

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerabilities in Mozilla Thunderbird

Tracking #:432319341

Date:26-07-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Mozilla has released security updates for Thunderbird to address numerous security vulnerabilities affecting the Thunderbird email client.

TECHNICAL DETAILS:

Mozilla has released Thunderbird 140.13 to address numerous security vulnerabilities affecting the Thunderbird email client. The update fixes over 30 vulnerabilities, including several critical flaws involving JavaScript, WebAssembly, DOM navigation, sandbox escapes, privilege escalation, memory corruption, and multiple memory safety issues.

While Mozilla notes that email-based exploitation is generally limited because scripting is disabled when reading email messages, several vulnerabilities remain significant in browser-like contexts, such as HTML rendering, embedded web content, extensions, and integrated browser components.

Two critical vulnerabilities (CVE-2026-15718 and CVE-2026-15719) are particularly noteworthy because public exploit code is available, although Mozilla reports no evidence of active exploitation in the wild at the time of disclosure.

Key Security Observations

- **31+ vulnerabilities** addressed in this release.
- **2 Critical vulnerabilities** with **public exploit code available**:
 - **CVE-2026-15718**
 - **CVE-2026-15719**
- Multiple **High-severity memory safety vulnerabilities** could potentially lead to arbitrary code execution.

Critical Vulnerabilities

1. CVE-2026-15718 – Invalid Pointer in JavaScript: WebAssembly Component
 - Severity: Critical
 - Description: A critical memory handling vulnerability exists within Thunderbird's JavaScript WebAssembly implementation due to improper pointer validation.
2. CVE-2026-15719 – Site Isolation Issue in DOM Navigation
 - Severity: Critical
 - Description: A flaw in the DOM Navigation component weakens site isolation protections.

Fixed Versions:

- Thunderbird ESR 140.13
- Thunderbird 153

RECOMMENDATIONS:

Immediate Actions:

- Upgrade immediately Thunderbird to fixed version or later.

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/mfsa2026-72/>