مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Firefox and Thunderbird
Tracking #:432317519
Date:23-07-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Mozilla has released security updates, addressing multiple high severity vulnerabilities in its products. The vulnerabilities may allow attackers to execute arbitrary code, manipulate browser behavior, or bypass security restrictions.

TECHNICAL DETAILS:

Vulnerability Details (including but not limited to):

- **CVE-2025-8027:** JavaScript engine only wrote partial return value to stack
  - **Severity**: High
  - **Description:** On 64-bit platforms IonMonkey-JIT only wrote 32 bits of the 64-bit return value space on the stack. Baseline-JIT, however, read the entire 64 bits.

- **CVE-2025-8028:** Large branch table could lead to truncated instruction
  - **Severity**: High
  - **Description:** On arm64, a WASM br_table instruction with a lot of entries could lead to the label being too far from the instruction causing truncation and incorrect computation of the branch address.

- **CVE-2025-8034:** Memory safety bugs
  - **Severity**: High
  - **Description:** These bugs showed evidence of memory corruption, and it is presumed that with enough effort some of these could have been exploited to run arbitrary code.

Affected Products:
- Thunderbird
- Firefox

Fixed Versions:
- Thunderbird 141
- Thunderbird 128.13
- Thunderbird 140.1
- Firefox 141
- Firefox ESR 115.26
- Firefox ESR 128.13
- Firefox ESR 140.1

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.

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

REFERENCES:

TLP: WHITE

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-57/#CVE-2025-8028
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-58/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-61/#CVE-2025-8029
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-62/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-63/