Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Application					
Gethue					
HUE					
XSS	01-06-2018	**4.3**	Hue 3.12 has XSS via the /pig/save/ name and script parameters. **CVE-ID:CVE-2018-11649**	https://github.com/Blck4/HUE-Exploit	A-Get-HUE/02-07-18/1
Liblouis					
Liblouis					
Overflow	09-06-2018	**6.8**	Liblouis 3.6.0 has a stack-based Buffer Overflow in the function parse Chars in compile Translation Table.c, a different vulnerability than CVE-2018-11440. **CVE-ID:CVE-2018-12085**	https://github.com/liblouis/liblouis/issues/595	A-Lib-Liblo/02-07-18/2
Miniupnp Project					
Ngiflib					
NA	01-06-2018	**5**	ngiflib.c in MiniUPnP ngiflib 0.4 has an infinite loop in Decode GifImg and LoadGif. **CVE-ID:CVE-2018-11657**	https://github.com/miniupnp/ngiflib/issues/7	A-Min-Ngifl/02-07-18/3
Modx					
Modx Revolution					
XSS	01-06-2018	**3.5**	MODX Revolution 2.6.3 has XSS. **CVE-ID:CVE-2018-10382**	https://github.com/modxcms/revolution/pull/13887 https://github.com/modxcms/revolution/pull/13887/commits/3241473d8213e9551cef4ed0e8ac4645cfbd10c4	A-Mod-Modx/02-07-18/4
Mozilla					
Firefox					
Bypass	11-06-2018	**5**	The "instanceof" operator can bypass the Xray wrapper mechanism. When called on web	https://bugzilla.mozilla.org/show_b	A-Moz-Firef/02-07-18/5

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			content from the browser itself or an extension the web content can provide its own result for that operator, possibly tricking the browser or extension into mishandling the element. This vulnerability affects Firefox < 56. **CVE-ID:CVE-2017-7820**	ug.cgi?id=1378207 https://www.mozilla.org/security/advisories/mfsa2017-21/	
Execute Code XSS	11-06-2018	**4.3**	JavaScript can be injected into an exported bookmarks file by placing JavaScript code into user-supplied tags in saved bookmarks. If the resulting exported HTML file is later opened in a browser this JavaScript will be executed. This could be used in social engineering and self-cross-site-scripting (self-XSS) attacks if users were convinced to add malicious tags to bookmarks, export them, and then open the resulting file. This vulnerability affects Firefox < 57. **CVE-ID:CVE-2017-7840**	https://bugzilla.mozilla.org/show_bug.cgi?id=1366420 https://www.mozilla.org/security/advisories/mfsa2017-24/	A-Moz-Firef/02-07-18/6
Gain Information	11-06-2018	**5**	A vulnerability where the security wrapper does not deny access to some exposed properties using the deprecated "_exposedProps_" mechanism on proxy objects. These properties should be explicitly unavailable to proxy objects. This vulnerability affects Firefox < 57. **CVE-ID:CVE-2017-7831**	https://www.mozilla.org/security/advisories/mfsa2017-24/ https://bugzilla.mozilla.org/show_bug.cgi?id=1392026	A-Moz-Firef/02-07-18/7
Gain Information	11-06-2018	**5**	If a document's Referrer Policy attribute is set to "no-referrer" sometimes two network requests are made for "<link>" elements instead of one. One of these requests includes the referrer instead of respecting the set policy to not include a referrer on requests. This vulnerability affects Firefox < 57. **CVE-ID:CVE-2017-7842**	https://bugzilla.mozilla.org/show_bug.cgi?id=1397064 https://www.mozilla.org/security/advisories/mfsa2017-24/	A-Moz-Firef/02-07-18/8

