE-2020-15675
CVE	CVE-2020-15676
CVE	CVE-2020-15677
CVE	CVE-2020-15678
XREF	MFSA:2020-42
XREF	IAVA:2020-A-0435-S

Plugin Information

Published: 2020/09/22, Modified: 2020/10/30

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 81.0
```

142613 - Mozilla Firefox < 82.0.3

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 82.0.3. It is, therefore, affected by a vulnerability as referenced in the mfsa2020-49 advisory.

- In certain circumstances, the MCallGetProperty opcode can be emitted with unmet assumptions resulting in an exploitable use-after-free condition. (CVE-2020-26950)

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/mfsa2020-49/

Solution

Upgrade to Mozilla Firefox version 82.0.3 or later.

Risk Factor

High

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)

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-2020-26950
XREF	MFSA:2020-49
XREF	IAVA:2020-A-0531-S

Exploitable With

Metasploit (true)

Plugin Information

Published: 2020/11/09, Modified: 2022/03/01

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 82.0.3
```

142910 - Mozilla Firefox < 83.0

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 83.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2020-50 advisory, including the following:

- Mozilla developers reported memory safety bugs present in Firefox 82. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 83. (CVE-2020-26969)

- If the Compact() method was called on an nsTArray, the array could have been reallocated without updating other pointers, leading to a potential use-after-free and exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. (CVE-2020-26960)

- Mozilla developers reported memory safety bugs present in Firefox 82 and Firefox ESR 78.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5. (CVE-2020-26968)

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/mfsa2020-50/

Solution

Upgrade to Mozilla Firefox version 83.0 or later.

Risk Factor

High

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)

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)

STIG Severity

I

References

CVE	CVE-2020-15999
CVE	CVE-2020-16012
CVE	CVE-2020-26951
CVE	CVE-2020-26952
CVE	CVE-2020-26953
CVE	CVE-2020-26954
CVE	CVE-2020-26955
CVE	CVE-2020-26956
CVE	CVE-2020-26957
CVE	CVE-2020-26958
CVE	CVE-2020-26959
CVE	CVE-2020-26960
CVE	CVE-2020-26961
CVE	CVE-2020-26962
CVE	CVE-2020-26963
CVE	CVE-2020-26964
CVE	CVE-2020-26965
CVE	CVE-2020-26966
CVE	CVE-2020-26967
CVE	CVE-2020-26968
CVE	CVE-2020-26969
XREF	MFSA:2020-50
XREF	IAVA:2020-A-0537-S
XREF	CISA-KNOWN-EXPLOITED:2021/11/17

Plugin Information

Published: 2020/11/17, Modified: 2021/11/30

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
```

```
    Fixed version     : 83.0
```

144771 - Mozilla Firefox < 84.0.2

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 84.0.2. It is, therefore, affected by a vulnerability as referenced in the mfsa2021-01 advisory.

- A malicious peer could have modified a COOKIE-ECHO chunk in a SCTP packet in a way that potentially resulted in a use-after-free. We presume that with enough effort it could have been exploited to run arbitrary code. (CVE-2020-16044)

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/mfsa2021-01/

Solution

Upgrade to Mozilla Firefox version 84.0.2 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)

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-2020-16044
XREF	IAVA:2021-A-0005-S

Plugin Information

Published: 2021/01/06, Modified: 2021/08/12

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 84.0.2
```

145465 - Mozilla Firefox < 85.0

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 85.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-03 advisory.

- If a user clicked into a specifically crafted PDF, the PDF reader could be confused into leaking cross- origin information, when said information is served as chunked data. (CVE-2021-23953)

- Using the new logical assignment operators in a JavaScript switch statement could have caused a type confusion, leading to a memory corruption and a potentially exploitable crash. (CVE-2021-23954)

- The browser could have been confused into transferring a pointer lock state into another tab, which could have lead to clickjacking attacks. (CVE-2021-23955)

- An ambiguous file picker design could have confused users who intended to select and upload a single file into uploading a whole directory. This was addressed by adding a new prompt. (CVE-2021-23956)

- Navigations through the Android-specific `intent` URL scheme could have been misused to escape iframe sandbox.Note: This issue only affected Firefox for Android. Other operating systems are unaffected.

(CVE-2021-23957)

- The browser could have been confused into transferring a screen sharing state into another tab, which would leak unintended information. (CVE-2021-23958)

- An XSS bug in internal error pages could have led to various spoofing attacks, including other error pages and the address bar.Note: This issue only affected Firefox for Android. Other operating systems are unaffected. (CVE-2021-23959)

- Performing garbage collection on re-declared JavaScript variables resulted in a user-after-poison, and a potentially exploitable crash. (CVE-2021-23960)

- Further techniques that built on the slipstream research combined with a malicious webpage could have exposed both an internal network's hosts as well as services running on the user's local machine.

