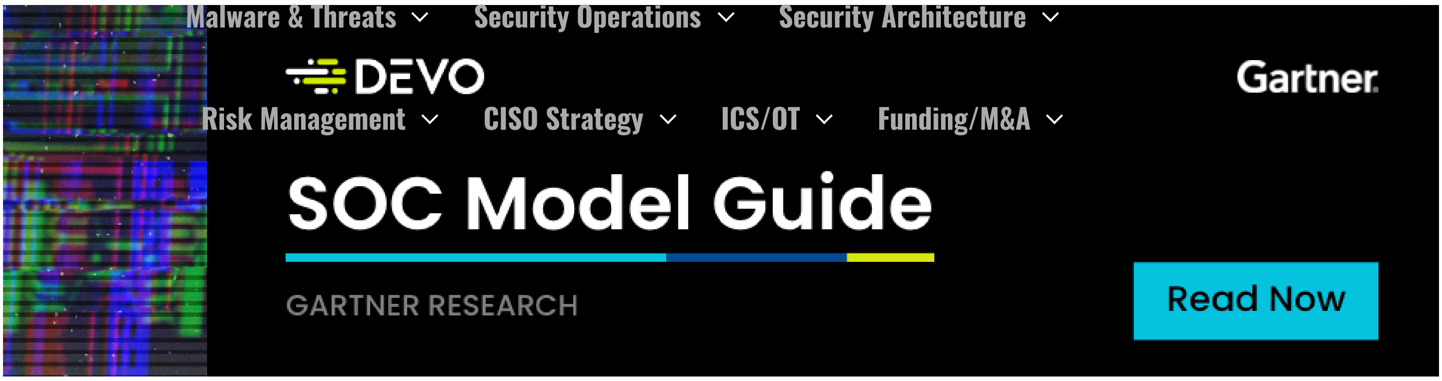

VULNERABILITIES

Firefox Updates Patch 10 High-Severity Vulnerabilities

Mozilla releases Firefox 110 and Firefox ESR 102.8 with patches for 10 high-severity vulnerabilities.

By Ionut Arghire
February 16, 2023

Mozilla this week announced the release of Firefox 110 and Firefox ESR 102.8 with patches for 10 high-severity vulnerabilities.

Tracked as CVE-2023-25728, the first of the security defects could result in an attacker being able to leak a child iframe's unredacted

TRENDING

1 Apple Patches Actively Exploited WebKit Zero-Day Vulnerability

2 Critical Vulnerability Patched in Cisco Security Products

3 Patch Tuesday: Microsoft Warns of Exploited Windows Zero-Days

4 Splunk Enterprise Updates Patch High-Severity Vulnerabilities

URI, provided that a redirect is triggered when interacting with that iframe.

The latest Firefox releases also resolve a flaw related to screen hijacking via browser fullscreen mode. Tracked as CVE-2023-25730, the issue exists because a background script could invoke the fullscreen mode and then block the main thread to force the mode indefinitely.

Successful exploitation of the vulnerability, Mozilla explains in its advisory, could result in potential user confusion or spoofing attacks.

The browser maker also resolved an issue in Firefox Focus, where fullscreen notifications would not be shown, thus potentially allowing malicious websites to spoof the browser chrome (CVE-2023-25743).

Another issue resolved this week can allow an attacker to craft a PKCS 12 certificate bundle so that it would allow for arbitrary memory writes via mishandling of PKCS 12 SafeBag attributes (CVE-2023-0767).

Mozilla also resolved a vulnerability in SpiderMonkey

5 Ransomware Attack Pushes City of Oakland Into State of Emergency

6 Surge in ESXiArgs Ransomware Attacks as Questions Linger Over Exploited Vulnerability

7 Microsoft OneNote Abuse for Malware Delivery Surges

8 Firefox Updates Patch 10 High-Severity Vulnerabilities

(CVE-2023-25735) that could result in cross-compartment wrappers causing the storing of objects from other compartments in the main compartment when wrapping a scripted proxy.

Tracked as CVE-2023-25735, the issue would trigger a use-after-free after the unwrapping of the proxy, Mozilla says.

Three other high-severity vulnerabilities resolved this week could lead to undefined behavior via an invalid downcast (CVE-2023-25737), Firefox crashes when printing on Windows (CVE-2023-25738), or a use-after-free due to a missing check on failed module load requests (CVE-2023-25739).

Additionally, Mozilla announced patches for multiple memory safety bugs impacting Firefox 109 and Firefox ESR 102.7, which are tracked collectively as CVE-2023-25744 and CVE-2023-25745.

Firefox 110 and Firefox ESR 102.8 also arrived with patches for several medium- and low-severity vulnerabilities.

Related: Firefox 107 Patches High-Impact Vulnerabilities

EXPERT INSIGHTS

Application Security Protection for the Masses

While there are many routes to application security, bundles that allow security teams to quickly and easily secure applications and affect security posture in a self-service manner are becoming increasingly popular. (Joshua Goldfarb)