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Gain Information	11-06-2018	**5**	If web content on a page is dragged onto portions of the browser UI, such as the tab bar, links can be opened that otherwise would not be allowed to open. This can allow malicious web content to open a locally stored file through "file:" URLs. This vulnerability affects Firefox < 56. **CVE-ID:CVE-2017-7812**	https://www.mozilla.org/security/advisories/mfsa2017-21/ https://bugzilla.mozilla.org/show_bug.cgi?id=1379842	A-Moz-Firef/02-07-18/9
Gain Information	11-06-2018	**6.4**	Inside the JavaScript parser, a cast of an integer to a narrower type can result in data read from outside the buffer being parsed. This usually results in a non-exploitable crash, but can leak a limited amount of information from memory if it matches JavaScript identifier syntax. This vulnerability affects Firefox < 56. **CVE-ID:CVE-2017-7813**	https://bugzilla.mozilla.org/show_bug.cgi?id=1383951 https://www.mozilla.org/security/advisories/mfsa2017-21/	A-Moz-Firef/02-07-18/10
NA	11-06-2018	**4.6**	The "pingsender" executable used by the Firefox Health Report dynamically loads a system copy of libcurl, which an attacker could replace. This allows for privilege escalation as the replaced libcurl code will run with Firefox's privileges. Note: This attack requires an attacker have local system access and only affects OS X and Linux. Windows systems are not affected. This vulnerability affects Firefox < 57. **CVE-ID:CVE-2017-7836**	https://www.mozilla.org/security/advisories/mfsa2017-24/ https://bugzilla.mozilla.org/show_bug.cgi?id=1401339	A-Moz-Firef/02-07-18/11
NA	11-06-2018	**5**	A spoofing vulnerability can occur when a page switches to fullscreen mode without user notification, allowing a fake address bar to be displayed. This allows an attacker to spoof which page is actually loaded and in use. Note: This attack only affects Firefox for Android.	https://www.mozilla.org/security/advisories/mfsa2017-21/ https://bugzilla.mozilla.org/show_bug.cgi?id=1356596	A-Moz-Firef/02-07-18/12

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Other operating systems are not affected. This vulnerability affects Firefox < 56. **CVE-ID:CVE-2017-7817**		
NA	11-06-2018	**5**	If cursor visibility is toggled by script using from 'none' to an image and back through script, the cursor will be rendered temporarily invisible within Firefox. Note: This vulnerability only affects OS X. Other operating systems are not affected. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5110**	https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1423275	A-Moz-Firef/02-07-18/13
NA	11-06-2018	**5**	Low descenders on some Tibetan characters in several fonts on OS X are clipped when rendered in the addressbar. When used as part of an Internationalized Domain Name (IDN) this can be used for domain name spoofing attacks. Note: This attack only affects OS X operating systems. Other operating systems are unaffected. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5121**	https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1402368	A-Moz-Firef/02-07-18/14
NA	11-06-2018	**5**	On pages containing an iframe, the "data:" protocol can be used to create a modal dialog through Javascript that will have an arbitrary domains as the dialog's location, spoofing of the origin of the modal dialog from the user view. Note: This attack only affects installations with e10 multiprocess turned off. Installations with e10s turned on do not support the modal dialog functionality. This vulnerability affects Firefox < 56. **CVE-ID:CVE-2017-7815**	https://bugzilla.mozilla.org/show_bug.cgi?id=1368981 https://www.mozilla.org/security/advisories/mfsa2017-21/	A-Moz-Firef/02-07-18/15

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	11-06-2018	**5**	Punycode format text will be displayed for entire qualified international domain names in some instances when a sub-domain triggers the punycode display instead of the primary domain being displayed in native script and the sub-domain only displaying as punycode. This could be used for limited spoofing attacks due to user confusion. This vulnerability affects Firefox < 57. **CVE-ID:CVE-2017-7838**	https://www.mozilla.org/security/advisories/mfsa2017-24/ https://bugzilla.mozilla.org/show_bug.cgi?id=1399540	A-Moz-Firef/02-07-18/16
NA	11-06-2018	**5**	Some Arabic and Indic vowel marker characters can be combined with Latin characters in a domain name to eclipse the non-Latin character with some font sets on the addressbar. The non-Latin character will not be visible to most viewers. This allows for domain spoofing attacks because these combined domain names do not display as punycode. This vulnerability affects Firefox < 57. **CVE-ID:CVE-2017-7833**	https://bugzilla.mozilla.org/show_bug.cgi?id=1370497 https://www.mozilla.org/security/advisories/mfsa2017-24/	A-Moz-Firef/02-07-18/17
NA	11-06-2018	**5**	SVG loaded through "<img>" tags can use "<meta>" tags within the SVG data to set cookies for that page. This vulnerability affects Firefox < 57. **CVE-ID:CVE-2017-7837**	https://www.mozilla.org/security/advisories/mfsa2017-24/ https://bugzilla.mozilla.org/show_bug.cgi?id=1325923	A-Moz-Firef/02-07-18/18
NA	11-06-2018	**5**	The AES-GCM implementation in WebCrypto API accepts 0-length IV when it should require a length of 1 according to the NIST Special Publication 800-38D specification. This might allow for the authentication key to be determined in some instances. This	https://www.mozilla.org/security/advisories/mfsa2017-21/ https://bugzilla.mozilla.org/show_bug.cgi?id=1368859	A-Moz-Firef/02-07-18/19

