مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Mozilla Thunderbird

Tracking #:432316635

Date:16-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Mozilla has released security updates to address multiple vulnerabilities in Thunderbird. These vulnerabilities could potentially be exploited by malicious actors to compromise user systems or steal sensitive information.

TECHNICAL DETAILS:

Vulnerabilities Details:

CVE-2024-11691: Out-of-Bounds Write in Apple GPU Drivers via WebGL

- Severity-High
- A flaw in Apple's GPU driver on Apple Silicon M series devices could lead to out-of-bounds writes and memory corruption during certain WebGL operations. This issue only affects Apple M series hardware.

CVE-2024-11694: CSP Bypass and XSS Exposure via Web Compatibility Shims

- Severity- Moderate
- Enhanced Tracking Protection's Strict mode could inadvertently allow a CSP frame-src bypass and DOM-based XSS through the Google SafeFrame shim in the Web Compatibility extension, exposing users to malicious frames.

CVE-2024-50336: Insufficient MXC URI Validation in matrix-js-sdk

- Severity- Moderate
- The Matrix specification requires server-side validation of MXC URIs to prevent path traversal but does not mandate client-side validation. This flaw in matrix-js-sdk could allow a malicious room member to exploit client-side path traversal and issue arbitrary authenticated GET requests.

Fixed Versions:

- Thunderbird 115.18
- Thunderbird 128.5.2

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/mfsa2024-69/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-70/