



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates – Mozilla Thunderbird

Tracking #:432318875

Date:02-05-2026

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 address multiple vulnerabilities in Thunderbird.

TECHNICAL DETAILS:

Mozilla has released security updates to address multiple vulnerabilities in Thunderbird, including critical memory safety flaws, information disclosure, and sandbox escape issues. Successful exploitation could lead to arbitrary code execution, sensitive information disclosure, or security boundary bypass in browser-like contexts.

Vulnerability Details

Critical Severity

- CVE-2026-7322: Memory safety bugs

High Severity

- CVE-2026-7320: Information disclosure due to incorrect boundary conditions in the Audio/Video component
- CVE-2026-7323: Memory safety bugs
- CVE-2026-7324: Memory safety bugs

Moderate Severity

- CVE-2026-7321: Sandbox escape due to incorrect boundary conditions in the WebRTC Networking component

Fixed Versions

- Thunderbird 150.0.1
- Thunderbird ESR 140.10.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends installing the latest versions 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/mfsa2026-38/>
- <https://www.mozilla.org/en-US/security/advisories/mfsa2026-39/>