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

2 September 2026

Advisory 236: Mozilla Firefox and Thunderbird Sandbox Escape Vulnerability (CVE-2026-84119).

Release Date: 1st September 2026
Impact: CRITICAL
TLP: CLEAR

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

This alert is relevant to all Organizations and individual users that use Mozilla Firefox or Mozilla Thunderbird, including the Firefox Extended Support Release (ESR) branches commonly deployed in managed enterprise and government environments. This alert is intended to be understood by both technical and general users.

What is it?

CVE-2026-84119 (CVSS 3.1 base score 9.6, Critical, CWE-416: Use After Free) is a sandbox escape vulnerability caused by a use-after-free flaw in the DOM Navigation component of Mozilla Firefox and Thunderbird. An attacker who can get a user to interact with malicious web content can trigger the flaw to escape the browser's security sandbox, with no privileges required and no exploitation preconditions beyond a single user interaction.

CVE-2026-84119 was disclosed on 1 September 2026 as part of the Firefox 155 security release, which addresses 24 distinct vulnerabilities in total; this advisory covers CVE-2026-84119 specifically as the highest-severity issue in that batch. Mozilla rates the underlying bug as "High" impact and has not indicated that it is being actively exploited in the wild, but a sandbox escape is a significant class of vulnerability because it can allow an attacker to break out of the browser's

isolation and gain broader access to the host system, beyond what a compromised web page or email would normally be able to do.

What are the systems affected?

The following version(s) are affected:

- Mozilla Firefox before 155, and Firefox ESR before 115.40, 140.15, or 153.2 (depending on ESR branch) – (Affected)
- Mozilla Thunderbird before 155, and Thunderbird before 140.15 or 153.2 (depending on branch) – (Affected)

Firefox 155, Firefox ESR 115.40 / 140.15 / 153.2, and Thunderbird 155 / 140.15 / 153.2 – (Not affected, patched)

CERTVU verify Mozilla's own security advisory (MFSA 2026-82, and the related MFSA 2026-83 through 2026-88 covering the ESR and Thunderbird branches) is the authoritative source for these fixed versions and was fetched and confirmed directly. Firefox and Thunderbird update automatically by default; organizations managing deployments centrally should confirm their update policy has actually delivered version 155 (or the relevant ESR/Thunderbird fixed build) rather than assuming auto-update has already applied it.

What does this mean?

Typical attack flow:

1. **Lure the user to malicious content**
    - An attacker crafts a malicious web page or email message and gets a user of an affected Firefox or Thunderbird version to open or interact with it.
2. **Trigger the use-after-free and escape the sandbox**
    - The malicious content triggers the use-after-free flaw in the DOM Navigation component, allowing the attacker's code to escape the browser's sandbox and gain broader access to the host system than the sandboxed browsing context would normally allow.

Attack vectors:

- A malicious or compromised website visited in an affected Firefox version, requiring only a single user interaction to trigger.
- A malicious email opened or rendered in an affected Thunderbird version.

Successful exploitation may allow attackers to:

- Escape the browser or mail client's security sandbox, breaking the isolation that normally limits the impact of untrusted web or email content.
- Gain broader access to the affected system, with full confidentiality, integrity, and availability impact once the sandbox is escaped.

Mitigation process

CERTVU recommends the following:

1. Apply the Mozilla update without delay

    - Update Firefox to version 155 or later, and any Firefox ESR deployment to 115.40, 140.15, or 153.2 as applicable; update Thunderbird to 155, 140.15, or 153.2 as applicable. Confirm centrally-managed deployments have actually received the update rather than assuming automatic update has applied it.

2. Verify browser and mail-client versions across the estate
3. Encourage users to restart the browser/mail client after updating
4. Audit the estate for the affected products
5. Conduct a compromise assessment

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

Reference

1. https://www.mozilla.org/security/advisories/mfsa2026-82/
2. https://www.cve.org/CVERecord?id=CVE-2026-84119