مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Mozilla

Tracking #:432316713

Date:08-01-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Mozilla has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Mozilla has issued security updates to fix several vulnerabilities in Firefox and Firefox ESR products. These flaws could allow attackers to spoof the address bar, exploit memory safety bugs, and potentially execute arbitrary code on affected systems.

High-Severity Vulnerabilities:

- CVE-2025-0244: Address Bar Spoofing on Firefox for Android
  - Impact: An attacker could spoof the address bar when redirecting to an invalid protocol scheme
  - Affected Systems: Firefox for Android only
- CVE-2025-0242: Memory Safety Bugs
  - Impact: Memory corruption issues that could potentially be exploited to run arbitrary code
  - Affected Products: Firefox, Thunderbird, Firefox ESR
- CVE-2025-0247: Memory Safety Bugs
  - Impact: Memory corruption issues that could potentially be exploited to run arbitrary code
  - Affected Products: Firefox, Thunderbird

Fixed Versions:

- Firefox 134
- Firefox ESR 128.6
- Firefox ESR 115.19

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently 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/mfsa2025-01/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-02/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-03/