



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates – Mozilla

Tracking #:432318860

Date:29-04-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Mozilla has released security updates to address multiple vulnerabilities in Firefox and Firefox ESR.

TECHNICAL DETAILS:

Mozilla has released security updates for Firefox and Firefox ESR to address multiple vulnerabilities, including critical memory safety flaws that may allow arbitrary code execution, an information disclosure issue in media processing, and a sandbox escape in WebRTC networking.

Vulnerability Details

Critical

- CVE-2026-7322 — Memory Safety Vulnerabilities

High

- CVE-2026-7320 — Information Disclosure in Audio/Video Component
- CVE-2026-7323 — Memory Safety Vulnerabilities
- CVE-2026-7324 — Memory Safety Vulnerabilities

Moderate

- CVE-2026-7321 — Sandbox Escape in WebRTC Networking Component

Multiple memory safety vulnerabilities in Firefox and Firefox ESR may result in memory corruption and could potentially be exploited for arbitrary code execution. An information disclosure flaw in the Audio/Video component may expose sensitive information, while a sandbox escape vulnerability in WebRTC networking could allow attackers to bypass browser isolation protections under specific conditions.

Fixed Versions

- Firefox 150.0.1
- Firefox ESR 140.10.1
- Firefox ESR 115.35.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends installing the latest versions released by Mozilla.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-35/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-36/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-37/>