



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates - Mozilla**  
Tracking #:432316569  
Date:27-11-2024

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 important security updates to address multiple vulnerabilities in its Firefox, Firefox ESR, Firefox for iOS, and Thunderbird products. These vulnerabilities could potentially allow attackers to compromise affected systems.

### High-Severity Vulnerabilities:

- **CVE-2024-11691: Out-of-bounds write in Apple GPU drivers via WebGL**
  - A vulnerability exists in Apple GPU drivers that could lead to an out-of-bounds write and memory corruption when performing certain WebGL operations.
  - Impact: Memory corruption, potential arbitrary code execution
  - Affected Platforms: Apple Silicon M series devices
- **CVE-2024-11699: Memory safety bugs**
  - Memory safety bugs exist in Firefox and related products which could potentially be exploited to run arbitrary code on affected systems.
  - Impact: Potential arbitrary code execution
  - Affected Versions: Firefox 132, Firefox ESR 128.4, Thunderbird 128.4

### Other Notable Vulnerabilities:

- **CVE-2024-53975: SSL security padlock icon spoofing**
  - Severity: Moderate
  - Accessing a non-secure HTTP site using a non-existent port may cause the SSL padlock icon in the location URL bar to appear secure, potentially misleading users about the site's security status.
  - Impact: Misleading security indicator
  - Affected Versions: Firefox for iOS < 133
- **CVE-2024-53976: Missing address from location URL bar**
  - Severity: Moderate
  - Under specific conditions, navigating to a webpage could lead to the address being absent from the location URL bar. This could potentially expose users to malicious websites or phishing attacks, as it becomes difficult to verify the actual URL of the loaded page.
  - Impact: Unclear webpage origin
  - Affected Versions: Firefox for iOS < 133

### Fixed Versions:

- Firefox 133
- Firefox ESR 128.5
- Firefox ESR 115.18
- Firefox for iOS 133
- Thunderbird 133
- Thunderbird 128.5

## 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:

- <http://mozilla.org/en-US/security/advisories/mfsa2024-63/>
- <http://mozilla.org/en-US/security/advisories/mfsa2024-64/>
- <http://mozilla.org/en-US/security/advisories/mfsa2024-65/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2024-66/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2024-67/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2024-68/>