

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates – Mozilla**

Tracking #:432318262

Date:16-01-2026

## EXECUTIVE SUMMARY:

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

## TECHNICAL DETAILS:

Mozilla has released security updates for Firefox and Thunderbird addressing multiple high-severity vulnerabilities that could allow attackers to bypass security restrictions, escape sandboxes, or execute arbitrary code.

### High-Severity Vulnerabilities:

- CVE-2026-0877: Mitigation bypass in the DOM: Security component
- CVE-2026-0878: Sandbox escape due to incorrect boundary conditions in the Graphics: CanvasWebGL component
- CVE-2026-0879: Sandbox escape due to incorrect boundary conditions in the Graphics component
- CVE-2026-0880: Sandbox escape due to integer overflow in the Graphics component
- CVE-2026-0881: Sandbox escape in the Messaging System component
- CVE-2026-0882: Use-after-free in the IPC component
- CVE-2026-0891: Memory safety bugs fixed in Firefox ESR 140.7, Thunderbird ESR 140.7, Firefox 147 and Thunderbird 147

### Impact:

Exploitation of these vulnerabilities can lead to remote code execution, sandbox escape, security mitigation bypass, memory corruption, application crashes, and potential compromise of sensitive user data.

### Fixed Versions:

- Firefox 147
- Firefox ESR 115.32
- Firefox ESR 140.7
- Thunderbird 147
- Thunderbird 140.7

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest updates 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/mfsa2026-01/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2026-02/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2026-03/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2026-04/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2026-05/>