مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates-Mozilla Products

Tracking #:432317321

Date:29-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Mozilla released a series of security advisories addressing multiple vulnerabilities across its Firefox and Thunderbird product lines, including Extended Support Releases (ESR).

TECHNICAL DETAILS:

Mozilla released a series of security advisories addressing multiple vulnerabilities across its Firefox and Thunderbird product lines, including Extended Support Releases (ESR). The most severe issue involves a double-free vulnerability in the libvpx encoder used for WebRTC, potentially leading to memory corruption and exploitable crashes. Other vulnerabilities encompass local code execution risks, cross-origin data leaks, and clickjacking threats. Immediate updates are strongly recommended to mitigate these risks.

Critical Vulnerability:

1. Double-Free in libvpx Encoder (**CVE-2025-5262**)
    - Impact: Critical
    - Description: A double-free could occur in vpx_codec_enc_init_multi after a failed allocation when initializing the encoder for WebRTC. This could lead to memory corruption and a potentially exploitable crash

Fixed Version:

- Firefox 139
- Firefox ESR 115.24 or 128.11
- Thunderbird 139 or 128.11

RECOMMENDATIONS:

- Users and administrators should promptly update to the latest versions for the affected products.

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/mfsa2025-42/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-43/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-44/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-45/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-46/