مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Multiple Vulnerabilities Mozilla Products

Tracking #:432315793

Date:26-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Mozilla recently released security updates to patch multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Mozilla has released security updates to address multiple vulnerabilities in Firefox, Firefox ESR, and Thunderbird. These vulnerabilities could be exploited by malicious actors to gain unauthorized access to systems, steal data, or execute arbitrary code.

High-Severity Vulnerability Details:

- CVE-2024-3852: GetBoundName in the JIT returned the wrong object
- CVE-2024-3853: Use-after-free if garbage collection runs during realm initialization
- CVE-2024-3854: Out-of-bounds-read after mis-optimized switch statement
- CVE-2024-3855: Incorrect JIT optimization of MSubstr leads to out-of-bounds reads
- CVE-2024-3856: Use-after-free in WASM garbage collection
- CVE-2024-3857: Incorrect JITting of arguments led to use-after-free during garbage collection
- CVE-2024-3858: Corrupt pointer dereference in js::CheckTracedThing<js::Shape>
- CVE-2024-3864: Memory safety bug
- CVE-2024-3865: Memory safety bugs

Fixed Versions:

- Firefox 125
- Firefox ESR 115.10
- Thunderbird 115.10

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/mfsa2024-18/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-19/
- https://www.mozilla.org/en-US/security/advisories/mfsa2024-20/