مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – Mozilla Thunderbird and Firefox

Tracking #:432317355

Date:12-06-2025

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 for Firefox and Thunderbird to address multiple high-severity vulnerabilities. These vulnerabilities could allow attackers to execute arbitrary code, crash applications, exhaust disk space, and leak sensitive credentials.

TECHNICAL DETAILS:

Vulnerability Details:
Firefox

- **CVE-2025-49709: Memory Corruption in Canvas Surfaces**
  - **Severity:** High
  - **Impact:** Memory corruption could lead to arbitrary code execution or application crash.
- **CVE-2025-49710: Integer Overflow in OrderedHashTable**
  - **Severity:** High
  - **Impact:** Integer overflow in OrderedHashTable (JavaScript engine) could result in unexpected behavior or application crash.

Thunderbird

- **CVE-2025-5986: Unsolicited File Download, Disk Space Exhaustion, and Credential Leakage via mailbox:/// Links**
  - **Severity:** High
  - **Impact:** Crafted HTML emails with mailbox:/// links can trigger automatic downloads without user prompting. This can exhaust disk space and leak Windows credentials via SMB links when viewed in HTML mode.

Fixed Versions:

- Firefox 139.0.4
- Thunderbird 128.11.1
- Thunderbird 139.0.2

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/mfsa2025-47/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-49/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-50/