(CVE-2021-23961)

- Incorrect use of the RowCountChanged method could have led to a user-after-poison and a potentially exploitable crash. (CVE-2021-23962)

- When sharing geolocation during an active WebRTC share, Firefox could have reset the webRTC sharing state in the user interface, leading to loss of control over the currently granted permission (CVE-2021-23963)

- Mozilla developers Andrew McCreight, Tyson Smith, Jesse Schwartzentruber, Jon Coppeard, Byron Campen, Andr Bargull, Steve Fink, Jason Kratzer, Christian Holler, Alexis Beingessner reported memory safety bugs present in Firefox 84 and Firefox ESR 78.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.

(CVE-2021-23964)

- Mozilla developers Sebastian Hengst, Christian Holler, Tyson Smith reported memory safety bugs present in Firefox 84. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-23965)

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/mfsa2021-03/

Solution

Upgrade to Mozilla Firefox version 85.0 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)

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-2021-23953
CVE	CVE-2021-23954
CVE	CVE-2021-23955
CVE	CVE-2021-23956
CVE	CVE-2021-23957
CVE	CVE-2021-23958
CVE	CVE-2021-23959
CVE	CVE-2021-23960

CVE	CVE-2021-23961
CVE	CVE-2021-23962
CVE	CVE-2021-23963
CVE	CVE-2021-23964
CVE	CVE-2021-23965
XREF	IAVA:2021-A-0051-S
XREF	IAVA:2021-A-0185-S

Plugin Information

Published: 2021/01/27, Modified: 2021/08/23

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 85.0
```

146780 - Mozilla Firefox < 86.0

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 86.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-07 advisory.

- As specified in the W3C Content Security Policy draft, when creating a violation report, User agents need to ensure that the source file is the URL requested by the page, pre-redirects. If thats not possible, user agents need to strip the URL down to an origin to avoid unintentional leakage. Under certain types of redirects, Firefox incorrectly set the source file to be the destination of the redirects. This was fixed to be the redirect destination's origin. (CVE-2021-23969)

- Context-specific code was included in a shared jump table; resulting in assertions being triggered in multithreaded wasm code. (CVE-2021-23970)

- If Content Security Policy blocked frame navigation, the full destination of a redirect served in the frame was reported in the violation report; as opposed to the original frame URI. This could be used to leak sensitive information contained in such URIs. (CVE-2021-23968)

- The DOMParser API did not properly process <noscript> elements for escaping. This could be used as an mXSS vector to bypass an HTML Sanitizer. (CVE-2021-23974)

- When processing a redirect with a conflicting Referrer-Policy, Firefox would have adopted the redirect's Referrer-Policy. This would have potentially resulted in more information than intended by the original origin being provided to the destination of the redirect. (CVE-2021-23971)

- When accepting a malicious intent from other installed apps, Firefox for Android accepted manifests from arbitrary file paths and allowed declaring webapp manifests for other origins. This could be used to gain fullscreen access for UI spoofing and could also lead to cross-origin attacks on targeted websites.Note: This issue is a different issue from CVE-2020-26954 and only affected Firefox for Android. Other operating systems are unaffected. (CVE-2021-23976)

- Firefox for Android suffered from a time-of-check-time-of-use vulnerability that allowed a malicious application to read sensitive data from application directories.Note: This issue is only affected Firefox for Android. Other operating systems are unaffected. (CVE-2021-23977)

- One phishing tactic on the web is to provide a link with HTTP Auth. For example https://www.phishingtarget.com@evil.com. To mitigate this type of attack, Firefox will display a warning dialog; however, this warning dialog would not have been displayed if evil.com used a redirect that was cached by the browser. (CVE-2021-23972)

- The developer page about:memory has a Measure function for exploring what object types the browser has allocated and their sizes. When this function was invoked; we incorrectly called the sizeof function, instead of using the API method that checks for invalid pointers. (CVE-2021-23975)

- When trying to load a cross-origin resource in an audio/video context a decoding error may have resulted, and the content of that error may have revealed information about the resource. (CVE-2021-23973)

- Mozilla developers Alexis Beingessner, Tyson Smith, Nika Layzell, and Mats Palmgren reported memory safety bugs present in Firefox 85 and Firefox ESR 78.7. Some of these bugs showed evidence of memory

corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.

(CVE-2021-23978)

- Mozilla developers Tyson Smith, Lars T Hansen, Valentin Gosu, and Sebastian Hengst reported memory safety bugs present in Firefox 85. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-23979)

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/mfsa2021-07/

Solution

Upgrade to Mozilla Firefox version 86.0 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)

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-2021-23968
CVE	CVE-2021-23969
CVE	CVE-2021-23970
CVE	CVE-2021-23971

CVE	CVE-2021-23972
CVE	CVE-2021-23973
CVE	CVE-2021-23974
CVE	CVE-2021-23975
CVE	CVE-2021-23976
CVE	CVE-2021-23977
CVE	CVE-2021-23978
CVE	CVE-2021-23979
XREF	IAVA:2021-A-0107-S

Plugin Information

Published: 2021/02/23, Modified: 2021/06/03

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 86.0
```

148014 - Mozilla Firefox < 87.0

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 87.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-10 advisory.

