

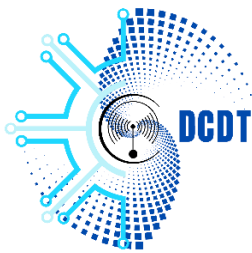
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

9 September 2026

Advisory 279: Mozilla Thunderbird Calendar Invitation File URI Attachment Execution Vulnerability (CVE-2026-84637).

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 users of the Mozilla Thunderbird email client, including Organizations, System/Network administrators, and members of the general public. This alert is intended to be understood by both technical and general readers.

What is it?

CVE-2026-84637 affects Mozilla Thunderbird's handling of calendar invitations. A malicious calendar invitation can carry a file URI attachment that, when opened, launches a local or network-hosted executable on Windows, bypassing Thunderbird's normal protections against opening executable attachments directly. With Thunderbird's newer invitation-display feature enabled, the malicious attachment can additionally be shown to the victim under a misleading, disguised filename. This is a separate Mozilla security release (MFSA 2026-87) from the Firefox 155 release already covered by CERTVU Advisory 236 (CVE-2026-84119) - noted here since both concern Mozilla products but address different components and different underlying bugs, so Advisory 236 does not already cover this issue.

What are the systems affected?

The following version(s) are affected:

- Mozilla Thunderbird prior to 153.2 - (Affected)
- Mozilla Thunderbird prior to 154 - (Affected)

Mozilla Thunderbird 153.2, 154, and later - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Send a malicious calendar invitation**
 - An attacker sends the victim a calendar invitation (e.g. via email) containing a crafted file URI attachment, optionally disguised with a misleading filename if the victim has Thunderbird's new invitation display enabled.
2. **Victim opens the attachment, executing the payload**
 - If the victim opens the disguised attachment, Thunderbird launches the referenced local or network-hosted executable on Windows, bypassing the normal protections that would otherwise block direct execution of an email attachment.

Attack vectors:

- An email-based social-engineering attack requiring the victim to receive and open a malicious calendar invitation in Thunderbird on Windows; Mozilla notes that Thunderbird's disabled mail-scripting model otherwise limits exploitation through ordinary email content.
- No privileges are required beyond the victim opening the malicious attachment (CVSS AV:N/PR:N/UI:N in the underlying CVE record, reflecting the network delivery vector; practical exploitation still depends on the victim interacting with the invitation).

Successful exploitation may allow attackers to:

- Launch an arbitrary local or network-hosted executable on the victim's Windows machine under a disguised filename, achieving code execution on the victim's device.
- Use the compromised Windows workstation as a foothold into any government or organizational network it is connected to.

Mitigation process

CERTVU recommends the following:

1. Update Thunderbird without delay

- Update Mozilla Thunderbird to version 153.2 or 154 (whichever release channel applies), and confirm the installed version directly (Help > About Thunderbird) rather than assuming it has already updated.

2. Treat unexpected calendar invitations with the same caution as email attachments
3. Prioritise Windows workstations running Thunderbird
4. Advise staff on the risk of disguised attachment filenames
5. Report suspected compromise

Report any suspected compromise following receipt of a suspicious calendar invitation in Thunderbird to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.mozilla.org/en-US/security/advisories/mfsa2026-87/>
2. <https://www.cve.org/CVERecord?id=CVE-2026-84637>