مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – Mozilla

Tracking #:432318459

Date:25-02-2026

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 INTELLGIENCE 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, Firefox ESR and Thunderbird.

TECHNICAL DETAILS:

Mozilla has released security updates to address multiple vulnerabilities affecting Firefox, Firefox ESR and Thunderbird. Successful exploitation of these vulnerabilities could allow arbitrary code execution, information disclosure, sandbox escape, or system compromise.

High-Severity Vulnerabilities:

- **CVE-2026-2757** – Incorrect boundary conditions in WebRTC: Audio/Video component
- **CVE-2026-2794** – Information disclosure due to uninitialized memory in Firefox and Firefox Focus for Android
- **CVE-2026-2758, CVE-2026-2795, CVE-2026-2763, CVE-2026-2765, CVE-2026-2766, CVE-2026-2767, CVE-2026-2797** – Multiple use-after-free vulnerabilities in JavaScript Engine and GC components
- **CVE-2026-2759** – Incorrect boundary conditions in Graphics: ImageLib component
- **CVE-2026-2760, CVE-2026-2761, CVE-2026-2768, CVE-2026-2769, CVE-2026-2778** – Sandbox escape vulnerabilities in Graphics, Storage, and DOM components
- **CVE-2026-2762** – Integer overflow in JavaScript Standard Library
- **CVE-2026-2764, CVE-2026-2796** – JIT and WebAssembly miscompilation issues
- **CVE-2026-2770, CVE-2026-2798, CVE-2026-2799** – Use-after-free vulnerabilities in DOM Core, HTML, and WebIDL components
- **CVE-2026-2771** – Undefined behavior in DOM Core and HTML components
- **CVE-2026-2772, CVE-2026-2774** – Audio/Video processing vulnerabilities
- **CVE-2026-2773** – Web Audio component boundary condition flaw
- **CVE-2026-2775** – Mitigation bypass in HTML Parser component
- **CVE-2026-2776** – Sandbox escape via Telemetry component
- **CVE-2026-2777** – Privilege escalation in Messaging System component
- **CVE-2026-2790** – Same-origin policy bypass in Networking: JAR component
- **CVE-2026-2791** – Mitigation bypass in Networking: Cache component
- **CVE-2026-2806** – Uninitialized memory in Graphics: Text component
- **CVE-2026-2807, CVE-2026-2792, CVE-2026-2793** – Memory safety bugs that could allow arbitrary code execution

Fixed Versions:

- Firefox 148
- Firefox ESR 115.33
- Firefox ESR 140.8
- Thunderbird 148
- Thunderbird 140.8

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest updates 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/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/