- A texture upload of a Pixel Buffer Object could have confused the WebGL code to skip binding the buffer used to unpack it, resulting in memory corruption and a potentially exploitable information leak or crash.

(CVE-2021-23981)

- Using techniques that built on the slipstream research, a malicious webpage could have scanned both an internal network's hosts as well as services running on the user's local machine utilizing WebRTC connections. (CVE-2021-23982)

- By causing a transition on a parent node by removing a CSS rule, an invalid property for a marker could have been applied, resulting in memory corruption and a potentially exploitable crash. (CVE-2021-23983)

- A malicious extension could have opened a popup window lacking an address bar. The title of the popup lacking an address bar should not be fully controllable, but in this situation was. This could have been used to spoof a website and attempt to trick the user into providing credentials. (CVE-2021-23984)

- If an attacker is able to alter specific about:config values (for example malware running on the user's computer), the Devtools remote debugging feature could have been enabled in a way that was unnoticable to the user. This would have allowed a remote attacker (able to make a direct network connection to the victim) to monitor the user's browsing activity and (plaintext) network traffic. This was addressed by providing a visual cue when Devtools has an open network socket. (CVE-2021-23985)

- A malicious extension with the 'search' permission could have installed a new search engine whose favicon referenced a cross-origin URL. The response to this cross-origin request could have been read by the extension, allowing a same-origin policy bypass by the extension, which should not have cross-origin permissions. This cross-origin request was made without cookies, so the sensitive information disclosed by the violation was limited to local-network resources or resources that perform IP-based authentication.

(CVE-2021-23986)

- Mozilla developers and community members Matthew Gregan, Tyson Smith, Julien Wajsberg, and Alexis Beingessner reported memory safety bugs present in Firefox 86 and Firefox ESR 78.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-23987)

- Mozilla developers Tyson Smith and Christian Holler reported memory safety bugs present in Firefox 86.

Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-23988)

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/mfsa2021-10/

Solution

Upgrade to Mozilla Firefox version 87.0 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)

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-2021-23981
CVE	CVE-2021-23982
CVE	CVE-2021-23983
CVE	CVE-2021-23984
CVE	CVE-2021-23985
CVE	CVE-2021-23986
CVE	CVE-2021-23987
CVE	CVE-2021-23988
XREF	IAVA:2021-A-0144-S

Plugin Information

Published: 2021/03/23, Modified: 2021/06/03

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
  Fixed version     : 87.0
```

148767 - Mozilla Firefox < 88.0

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 88.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-16 advisory.

- A WebGL framebuffer was not initialized early enough, resulting in memory corruption and an out of bound write. (CVE-2021-23994)

- When Responsive Design Mode was enabled, it used references to objects that were previously freed. We presume that with enough effort this could have been exploited to run arbitrary code. (CVE-2021-23995)

- By utilizing 3D CSS in conjunction with Javascript, content could have been rendered outside the webpage's viewport, resulting in a spoofing attack that could have been used for phishing or other attacks on a user. (CVE-2021-23996)

- Due to unexpected data type conversions, a use-after-free could have occurred when interacting with the font cache. We presume that with enough effort this could have been exploited to run arbitrary code.

(CVE-2021-23997)

- Through complicated navigations with new windows, an HTTP page could have inherited a secure lock icon from an HTTPS page. (CVE-2021-23998)

- If a Blob URL was loaded through some unusual user interaction, it could have been loaded by the System Principal and granted additional privileges that should not be granted to web content. (CVE-2021-23999)

- A race condition with requestPointerLock() and setTimeout() could have resulted in a user interacting with one tab when they believed they were on a separate tab. In conjunction with certain elements (such as <input type=file>) this could have led to an attack where a user was confused about the origin of the webpage and potentially disclosed information they did not intend to. (CVE-2021-24000)

- A compromised content process could have performed session history manipulations it should not have been able to due to testing infrastructure that was not restricted to testing-only configurations.

(CVE-2021-24001)

- When a user clicked on an FTP URL containing encoded newline characters (%0A and %0D), the newlines would have been interpreted as such and allowed arbitrary commands to be sent to the FTP server.

(CVE-2021-24002)

- The WebAssembly JIT could miscalculate the size of a return type, which could lead to a null read and result in a crash. Note: This issue only affected x86-32 platforms. Other platforms are unaffected.

(CVE-2021-29945)

- Lack of escaping allowed HTML injection when a webpage was viewed in Reader View. While a Content Security Policy prevents direct code execution, HTML injection is still possible.Note: This issue only affected Firefox for Android. Other operating systems are unaffected. (CVE-2021-29944)

- Ports that were written as an integer overflow above the bounds of a 16-bit integer could have bypassed port blocking restrictions when used in the Alt-Svc header. (CVE-2021-29946)

- Mozilla developers and community members Ryan VanderMeulen, Sean Feng, Tyson Smith, Julian Seward, Christian Holler reported memory safety bugs present in Firefox 87. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29947)

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/mfsa2021-16/

Solution

Upgrade to Mozilla Firefox version 88.0 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)

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

II

References

CVE	CVE-2021-23994
CVE	CVE-2021-23995
CVE	CVE-2021-23996
CVE	CVE-2021-23997
CVE	CVE-2021-23998
CVE	CVE-2021-23999
CVE	CVE-2021-24000

CVE	CVE-2021-24001
CVE	CVE-2021-24002
CVE	CVE-2021-29944
CVE	CVE-2021-29945
CVE	CVE-2021-29946
CVE	CVE-2021-29947
XREF	IAVA:2021-A-0185-S

Plugin Information

Published: 2021/04/19, Modified: 2021/08/19

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 88.0
```

149281 - Mozilla Firefox < 88.0.1

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 88.0.1. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-20 advisory.

