Hive Pro

THREAT ADVISORY

Mozilla Firefox patches multiple vulnerabilities

TA2022007

Threat Level AMBER

Publish Date – Jan 12, 2022

Mozilla Firefox has released a major security update which patches 9 high, 6 moderate and 3 low impact vulnerabilities.

Vulnerabilities classified as high are:
- CVE-2022-22746: Callnnto reportValdty could ave lead to fullscreen wndow spoof
- CVE-2022-22743: Browser wndow spoof usnfullscreen mode
- CVE-2022-22742: Out-of-bounds memory access wen nsertntext n edt mode
- CVE-2022-22741: Browser wndow spoof usnfullscreen mode
- CVE-2022-22740: Use-after-free of CannelEventQueue::mOwner
- CVE-2022-22738: eap-buffer-overflow n blendaussanBlur
- CVE-2022-22737: Race condton wen playnaudo fles
- CVE-2021-4140 : frame sandbox bypass wtXSLT
- CVE-2022-22751: Memory safety bus

Vulnerabilities classified as moderate are:
- CVE-2022-22750:IPC passing of resource handles could have lead to sandbox bypass
- CVE-2022-22749:Lack of URL restrictions when scanning QR codes
- CVE-2022-22748:Spoofed origin on external protocol launch dialog
- CVE-2022-22745:Leaking cross-origin URLs through securitypolicyviolation event
- CVE-2022-22744:The 'Copy as curl' feature in DevTools did not fully escape website-controlled data, potentially leading to command injection
- CVE-2022-22752:Memory safety bugs

Vulnerabilities classified as low are:
- CVE-2022-22747: Crash when handling empty pkcs7 sequence
- CVE-2022-22736: Potential local privilege escalation when loading modules from the install directory.
- CVE-2022-22739: Missing throttling on external protocol launch dialog

All these vulnerability can be patched by upgrading to Mozilla Firefox 96, Mozilla Firefox ESR 91.5, and Mozilla Thunderbird 91.5

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-22746	Mozilla Firefox versions till 95.0.2, Mozilla Firefox ESR versions till 91.4.1, Mozilla Firefox Thunderbird versions till 91.4.1	cpe:2.3:a:mozilla:firefox:-:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*	Calling into reportValidity could have lead to fullscreen window spoof	CWE-1021
CVE-2022-22743			Browser window spoof using fullscreen mode	CWE-1021
CVE-2022-22742			Out-of-bounds memory access when inserting text in edit mode	CWE-787

Hive Pro

THREAT ADVISORY

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-22741	Mozilla Firefox versions till 95.0.2, Mozilla Firefox ESR versions till 91.4.1, Mozilla Firefox Thunderbird versions till 91.4.1	cpe:2.3:a:mozilla:firefox:-:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*	Browser window spoof using fullscreen mode	CWE-1021
CVE-2022-22740			Use-after-free of ChannelEventQueue::mOwner	CWE-416
CVE-2022-22738			Heap-buffer-overflow in blendGaussianBlur	CWE-122
CVE-2022-22737			Race condition when playing audio files	CWE-416
CVE-2021-4140			Iframe sandbox bypass with XSLT	CWE-254
CVE-2022-22750	Mozilla Firefox versions till 95.0.2	cpe:2.3:a:mozilla:firefox:-:*:*:*:*:*:*:*	IPC passing of resource handles could have lead to sandbox bypass	CWE-254
CVE-2022-22749			Lack of URL restrictions when scanning QR codes	CWE-20
CVE-2022-22748	Mozilla Firefox versions till 95.0.2, Mozilla Firefox ESR versions till 91.4.1, Mozilla Firefox Thunderbird versions till 91.4.1	cpe:2.3:a:mozilla:firefox:-:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*	Spoofed origin on external protocol launch dialog	CWE-451
CVE-2022-22745			Leaking cross-origin URLs through securitypolicyviolation event	CWE-200
CVE-2022-22744			The 'Copy as curl' feature in DevTools did not fully escape website-controlled data, potentially leading to command injection	CWE-78
CVE-2022-22747			Crash when handling empty pkcs7 sequence	CWE-20
CVE-2022-22736	Mozilla Firefox versions till 95.0.2	cpe:2.3:a:mozilla:firefox:-:*:*:*:*:*:*:*	Potential local privilege escalation when loading modules from the install directory.	CWE-428
CVE-2022-22739	Mozilla Firefox versions till 95.0.2, Mozilla Firefox ESR versions till 91.4.1, Mozilla Firefox Thunderbird versions till 91.4.1	cpe:2.3:a:mozilla:firefox:-:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*	Missing throttling on external protocol launch dialog	CWE-254

Hive Pro

THREAT ADVISORY

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-22751	Mozilla Firefox versions till 95.0.2, Mozilla Firefox ESR versions till 91.4.1	cpe:2.3:a:mozilla:firefox:-:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*	Memory safety vulnerability	CWE-119
CVE-2022-22752	Mozilla Firefox versions till 95.0.2	cpe:2.3:a:mozilla:firefox:-:*:*:*:*:*:*:*		CWE-119

References

https://www.mozilla.org/en-US/security/advisories/mfsa2022-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-02/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-03/
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/11/mozilla-releases-security-updates-firefox-firefox-esr-and