

Menu

Mozilla Security



# Mozilla Foundation Security Advisory 2025-10

## Security Vulnerabilities fixed in Thunderbird ESR 128.7

**Announced** February 4, 2025

**Impact** high

**Products** Thunderbird

**Fixed in** Thunderbird 128.7

*Flaws inherited from the Firefox code base are generally not exploitable through email in Thunderbird, as scripting is disabled when reading mail. However, they may pose a risk in other features that display remote web content.*

### # CVE-2025-1009: Use-after-free in XSLT

**Reporter** Ivan Fratric of Google Project Zero

**Impact** high

#### Description

An attacker could have caused a use-after-free via crafted XSLT data, leading to a potentially exploitable crash.

#### References

[Bug 1936613](#)

### # CVE-2025-1010: Use-after-free in Custom Highlight

**Reporter** Atte Kettunen

**Impact** high

**Description**

An attacker could have caused a use-after-free via the Custom Highlight API, leading to a potentially exploitable crash.

**References**

[Bug 1936982](#)

## # CVE-2025-1011: A bug in WebAssembly code generation could result in a crash

**Reporter** Nan Wang

**Impact** moderate

**Description**

A bug in WebAssembly code generation could have lead to a crash. It may have been possible for an attacker to leverage this to achieve code execution.

**References**

[Bug 1936454](#)

## # CVE-2025-1012: Use-after-free during concurrent delazification

**Reporter** Nils Bars

**Impact** moderate

**Description**

A race during concurrent delazification could have led to a use-after-free.

**References**

[Bug 1939710](#)

## # CVE-2024-11704: Potential double-free vulnerability in PKCS#7 decryption handling

**Reporter** Ronald Crane

**Impact** low

**Description**

A double-free issue could have occurred in `sec_pkcs7_decoder_start_decrypt()` when handling an error path. Under specific conditions, the same symmetric key could have been freed twice, potentially leading to memory corruption.

#### References

[Bug 1899402](#)

## # CVE-2025-1013: Potential opening of private browsing tabs in normal browsing windows

**Reporter** Maruf Bin Murtuza

**Impact**

#### Description

A race condition could have led to private browsing tabs being opened in normal browsing windows. This could have resulted in a potential privacy leak.

#### References

[Bug 1932555](#)

## # CVE-2025-1014: Certificate length was not properly checked

**Reporter** Theemathas

**Impact**

#### Description

Certificate length was not properly checked when added to a certificate store. In practice only trusted data was processed.

#### References

[Bug 1940804](#)

## # CVE-2025-1015: Unsanitized address book fields

**Reporter** r3m0t3nu11

**Impact**

#### Description

The Thunderbird Address Book URI fields contained unsanitized links. This could be used by an attacker to create and export an address book containing a malicious payload in a field. For example, in the “Other” field of the Instant Messaging section. If another user imported the address book, clicking on the link could result in opening a web page inside Thunderbird, and that page could execute (unprivileged) JavaScript.

#### References

[Bug 1939458](#)

## # CVE-2025-0510: Address of e-mail sender can be spoofed by malicious email

**Reporter** Fabian Densborn

**Impact** high

### Description

Thunderbird displayed an incorrect sender address if the From field of an email used the invalid group name syntax that is described in CVE-2024-49040.

### References

[Bug 1940570](#)

## # CVE-2025-1016: Memory safety bugs fixed in Firefox 135, Thunderbird 135, Firefox ESR 115.20, Firefox ESR 128.7, Thunderbird 115.20, and Thunderbird 128.7

**Reporter** Randell Jesup, Andrew McCreight, Andrew Osmond, Akmat Suleimanov and the Mozilla Fuzzing Team

**Impact** high

### Description

Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 115.19, Firefox ESR 128.6, Thunderbird 115.19, and Thunderbird 128.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.

### References

[Memory safety bugs fixed in Firefox 135, Thunderbird 135, Firefox ESR 115.20, Firefox ESR 128.7, Thunderbird 115.20, and Thunderbird 128.7](#)

## # CVE-2025-1017: Memory safety bugs fixed in Firefox 135, Thunderbird 135, Firefox ESR 128.7, and Thunderbird 128.7

**Reporter** Sebastian Hengst, Maurice Dauer and the Mozilla Fuzzing Team

**Impact** moderate

### Description

Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 128.6, and Thunderbird 128.6. Some of these bugs showed evidence of memory corruption and we

presume that with enough effort some of these could have been exploited to run arbitrary code.

## References

[Memory safety bugs fixed in Firefox 135, Thunderbird 135, Firefox ESR 128.7, and Thunderbird 128.7](#)

# Mozilla Ads

Add trust to your ad buy.

[Learn more →](#)

Company

Leadership

Press Center

Careers

Contact

Support

Product Help

File a Bug

Localize Mozilla

Security

Developers

Developer Edition

Enterprise

Tools

MDN

Firefox Release Notes

Follow @Mozilla



Follow @Firefox



[♥ Donate](#)

Visit [Mozilla Corporation's](#) not-for-profit parent, [Mozilla Foundation](#).

Portions of this content are ©1998–2026 by individual mozilla.org contributors. Content available under a [Creative Commons license](#).

[Website Privacy Notice](#)

[Cookies](#)

[Legal](#)

[Community Participation Guidelines](#)

[About this site](#)

# Mozilla