- A malicious webpage could have forced a Firefox for Android user into executing attacker-controlled JavaScript in the context of another domain, resulting in a Universal Cross-Site Scripting vulnerability.Note: This issue only affected Firefox for Android. Other operating systems are unaffected. Further details are being temporarily withheld to allow users an opportunity to update.

(CVE-2021-29953)

- When Web Render components were destructed, a race condition could have caused undefined behavior, and we presume that with enough effort may have been exploitable to run arbitrary code. (CVE-2021-29952)

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/mfsa2021-20/

Solution

Upgrade to Mozilla Firefox version 88.0.1 or later.

Risk Factor

Medium

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)

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-2021-29952
CVE	CVE-2021-29953
XREF	IAVA:2021-A-0214-S

Plugin Information

Published: 2021/05/05, Modified: 2021/06/28

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 88.0.1
```

150119 - Mozilla Firefox < 89.0

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 89.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-23 advisory.

- A malicious website that causes an HTTP Authentication dialog to be spawned could trick the built-in password manager to suggest passwords for the currently active website instead of the website that triggered the dialog. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29965)

- Firefox used to cache the last filename used for printing a file. When generating a filename for printing, Firefox usually suggests the web page title. The caching and suggestion techniques combined may have lead to the title of a website visited during private browsing mode being stored on disk. (CVE-2021-29960)

- When styling and rendering an oversized `` element, Firefox did not apply correct clipping which allowed an attacker to paint over the user interface. (CVE-2021-29961)

- Address bar search suggestions in private browsing mode were re-using session data from normal mode.

This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29963)

- A locally-installed hostile program could send `WMCOPYDATA` messages that Firefox would process incorrectly, leading to an out-of-bounds read. This bug only affects Firefox on Windows. Other operating systems are unaffected. (CVE-2021-29964)

- When a user has already allowed a website to access microphone and camera, disabling camera sharing would not fully prevent the website from re-enabling it without an additional prompt. This was only possible if the website kept recording with the microphone until re-enabling the camera. (CVE-2021-29959)

- Firefox for Android would become unstable and hard-to-recover when a website opened too many popups.

This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29962)

- Mozilla developers Christian Holler, Anny Gakhokidze, Alexandru Michis, Gabriele Svelto reported memory safety bugs present in Firefox 88 and Firefox ESR 78.11. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29967)

- Mozilla developers Christian Holler, Tooru Fujisawa, Tyson Smith reported memory safety bugs present in Firefox 88. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29966)

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/mfsa2021-23/

Solution

Upgrade to Mozilla Firefox version 89.0 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)

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-2021-29959
CVE	CVE-2021-29960
CVE	CVE-2021-29961
CVE	CVE-2021-29962
CVE	CVE-2021-29963
CVE	CVE-2021-29964
CVE	CVE-2021-29965
CVE	CVE-2021-29966
CVE	CVE-2021-29967
XREF	IAVA:2021-A-0264-S

Plugin Information

Published: 2021/06/01, Modified: 2021/09/10

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 89.0
```

150802 - Mozilla Firefox < 89.0.1

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 89.0.1. It is, therefore, affected by a vulnerability as referenced in the mfsa2021-27 advisory.

- When drawing text onto a canvas with WebRender disabled, an out of bounds read could occur. This bug only affects Firefox on Windows. Other operating systems are unaffected. (CVE-2021-29968)

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/mfsa2021-27/

Solution

Upgrade to Mozilla Firefox version 89.0.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2021-29968
XREF	IAVA:2021-A-0292-S

