Hive Pro

THREAT ADVISORY

Mozilla release Security Advisories for multiple vulnerabilities affecting Firefox and Firefox ESR

TA2022054

Threat Level GREEN

Publish Date –March 9, 2022

Mozilla addressed multiple security vulnerabilities by releasing two security advisories and four of the bugs have high impact.

One of the four vulnerabilities is a Time-of-Check Time-of-Use bug (CVE-2022-26387), which occurs when installing an add-on and Firefox verifies the signature before prompting the user; however, while the user was confirming the prompt, the underlying add-on file could have been modified without Firefox noticing.

The second vulnerability(CVE-2022-26384) allows an attacker to control the contents of an iframe sandboxed with allow-popups but not allow-scripts, allowing them to build a link that, when clicked, will result in JavaScript execution outside of the sandbox.

Third in the lot, is a spoofing vulnerability that occurs when resizing a popup after requesting Fullscreen access, the popup would not display the Fullscreen notification

The last one is the Use-After-free flaw, which is a well-known vulnerability in browsers. An attacker can exploit this flaw to force a text reflow in an SVG object, potentially leading to a crash.

All these vulnerabilities has been patched in Firefox ESR 91.7 and Firefox 98

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-26384	Mozilla Firefox: 90.0 - 97.0.2 Firefox ESR: 91.0 - 91.6.1	cpe:2.3:a:mozilla:mozilla_firefox:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:10.0:*:*:*:*:*:*:*	iframe allow-scripts sandbox bypass	CWE-264
CVE-2022-26383			Browser window spoof using fullscreen mode	CWE-357
CVE-2022-26387			Time-of-check time-of-use bug when verifying add-on signatures	CWE-367
CVE-2022-26381			Use-after-free in text reflows	CWE-416

Patch Link

https://cdn.stubdownloader.services.mozilla.com/builds/firefox-stub/en-US/win/bb09da6defac4081f06e02ac17730b9b6f1e13db4315d371a03b167a2f4b3155/Firefox%20Installer.exe

References

https://www.mozilla.org/en-US/security/advisories/mfsa2022-11/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-10/