GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

31 August 2026

Advisory 211: Mozilla Firefox and Thunderbird Multiple Use-After-Free Vulnerabilities (CVE-2026-74936, CVE-2026-74940, CVE-2026-74943, CVE-2026-74944).

Release Date: 24th August 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

What is it?

CVE-2026-74936, CVE-2026-74940, CVE-2026-74943 and CVE-2026-74944 are four separate critical use-after-free memory-corruption vulnerabilities in Mozilla Firefox and Thunderbird, affecting the JavaScript WebAssembly engine, Graphics Text rendering, Graphics ImageLib, and DOM Core & HTML processing respectively. Each was fixed together in the same Mozilla security release.

A use-after-free occurs when code continues to reference memory after it has been freed; an attacker who can influence what is placed in that freed memory can potentially hijack program control flow. Malicious or compromised web content (or, for Thunderbird, malicious email content) can trigger any of these flaws simply by being viewed, with no further action needed from the user. All four carry a CVSS 3.1 score of 9.8 (Critical). Mozilla has not reported evidence of active exploitation for these specific CVEs.

What are the systems affected?

The following software and version(s) are affected:

- Mozilla Firefox prior to version 154 – (Affected)
- Mozilla Firefox ESR prior to 140.14 and 153.1 – (Affected)

Mozilla Thunderbird prior to version 154 is also affected.

- Firefox 154, Firefox ESR 140.14 / 153.1, and Thunderbird 154 – (Not affected, patched)

These four CVEs were part of a larger batch of memory-safety fixes in the same release. Mozilla's own advisories note some internally-discovered bugs in the release showed evidence of memory corruption and "we presume that with enough effort some of these could be exploited to run arbitrary code."

What does this mean?

Typical attack flow:

1. **Victim views malicious content**
    - The victim visits a malicious or compromised webpage, or opens a malicious email in Thunderbird — no further interaction is required to trigger the flaw.
2. **Memory corruption is triggered**
    - The vulnerable component frees a piece of memory but continues to reference it; an attacker who controls what fills that freed memory can potentially corrupt program state and, in the worst case, execute code.

Attack vectors:

- Malicious or compromised websites, viewed in Firefox
- Malicious email content or attachments, opened in Thunderbird

Successful exploitation may allow attackers to:

- Crash the browser or email client (denial of service)
- In the worst case, execute arbitrary code in the context of the browser or email client, potentially as a first step toward broader system compromise

Mitigation process

CERTVU recommends the following:

1. Update Firefox and Thunderbird Immediately

- Update to Firefox 154, Firefox ESR 140.14 or 153.1, and Thunderbird 154. Most consumer installs auto-update; organisation-managed deployments should confirm the update has been applied.
- Restart the browser or email client after updating for the fix to take effect.

2. Verify auto-update is enabled on managed devices, since browsers and email clients are among the most common initial-access vectors into an organisation.
3. Reinforce Phishing Awareness

- Remind staff to be cautious of unsolicited links and unexpected email attachments, since malicious content is the delivery mechanism for these flaws.

4. Confirm patch status across the estate, particularly on any systems still running unsupported or unmanaged browser/email client versions.
5. Monitor Mozilla's security advisories for any follow-up guidance on this release.

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.mozilla.org/en-US/security/advisories/mfsa2026-74/
2. https://www.mozilla.org/en-US/security/advisories/mfsa2026-78/