Plugin Information

Published: 2021/06/16, Modified: 2021/07/16

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 89.0.1
```

152412 - Mozilla Firefox < 91.0

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 91.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-33 advisory.

- A suspected race condition when calling getaddrinfo led to memory corruption and a potentially exploitable crash. Note: This issue only affected Linux operating systems. Other operating systems are unaffected. (CVE-2021-29986)

- An issue present in lowering/register allocation could have led to obscure but deterministic register confusion failures in JITted code that would lead to a potentially exploitable crash. (CVE-2021-29981)

- Firefox incorrectly treated an inline list-item element as a block element, resulting in an out of bounds read or memory corruption, and a potentially exploitable crash. (CVE-2021-29988)

- Firefox for Android could get stuck in fullscreen mode and not exit it even after normal interactions that should cause it to exit. Note: This issue only affected Firefox for Android. Other operating systems are unaffected. (CVE-2021-29983)

- Instruction reordering resulted in a sequence of instructions that would cause an object to be incorrectly considered during garbage collection. This led to memory corruption and a potentially exploitable crash.

(CVE-2021-29984)

- Uninitialized memory in a canvas object could have caused an incorrect free() leading to memory corruption and a potentially exploitable crash. (CVE-2021-29980)

- After requesting multiple permissions, and closing the first permission panel, subsequent permission panels will be displayed in a different position but still record a click in the default location, making it possible to trick a user into accepting a permission they did not want to.This bug only affects Firefox on Linux. Other operating systems are unaffected. (CVE-2021-29987)

- A use-after-free vulnerability in media channels could have led to memory corruption and a potentially exploitable crash. (CVE-2021-29985)

- Due to incorrect JIT optimization, we incorrectly interpreted data from the wrong type of object, resulting in the potential leak of a single bit of memory. (CVE-2021-29982)

- Mozilla developers Christoph Kerschbaumer, Olli Pettay, Sandor Molnar, and Simon Giesecke reported memory safety bugs present in Firefox 90 and Firefox ESR 78.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29989)

- Mozilla developers and community members Kershaw Chang, Philipp, Chris Peterson, and Sebastian Hengst reported memory safety bugs present in Firefox 90. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.

(CVE-2021-29990)

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/mfsa2021-33/

Solution

Upgrade to Mozilla Firefox version 91.0 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)

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-2021-29980
CVE	CVE-2021-29981
CVE	CVE-2021-29982
CVE	CVE-2021-29983
CVE	CVE-2021-29984
CVE	CVE-2021-29985
CVE	CVE-2021-29986
CVE	CVE-2021-29987
CVE	CVE-2021-29988
CVE	CVE-2021-29989
CVE	CVE-2021-29990

XREF IAVA:2021-A-0366-S

Plugin Information

Published: 2021/08/10, Modified: 2021/09/10

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 91.0
```

152635 - Mozilla Firefox < 91.0.1

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 91.0.1. It is, therefore, affected by a vulnerability as referenced in the mfsa2021-37 advisory.

- Firefox incorrectly accepted a newline in a HTTP/3 header, interpretting it as two separate headers. This allowed for a header splitting attack against servers using HTTP/3. (CVE-2021-29991)

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/mfsa2021-37/

Solution

Upgrade to Mozilla Firefox version 91.0.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-29991
XREF	IAVA:2021-A-0386-S

Plugin Information

Published: 2021/08/17, Modified: 2021/11/05

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 91.0.1
```

153089 - Mozilla Firefox < 92.0

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 92.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-38 advisory.

- Firefox for Android allowed navigations through the `intent://` protocol, which could be used to cause crashes and UI spoofs. This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29993)

- Mixed-content checks were unable to analyze opaque origins which led to some mixed content being loaded.

(CVE-2021-38491)

- When delegating navigations to the operating system, Firefox would accept the `mk` scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. This bug only affects Firefox for Windows. Other operating systems are unaffected. (CVE-2021-38492)

- Mozilla developers Gabriele Svelto and Tyson Smith reported memory safety bugs present in Firefox 91 and Firefox ESR 78.13. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-38493)

- Mozilla developers Christian Holler and Lars T Hansen reported memory safety bugs present in Firefox 91.

Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-38494)

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/mfsa2021-38/

Solution

Upgrade to Mozilla Firefox version 92.0 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)

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-2021-4221
CVE	CVE-2021-29993
CVE	CVE-2021-38491
CVE	CVE-2021-38492
CVE	CVE-2021-38493
CVE	CVE-2021-38494
XREF	IAVA:2021-A-0405

Plugin Information

Published: 2021/09/07, Modified: 2022/02/22

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 92.0
```

155917 - Mozilla Firefox < 95.0

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 95.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2021-52 advisory.

- Under certain circumstances, asynchronous functions could have caused a navigation to fail but expose the target URL. (CVE-2021-43536)

- An incorrect type conversion of sizes from 64bit to 32bit integers allowed an attacker to corrupt memory leading to a potentially exploitable crash. (CVE-2021-43537)

- By misusing a race in our notification code, an attacker could have forcefully hidden the notification for pages that had received full screen and pointer lock access, which could have been used for spoofing attacks. (CVE-2021-43538)

- Failure to correctly record the location of live pointers across wasm instance calls resulted in a GC occurring within the call not tracing those live pointers. This could have led to a use-after-free causing a potentially exploitable crash. (CVE-2021-43539)

- WebExtensions with the correct permissions were able to create and install ServiceWorkers for third-party websites that would not have been uninstalled with the extension. (CVE-2021-43540)

- When invoking protocol handlers for external protocols, a supplied parameter URL containing spaces was not properly escaped. (CVE-2021-43541)

- Using XMLHttpRequest, an attacker could have identified installed applications by probing error messages for loading external protocols. (CVE-2021-43542)

- Documents loaded with the CSP sandbox directive could have escaped the sandbox's script restriction by embedding additional content. (CVE-2021-43543)

- When receiving a URL through a SEND intent, Firefox would have searched for the text, but subsequent usages of the address bar might have caused the URL to load unintentionally, which could lead to XSS and spoofing attacks. This bug only affects Firefox for Android. Other operating systems are unaffected.

