مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Mozilla Products

Tracking #:432317149

Date:30-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Mozilla released security updates to address multiple vulnerabilities across Firefox, Firefox ESR, Thunderbird, and Thunderbird ESR, including privilege escalation flaws, memory corruption bugs, and sandbox escape risks.

TECHNICAL DETAILS:

Mozilla released security updates to address multiple vulnerabilities across Firefox, Firefox ESR, Thunderbird, and Thunderbird ESR, including privilege escalation flaws, memory corruption bugs, and sandbox escape risks.

Key Vulnerabilities and Mitigations

1. CVE-2025-2817: Privilege Escalation in Firefox Updater (High)

- **Description**: A medium-integrity process could manipulate Firefox's updater file-locking mechanism to execute SYSTEM-level operations, enabling privilege escalation.
- **Affected**: All Firefox, Firefox ESR, Thunderbird, and Thunderbird ESR versions prior to patches.
- **Fix**: Update to Firefox 138, Firefox ESR 128.10/115.23, or Thunderbird 138/128.10.

2. CVE-2025-4082: WebGL Shader Memory Corruption in macOS (High)

- **Description**: Malicious WebGL shader attributes could trigger out-of-bounds reads, enabling privilege escalation when chained with other exploits.
- **Affected**: Firefox and Firefox ESR for macOS only.

3. CVE-2025-4083: Process Isolation Bypass via JavaScript URIs (High)

- **Description**: Improper handling of javascript: URIs in cross-origin frames allowed content execution in the top-level process, enabling sandbox escapes.
- **Affected**: Firefox, Firefox ESR 115.23/128.10.

4. CVE-2025-4084: Local Code Execution via "Copy as cURL" (Moderate)

- **Description**: Insufficient escaping of ampersands in the "Copy as cURL" feature (Windows-only) allowed command injection.
- **Mitigation**: Avoid using this feature on untrusted sites until patched.

5. Memory Safety Bugs (CVE-2025-4091, 4092, 4093)

- **Risk**: Memory corruption vulnerabilities in Firefox 137/ESR 128.9/115.22 and Thunderbird 137/ESR 128.9 could lead to arbitrary code execution

Patched Versions:

Product	Patched Versions
Firefox	138
Firefox ESR	115.23, 128.10
Thunderbird	138
Thunderbird ESR	128.10

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to promptly update affected Mozilla Products to the latest versions.

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/mfsa2025-28/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-29/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-30/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-31/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-32/#CVE-2025-2817