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			vulnerability affects Firefox < 56. **CVE-ID:CVE-2017-7822**		
NA	11-06-2018	**5**	The combined, single character, version of the letter 'i' with any of the potential accents in unicode, such as acute or grave, can be spoofed in the addressbar by the dotless version of 'i' followed by the same accent as a second character with most font sets. This allows for domain spoofing attacks because these combined domain names do not display as punycode. This vulnerability affects Firefox < 57. **CVE-ID:CVE-2017-7832**	https://www.mozilla.org/security/advisories/mfsa2017-24/ https://bugzilla.mozilla.org/show_bug.cgi?id=1408782	A-Moz-Firef/02-07-18/20
NA	11-06-2018	**5**	WebExtensions could use popups and panels in the extension UI to load an "about:" privileged URL, violating security checks that disallow this behavior. This vulnerability affects Firefox < 56. **CVE-ID:CVE-2017-7816**	https://www.mozilla.org/security/advisories/mfsa2017-21/ https://bugzilla.mozilla.org/show_bug.cgi?id=1380597	A-Moz-Firef/02-07-18/21
NA	11-06-2018	**7.5**	A vulnerability where WebExtensions can download and attempt to open a file of some non-executable file types. This can be triggered without specific user interaction for the file download and open actions. This could be used to trigger known vulnerabilities in the programs that handle those document types. This vulnerability affects Firefox < 56. **CVE-ID:CVE-2017-7821**	https://www.mozilla.org/security/advisories/mfsa2017-21/ https://bugzilla.mozilla.org/show_bug.cgi?id=1346515	A-Moz-Firef/02-07-18/22
NA	11-06-2018	**7.5**	Mixed content blocking of insecure (HTTP) sub-resources in a secure (HTTPS) document was not correctly applied for resources that redirect from HTTPS to HTTP, allowing content that should be blocked, such as scripts, to be loaded on a page. This vulnerability	https://www.mozilla.org/security/advisories/mfsa2017-24/ https://bugzilla.mozilla.org/show_bug.cgi?id=1402363	A-Moz-Firef/02-07-18/23

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			affects Firefox < 57. **CVE-ID:CVE-2017-7835**		
Overflow Memory Corruption	11-06-2018	**10**	Memory safety bugs were reported in Firefox 56. 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. This vulnerability affects Firefox < 57. **CVE-ID:CVE-2017-7827**	https://www.mozilla.org/security/advisories/mfsa2017-24/ https://bugzilla.mozilla.org/buglist.cgi?bug_id=1399922%2C1403646%2C1403716%2C1365894%2C1402876%2C1406154%2C1384121%2C1384615%2C1407375%2C1339485%2C1361432%2C1394031%2C1383019%2C1407032%2C1387845%2C1386490	A-Moz-Firef/02-07-18/24
XSS	11-06-2018	**4.3**	Control characters prepended before "javascript:" URLs pasted in the addressbar can cause the leading characters to be ignored and the pasted JavaScript to be executed instead of being blocked. This could be used in social engineering and self-cross-site-scripting (self-XSS) attacks where users are convinced to copy and paste text into the addressbar. This vulnerability affects Firefox < 57. **CVE-ID:CVE-2017-7839**	https://www.mozilla.org/security/advisories/mfsa2017-24/ https://bugzilla.mozilla.org/show_bug.cgi?id=1402896	A-Moz-Firef/02-07-18/25
XSS Bypass	11-06-2018	**4.3**	A "data:" URL loaded in a new tab did not inherit the Content Security Policy (CSP) of the original page, allowing for bypasses of the policy including the execution of JavaScript. In prior versions when "data:" documents also inherited the context of the original page this would allow for potential cross-site	https://www.mozilla.org/security/advisories/mfsa2017-24/ https://bugzilla.mozilla.org/show_bug.cgi?id=1358009	A-Moz-Firef/02-07-18/26