(CVE-2021-43544)

- Using the Location API in a loop could have caused severe application hangs and crashes. (CVE-2021-43545)

- It was possible to recreate previous cursor spoofing attacks against users with a zoomed native cursor.

(CVE-2021-43546)

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/mfsa2021-52/

Solution

Upgrade to Mozilla Firefox version 95.0 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)

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-2021-4128
CVE	CVE-2021-4129
CVE	CVE-2021-43536
CVE	CVE-2021-43537
CVE	CVE-2021-43538
CVE	CVE-2021-43539
CVE	CVE-2021-43540
CVE	CVE-2021-43541
CVE	CVE-2021-43542
CVE	CVE-2021-43543
CVE	CVE-2021-43544
CVE	CVE-2021-43545
CVE	CVE-2021-43546
XREF	IAVA:2021-A-0569-S

Plugin Information

Published: 2021/12/08, Modified: 2021/12/30

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 95.0
```

159530 - Mozilla Firefox < 99.0

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 99.0. It is, therefore, affected by multiple vulnerabilities as referenced in the mfsa2022-13 advisory.

- <code>NSSToken</code> objects were referenced via direct points, and could have been accessed in an unsafe way on different threads, leading to a use-after-free and potentially exploitable crash. (CVE-2022-1097)

- If a compromised content process sent an unexpected number of WebAuthN Extensions in a Register command to the parent process, an out of bounds write would have occurred leading to memory corruption and a potentially exploitable crash. (CVE-2022-28281)

- By using a link with <code>rel=localization</code> a use-after-free could have been triggered by destroying an object during JavaScript execution and then referencing the object through a freed pointer, leading to a potentially exploitable crash. (CVE-2022-28282)

- The sourceMapURL feature in devtools was missing security checks that would have allowed a webpage to attempt to include local files or other files that should have been inaccessible. (CVE-2022-28283)

- SVG's <code><use></code> element could have been used to load unexpected content that could have executed script in certain circumstances. While the specification seems to allow this, other browsers do not, and web developers relied on this property for script security so gecko's implementation was aligned with theirs. (CVE-2022-28284)

- When generating the assembly code for <code>MLoadTypedArrayElementHole</code>, an incorrect AliasSet was used. In conjunction with another vulnerability this could have been used for an out of bounds memory read. (CVE-2022-28285)

- Due to a layout change, iframe contents could have been rendered outside of its border. This could have led to user confusion or spoofing attacks. (CVE-2022-28286)

- In unusual circumstances, selecting text could cause text selection caching to behave incorrectly, leading to a crash. (CVE-2022-28287)

- The rust regex crate did not properly prevent crafted regular expressions from taking an arbitrary amount of time during parsing. If an attacker was able to supply input to this crate, they could have caused a denial of service in the browser. (CVE-2022-24713)

- Mozilla developers and community members Nika Layzell, Andrew McCreight, Gabriele Svelto, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 98 and Firefox ESR 91.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2022-28289)

- Mozilla developers and community members Randell Jesup, Sebastian Hengst, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 98. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.

(CVE-2022-28288)

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

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2022-13/

Solution

Upgrade to Mozilla Firefox version 99.0 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2022-1097
CVE	CVE-2022-24713
CVE	CVE-2022-28281
CVE	CVE-2022-28282
CVE	CVE-2022-28283
CVE	CVE-2022-28284
CVE	CVE-2022-28285
CVE	CVE-2022-28286
CVE	CVE-2022-28287
CVE	CVE-2022-28288
CVE	CVE-2022-28289

XREF IAVA:2022-A-0134-S

Plugin Information

Published: 2022/04/05, Modified: 2022/05/30

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 99.0
```

52767 - Firefox 3.6 < 3.6.16 Invalid HTTP Certificates

Synopsis

The remote Windows host contains a web browser with an out-of-date SSL certificate blacklist.

Description

The installed version of Firefox 3.6 is earlier than 3.6.16. Such versions have an out-of-date SSL certificate blacklist.

A certificate authority (CA) has revoked a number of fraudulent SSL certificates for several prominent public websites.

