



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Mozilla Security Updates**

Tracking #:432316124

Date:07-08-2024

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 INTELLIGENCE 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 to patch multiple vulnerabilities in its products.

## TECHNICAL DETAILS:

Mozilla has released security updates to address multiple vulnerabilities in Firefox, Firefox ESR, and Thunderbird products. These vulnerabilities could potentially allow an attacker to compromise affected systems.

### High-Severity Vulnerabilities Details:

- CVE-2024-7518: Fullscreen notification dialog can be obscured by document content
- CVE-2024-7519: Out of bounds memory access in graphics shared memory handling
- CVE-2024-7520: Type confusion in WebAssembly
- CVE-2024-7521: Incomplete WebAssembly exception handling
- CVE-2024-7522: Out of bounds read in editor component
- CVE-2024-7523: Document content could partially obscure security prompts
- CVE-2024-7524: CSP strict-dynamic bypass using web-compatibility shims
- CVE-2024-7525: Missing permission check when creating a StreamFilter
- CVE-2024-7526: Uninitialized memory used by WebGL
- CVE-2024-7527: Use-after-free in JavaScript garbage collection
- CVE-2024-7528: Use-after-free in IndexedDB

### Fixed Versions:

- Firefox 129
- Firefox ESR 115.14
- Firefox ESR 128.1
- Thunderbird 128.1
- Thunderbird 115.14

## 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/>