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			scripting (XSS) attacks. This vulnerability affects Firefox < 57. **CVE-ID:CVE-2017-7834**		
Njtech					
Greencms					
CSRF	01-06-2018	**6.8**	An issue was discovered in GreenCMS v2.3.0603. There is a CSRF vulnerability that can add an admin account via index.php?m=admin&c=access&a=adduserhandle. **CVE-ID:CVE-2018-11671**	https://github.com/GreenCMS/GreenCMS/issues/109 https://www.exploit-db.com/exploits/44826/	A-Njt-Green/02-07-18/27
Exec Code CSRF	01-06-2018	**6.8**	An issue was discovered in GreenCMS v2.3.0603. There is a CSRF vulnerability that allows attackers to execute arbitrary PHP code via the content parameter to index.php?m=admin&c=media&a=fileconnect. **CVE-ID:CVE-2018-11670**	https://www.exploit-db.com/exploits/44825/ https://github.com/GreenCMS/GreenCMS/issues/108	A-Njt-Green/02-07-18/28
Pivotal Software					
Spring Integration Zip					
Dir. Trav.	05-06-2018	**5.8**	Apache Storm version 1.0.6 and earlier, 1.2.1 and earlier, and version 1.1.2 and earlier expose an arbitrary file write vulnerability, that can be achieved using a specially crafted zip archive (affects other archives as well, bzip2, tar, xz, war, cpio, 7z), that holds path traversal filenames. So when the filename gets concatenated to the target extraction directory, the final path ends up outside of the target folder. **CVE-ID:CVE-2018-8008**	https://lists.apache.org/thread.html/613b2fca8bcd0a3b12c0b763ea8f7cf62e422e9f79fce6cfa5b08a58@%3Cdev.storm.apache.org%3E	A-Piv-Sprin/02-07-18/29
Synology					
Drive					
NA	01-06-2018	**4**	Improper access control vulnerability in Synology Drive before 1.0.2-10275 allows remote	https://www.synology.com/en-global/support/se	A-Syn-Drive/02-07-18/30

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			authenticated users to access non-shared files or folders via unspecified vectors. **CVE-ID:CVE-2018-8922**	curity/Synology_S18_11	
Application Operating System (Application,OS)					
Canonical,Imagemagick					
Imagemagick,Ubuntu Linux					
DoS	01-06-2018	**4.3**	In ImageMagick 7.0.7-20 Q16 x86_64, a memory leak vulnerability was found in the function GetImagePixelCache in MagickCore/cache.c, which allows attackers to cause a denial of service via a crafted CALS image file. **CVE-ID:CVE-2018-11655**	https://usn.ubuntu.com/3681-1/ https://github.com/ImageMagick/ImageMagick/issues/930	A-Can-Image/02-07-18/31
DoS	01-06-2018	**4.3**	In ImageMagick 7.0.7-20 Q16 x86_64, a memory leak vulnerability was found in the function ReadDCMImage in coders/dcm.c, which allows attackers to cause a denial of service via a crafted DCM image file. **CVE-ID:CVE-2018-11656**	https://usn.ubuntu.com/3681-1/ https://github.com/ImageMagick/ImageMagick/issues/931	A-Can-Image/02-07-18/32
Canonical,Liblouis					
Liblouis,Ubuntu Linux					
Overflow	04-06-2018	**6.8**	Liblouis 3.5.0 has a stack-based Buffer Overflow in the function compileHyphenation in compileTranslationTable.c. **CVE-ID:CVE-2018-11685**	https://github.com/liblouis/liblouis/issues/593 https://usn.ubuntu.com/3672-1/	A-Can-Liblo/02-07-18/33
Overflow	04-06-2018	**6.8**	Liblouis 3.5.0 has a stack-based Buffer Overflow in the function includeFile in compileTranslationTable.c. **CVE-ID:CVE-2018-11684**	https://github.com/liblouis/liblouis/issues/592 https://usn.ubuntu.com/3672-1/	A-Can-Liblo/02-07-18/34
Overflow	04-06-2018	**6.8**	Liblouis 3.5.0 has a stack-based Buffer Overflow in the function parseChars in compileTranslationTable.c, a different vulnerability than CVE-2018-11440. **CVE-ID:CVE-2018-11683**	https://github.com/liblouis/liblouis/issues/591 https://usn.ubuntu.com/3672-1/	A-Can-Liblo/02-07-18/35

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Canonical,Mozilla					
Firefox,Ubuntu Linux					
Bypass	11-06-2018	**5**	The printing process can bypass local access protections to read files available through symlinks, bypassing local file restrictions. The printing process requires files in a specific format so arbitrary data cannot be read but it is possible that some local file information could be exposed. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5107**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1379276	A-Can-Firef/02-07-18/36
Bypass	11-06-2018	**7.2**	WebExtensions can bypass user prompts to first save and then open an arbitrarily downloaded file. This can result in an executable file running with local user privileges without explicit user consent. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5105**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1390882	A-Can-Firef/02-07-18/37
Bypass	11-06-2018	**7.5**	WebExtensions with the "ActiveTab" permission are able to access frames hosted within the active tab even if the frames are cross-origin. Malicious extensions can inject frames from arbitrary origins into the loaded page and then interact with them, bypassing same-origin user expectations with this permission. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5116**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1396399	A-Can-Firef/02-07-18/38
Gain Information	11-06-2018	**4.3**	A Blob URL can violate origin attribute segregation, allowing it to be accessed from a private browsing tab and for data to be passed between the private browsing tab and a normal tab. This could allow for the leaking of private information specific to the	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_b	A-Can-Firef/02-07-18/39