If an attacker can trick someone into using the affected browser and visiting a malicious site using one of the fraudulent certificates, he may be able to fool that user into believing the site is a legitimate one. In turn, the user could send credentials to the malicious site or download and install applications.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2011-11/

http://www.nessus.org/u?a9b416a4

http://www.nessus.org/u?14606051

Solution

Upgrade to Firefox 3.6.16 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2011/03/23, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.16
```

56037 - Firefox 3.6.x < 3.6.21 Out-of-Date CA List

Synopsis

The remote Windows host contains a web browser that is affected by an out-of-date certificate authority list.

Description

The installed version of Firefox 3.6.x is earlier than 3.6.21 and is potentially affected by an out-of-date certificate authority list. Due to the issuance of several fraudulent SSL certificates, the certificate authority DigiNotar has been disabled in Mozilla Firefox.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2011-34/

http://www.nessus.org/u?abdae5f6

Solution

Upgrade to Firefox 3.6.21 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2011/08/31, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.21
```

56119 - Firefox 3.6.x < 3.6.22 Untrusted CA

Synopsis

The remote Windows host contains a web browser that contains support for an untrustworthy certificate authority.

Description

The installed version of Firefox 3.6.x is earlier than 3.6.22. Due to a recent attack against certificate authority DigiNotar, Mozilla has added explicit distrust to the DigiNotar root certificate and several intermediates in this version of Firefox.

Note this is a further fix to MFSA 2011-34, which removed the DigiNotar root certificate.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2011-35/

http://www.nessus.org/u?a36daf9d

Solution

Upgrade to Firefox 3.6.22 or later.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2011/09/08, Modified: 2017/06/09

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 3.6.22
```

62744 - Firefox < 16.0.2 Multiple Vulnerabilities

Synopsis

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

Description

The installed version of Firefox is earlier than 16.0.2 and is, therefore, 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 16.0.2 or later.

Risk Factor

Medium

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 : 3.6.12
Fixed version     : 16.0.2
```

82040 - Firefox < 36.0.3 JIT Code Execution

Synopsis

The remote Windows host contains a web browser that is affected by a remote code execution vulnerability.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 36.0.3. It is, therefore, affected by a remote code execution vulnerability due to an out-of-bounds error in typed array bounds checking within 'asmjs/AsmJSValidate.cpp', which relates to just-in-time compilation for JavaScript. A remote attacker, using a specially crafted web page, can exploit this to execute arbitrary code by reading and writing to memory.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-29/

Solution

Upgrade to Firefox 36.0.3 or later.

Risk Factor

Medium

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	73263
CVE	CVE-2015-0817

Plugin Information

Published: 2015/03/24, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 36.0.3
```

82583 - Firefox < 37.0.1 HTTP/2 Alt-Svc Header Certificate Verification Bypass

Synopsis

The remote Windows host contains a web browser that is affected by a security bypass vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 37.0.1. It is, therefore, affected by an error related to the HTTP/2 'Alt-Svc' header and SSL certificate verification, which allows man-in-the-middle (MitM) attacks.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-44/

Solution

Upgrade to Firefox 37.0.1 or later.

Risk Factor

Medium

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

BID	73905
CVE	CVE-2015-0799

Plugin Information

Published: 2015/04/06, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
```

```
  Fixed version     : 37.0.1
```

82998 - Firefox < 37.0.2 Failed Plugin Memory Corruption

Synopsis

The remote Windows host contains a web browser that is affected by a memory corruption vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 37.0.2. It is, therefore, affected by a use-after-free error, related to the AsyncPaintWaitEvent() method, due to a race condition caused when plugin initialization fails. A remote attacker, using a crafted web page, can exploit this to execute arbitrary code.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-45/

Solution

Upgrade to Firefox 37.0.2 or later.

Risk Factor

Medium

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	74247
CVE	CVE-2015-2706

Plugin Information

Published: 2015/04/22, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
```

```
    Fixed version     : 37.0.2
```

85275 - Firefox < 39.0.3 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 installed on the remote Windows host is prior to 39.0.3. 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 39.0.3 or later.

Risk Factor

Medium

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 : 3.6.12
  Fixed version     : 39.0.3
```

57316 - Firefox < 4 CSS Browser History Disclosure Vulnerability

Synopsis

The remote Windows host contains a web browser that is affected by an information disclosure vulnerability.

Description

The installed version of Firefox 3 is potentially affected by an information disclosure vulnerability.

The JavaScript function 'getComputedStyle', and functions like it, can be used in a timing attack to determine if a browser has visited links on the page.

See Also

http://www.nessus.org/u?15b35e55

http://www.nessus.org/u?86c7721b

Solution

Upgrade to Firefox 4.0 or later.

Risk Factor

Medium

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

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

References

BID	51051
CVE	CVE-2010-5074

Plugin Information

Published: 2011/12/15, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 4.0
```

86418 - Firefox < 41.0.2 'fetch' API Cross-Origin Bypass

Synopsis

The remote Windows host contains a web browser that is affected by a cross-origin restriction bypass vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 41.0.2. It is, therefore, affected by a cross-origin restriction bypass vulnerability in the fetch() API due to an incorrect implementation of the Cross-Origin Resource Sharing (CORS) specification. A remote attacker can exploit this, via a malicious website, to access private data from other origins.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2015-115/

Solution

Upgrade to Firefox 41.0.2 or later.

Risk Factor

Medium

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-2015-7184

Plugin Information

Published: 2015/10/16, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
```

```
    Fixed version     : 41.0.2
```

