Hive Pro

THREAT ADVISORY

Multiple vulnerabilities affect Mozilla Firefox and Firefox ESR

TA2022030

Threat Level GREEN

Publish Date – Feb 11, 2022

Mozilla has issued two security advisories, which addresses 13 security issues in Firefox and Firefox ESR. Four of the thirteen have been rated as high, and some of these vulnerabilities, if successfully exploited, might allow an attacker to take entire control of an infected system.

One of the four with high-impact is a Time-of-Check Time-of-Use vulnerability in the Maintenance (Updater) Service (CVE-2022-22753) which can be abused to provide users write access to an arbitrary directory. Attackers may further utilize this to gain access to the system.

Two memory corruption vulnerabilities have been assigned CVE-2022-22764 and CVE-2022-0511. Attackers can take advantage of these flaws to execute arbitrary code on the targeted machine.

The fourth vulnerability which has been reported is a security bypass vulnerability and has been assigned CVE-2022-22754. This vulnerability exists in the browser's extensions and can be exploited when a user installs a specific sort of extension; the extension may have auto-updated itself and, in doing so, bypasses the prompt that allows the new required rights.

In addition to these, seven vulnerabilities have been categorized as moderate, and two of them have been categorized as low. All these flaws have been fixed in Firefox 97 and Firefox ESR 91.6. The following are the high impacted vulnerabilities:

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0511	Mozilla Firefox till 96.0.3	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*	Mozilla Firefox buffer overflow vulnerability	CWE-119
CVE-2022-22764	Mozilla Firefox till 96.0.3 and Firefox ESR till 91.5.1	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:* , cpe:2.3:a:mozilla:firefox_esr:10.0:*:*:*:*:*:*:*	Mozilla Firefox buffer overflow vulnerability	CWE-119
CVE-2022-22754			Mozilla Firefox security bypass vulnerability	CWE-264
CVE-2022-22753			Mozilla Firefox privilege escalation vulnerability	CWE-367

Patch Link

https://www.mozilla.org/en-US/security/advisories/mfsa2022-04/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-05/

References

https://www.cisa.gov/uscert/ncas/current-activity/2022/02/08/mozilla-releases-security-updates-firefox-and-firefox-esr