مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Security Updates – Mozilla Firefox

Tracking #:432316057

Date:16-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-6606**: Out-of-bounds read in clipboard component- Clipboard code failed to check the index on an array access. This could have lead to an out-of-bounds read.
- **CVE-2024-6605**: Firefox Android missed activation delay to prevent tapjacking- Firefox Android allowed immediate interaction with permission prompts. This could be used for tapjacking.
- **CVE-2024-6604**: Memory safety bugs present in Firefox 127, Firefox ESR 115.12, and Thunderbird 115.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.

Fixed Versions:

- Firefox 128, Firefox ESR 115.13, and Thunderbird 115.13

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/mfsa2024-29/