105616 - Mozilla Firefox < 57.0.4 Speculative Execution Side-Channel Attack Vulnerability (Spectre)

Synopsis

A web browser installed on the remote Windows host is affected by a speculative execution side-channel attack vulnerability.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 57.0.4. It is, therefore, vulnerable to a speculative execution side-channel attack. Code from a malicious web page could read data from other web sites or private data from the browser itself.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/

https://spectreattack.com/

Solution

Upgrade to Mozilla Firefox version 57.0.4 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

BID	102371
BID	102376
CVE	CVE-2017-5715
CVE	CVE-2017-5753
XREF	MFSA:2018-01
XREF	IAVA:2018-A-0020

Exploitable With

CANVAS (true)

Plugin Information

Published: 2018/01/05, Modified: 2019/11/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 57.0.4
```

106561 - Mozilla Firefox < 58.0.1 Arbitrary Code Execution

Synopsis

A web browser installed on the remote Windows host is affected by an arbitrary code execution vulnerability.

Description

The version of Mozilla Firefox installed on the remote Windows host is prior to 58.0.1. It is, therefore, affected by an arbitrary code execution vulnerability.

See Also

https://www.mozilla.org/en-US/security/advisories/mfsa2018-05/

Solution

Upgrade to Mozilla Firefox version 58.0.1 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)

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

BID	102843
CVE	CVE-2018-5124
XREF	MFSA:2018-05

Plugin Information

Published: 2018/02/01, Modified: 2019/11/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 58.0.1
```

125877 - Mozilla Firefox < 67.0.2

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 67.0.2. It is, therefore, affected by a vulnerability as referenced in the mfsa2019-16 advisory.

- A hyperlink using protocols associated with Internet Explorer, such as IE.HTTP:, can be used to open local files at a known location with Internet Explorer if a user approves execution when prompted.

Note: this issue only occurs on Windows. Other operating systems are unaffected. (CVE-2019-11702)

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/mfsa2019-16/

Solution

Upgrade to Mozilla Firefox version 67.0.2 or later.

Risk Factor

Medium

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)

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

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

References

BID	108723

CVE	CVE-2019-11702
XREF	MFSA:2019-16

Plugin Information

Published: 2019/06/13, Modified: 2019/10/18

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 67.0.2
```

129101 - Mozilla Firefox < 69.0.1

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 69.0.1. It is, therefore, affected by the following vulnerability as referenced in the mfsa2019-31 advisory:

- When the pointer lock is enabled by a website though requestPointerLock(), no user notification is given.

This could allow a malicious website to hijack the mouse pointer and confuse users.

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/mfsa2019-31/

Solution

Upgrade to Mozilla Firefox version 69.0.1 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)

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-2019-11754
XREF	MFSA:2019-31

Plugin Information

Published: 2019/09/23, Modified: 2019/11/08

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 69.0.1
```

138445 - Mozilla Firefox < 78.0.2

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 78.0.2. It is, therefore, affected by a vulnerability as referenced in the mfsa2020-28 advisory.

- Using object or embed tags, it was possible to frame other websites, even if they disallowed framing using the X-Frame-Options header (CVE-2020-15648).

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/mfsa2020-28/

Solution

Upgrade to Mozilla Firefox version 78.0.2 or later.

Risk Factor

Medium

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

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

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-2020-15648
XREF	MFSA:2020-28

Plugin Information

Published: 2020/07/14, Modified: 2020/10/09

Plugin Output

tcp/445/cifs

```
Path              : C:\Program Files (x86)\Mozilla Firefox
Installed version : 3.6.12
Fixed version     : 78.0.2
```

146425 - Mozilla Firefox < 85.0.1

Synopsis

A web browser installed on the remote Windows host is affected by a vulnerability.

Description

The version of Firefox installed on the remote Windows host is prior to 85.0.1. It is, therefore, affected by a vulnerability as referenced in the mfsa2021-06 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/mfsa2021-06/

Solution

Upgrade to Mozilla Firefox version 85.0.1 or later.

Risk Factor

Medium

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)

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

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

References

CVE	CVE-2020-16048

Plugin Information

Published: 2021/02/11, Modified: 2022/01/21

Plugin Output

tcp/445/cifs

```
  Path              : C:\Program Files (x86)\Mozilla Firefox
  Installed version : 3.6.12
  Fixed version     : 85.0.1
```

96534 - Firefox Browser Extension Enumeration

Synopsis

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

Description

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

See Also

https://addons.mozilla.org/en-US/firefox/

Solution

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

Risk Factor

None

References

XREF IAVT:0001-T-0510

Plugin Information

Published: 2017/01/16, Modified: 2022/08/02

Plugin Output

tcp/445/cifs

```
User : user
|- Browser : Firefox
  |- Plugin information :

    Name        : Mozilla Default Plug-in
    Description : Default Plug-in
    Version     : 1.0.0.15
    Update Date : Oct. 27, 2010 at 06:10:21 GMT
    Path        : C:\Program Files (x86)\Mozilla Firefox\plugins\npnul32.dll
```