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			private browsing context. This issue is mitigated by the requirement that the user enter the Blob URL manually in order for the access violation to occur. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5108**	ug.cgi?id=1421099	
Gain Information	11-06-2018	**5**	If an existing cookie is changed to be "HttpOnly" while a document is open, the original value remains accessible through script until that document is closed. Network requests correctly use the changed HttpOnly cookie. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5114**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1421324	A-Can-Firef/02-07-18/40
Gain Information	11-06-2018	**5**	If an HTTP authentication prompt is triggered by a background network request from a page or extension, it is displayed over the currently loaded foreground page. Although the prompt contains the real domain making the request, this can result in user confusion about the originating site of the authentication request and may cause users to mistakenly send private credential information to a third party site. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5115**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1409449	A-Can-Firef/02-07-18/41
Gain Information	11-06-2018	**5**	Style editor traffic in the Developer Tools can be routed through a service worker hosted on a third party website if a user selects error links when these tools are open. This can allow style editor information used within Developer Tools to leak cross-origin. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5106**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1408708	A-Can-Firef/02-07-18/42

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Gain Information	11-06-2018	**5**	The reader view will display cross-origin content when CORS headers are set to prohibit the loading of cross-origin content by a site. This could allow access to content that should be restricted in reader view. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5119**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1420507	A-Can-Firef/02-07-18/43
Gain Information	11-06-2018	**5**	The screenshot images displayed in the Activity Stream page displayed when a new tab is opened is created from the meta tags of websites. An issue was discovered where the page could attempt to create these images through "file:" URLs from the local file system. This loading is blocked by the sandbox but could expose local data if combined with another attack that escapes sandbox protections. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5118**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1420049	A-Can-Firef/02-07-18/44
NA	11-06-2018	**4.3**	When the text of a specially formatted URL is dragged to the addressbar from page content, the displayed URL can be spoofed to show a different site than the one loaded. This allows for phishing attacks where a malicious page can spoof the identify of another site. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5111**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1321619	A-Can-Firef/02-07-18/45
NA	11-06-2018	**5**	An audio capture session can started under an incorrect origin from the site making the capture request. Users are still prompted to allow the request but the prompt can display the wrong origin, leading to user confusion about which site is making the request to	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_b	A-Can-Firef/02-07-18/46

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			capture an audio stream. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5109**	ug.cgi?id=1405599	
NA	11-06-2018	**5**	A use-after-free vulnerability can occur when arguments passed to the "IsPotentiallyScrollable" function are freed while still in use by scripts. This results in a potentially exploitable crash. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5100**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1417405	A-Can-Firef/02-07-18/47
NA	11-06-2018	**5**	A use-after-free vulnerability can occur when manipulating floating "first-letter" style elements, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5101**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1417661	A-Can-Firef/02-07-18/48
NA	11-06-2018	**5**	Development Tools panels of an extension are required to load URLs for the panels as relative URLs from the extension manifest file but this requirement was not enforced in all instances. This could allow the development tools panel for the extension to load a URL that it should not be able to access, including potentially privileged pages. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5112**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1425224	A-Can-Firef/02-07-18/49
NA	11-06-2018	**5**	The "browser.identity.launchWebAuthFlow" function of WebExtensions is only allowed to load content over "https:" but this requirement was not properly enforced. This can potentially allow privileged pages	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.m	A-Can-Firef/02-07-18/50

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			to be loaded by the extension. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5113**	ozilla.org/show_bug.cgi?id=1425267	
NA	11-06-2018	**7.5**	A use-after-free vulnerability can occur when the thread for a Web Worker is freed from memory prematurely instead of from memory in the main thread while cancelling fetch operations. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5092**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1418074	A-Can-Firef/02-07-18/51
Overflow	11-06-2018	**5**	A heap buffer overflow vulnerability may occur in WebAssembly during Memory/Table resizing, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5093**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1415291	A-Can-Firef/02-07-18/52
Overflow	11-06-2018	**5**	A heap buffer overflow vulnerability may occur in WebAssembly when "shrinkElements" is called followed by garbage collection on memory that is now uninitialized. This results in a potentially exploitable crash. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5094**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1415883	A-Can-Firef/02-07-18/53
Overflow	11-06-2018	**7.5**	A potential integer overflow in the "DoCrypt" function of WebCrypto was identified. If a means was found of exploiting it, it could result in an out-of-bounds write. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5122**	https://usn.ubuntu.com/3544-1/ https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/show_bug.cgi?id=1413841	A-Can-Firef/02-07-18/54

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Overflow Memory Corruption	11-06-2018	**10**	Memory safety bugs were reported in Firefox 57. 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. This vulnerability affects Firefox < 58. **CVE-ID:CVE-2018-5090**	https://www.mozilla.org/security/advisories/mfsa2018-02/ https://bugzilla.mozilla.org/buglist.cgi?bug_id=1413857%2C1412653%2C1418966%2C1427126%2C1412942%2C1401459%2C1364399%2C1382851%2C1423770%2C1401420%2C1281965%2C1389561%2C1409179%2C1416879%2C1421786%2C1426449%2C1416799%2C1400912%2C1415158%2C1415748%2C1415788%2C1371891%2C1415770%2C1416519%2C1413143%2C1418841%2C1384544%2C1410140%2C1411631%2C1412313%2C1412641%2C1412645%2C1412646%2C1412648%2C1261175 https://usn.ubuntu.com/3544-1/	A-Can-Firef/02-07-18/55
Operating System (OS)					
Microsoft					
Windows 10,Windows 7,Windows 8.1,Windows Rt 8.1,Windows Server 2008,Windows Server 2012,Windows Server 2016					
DoS Overflow	14-06-2018	**4.9**	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka "Windows Denial of Service	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory	O-Mic-Windo/02-07-18/56

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE-ID:CVE-2018-8205**	/CVE-2018-8205	
NA	14-06-2018	**6.9**	An elevation of privilege vulnerability exists when NTFS improperly checks access, aka "NTFS Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE-ID:CVE-2018-1036**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1036	O-Mic-Windo/02-07-18/57
NA	14-06-2018	**6.9**	An elevation of privilege vulnerability exists when the (Human Interface Device) HID Parser Library driver improperly handles objects in memory, aka "HIDParser Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE-ID:CVE-2018-8169**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8169	O-Mic-Windo/02-07-18/58
Overflow Memory Corruption	14-06-2018	**7.6**	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka "Media Foundation Memory Corruption Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows 8.1,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8251	O-Mic-Windo/02-07-18/59

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE-ID:CVE-2018-8251**		
Windows 10,Windows 7,Windows 8.1,Windows Server 2008,Windows Server 2012,Windows Server 2016					
Execute Code	14-06-2018	**9.3**	A remote code execution vulnerability exists in Windows Domain Name System (DNS) DNSAPI.dll when it fails to properly handle DNS responses, aka "Windows DNSAPI Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. **CVE-ID:CVE-2018-8225**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8225	O-Mic-Windo/02-07-18/60
Windows 10,Windows 8.1,Windows Rt 8.1,Windows Server 2012,Windows Server 2016					
Execute Code	14-06-2018	**7.2**	A remote code execution vulnerability exists when Windows improperly handles objects in memory, aka "Windows Remote Code Execution Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8213. **CVE-ID:CVE-2018-8210**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8210	O-Mic-Windo/02-07-18/61
Windows 10,Windows Server 2016					
NA	14-06-2018	**6.9**	An elevation of privilege vulnerability exists in Windows when Desktop Bridge does not properly manage the virtual registry, aka "Windows Desktop Bridge Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows 10 Servers. This CVE	https://www.exploit-db.com/exploits/44915/ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8214	O-Mic-Windo/02-07-18/62

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			ID is unique from CVE-2018-8208. **CVE-ID:CVE-2018-8214**		
NA	14-06-2018	**6.9**	An elevation of privilege vulnerability exists in Windows when Desktop Bridge does not properly manage the virtual registry, aka "Windows Desktop Bridge Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8214. **CVE-ID:CVE-2018-8208**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8208 https://www.exploit-db.com/exploits/44914/	O-Mic-Windo/02-07-18/63
NA	14-06-2018	**7.2**	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability." This affects Windows 10, Windows 10 Servers. **CVE-ID:CVE-2018-8233**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8233	O-Mic-Windo/02-07-18/64