

Menu

Mozilla Security



Mozilla Foundation Security Advisory 2025-02

Security Vulnerabilities fixed in Firefox ESR 128.6

Announced January 7, 2025

Impact moderate

Products Firefox ESR

Fixed in Firefox ESR 128.6

CVE-2025-0237: WebChannel APIs susceptible to confused deputy attack

Reporter Andrew McCreight

Impact moderate

Description

The WebChannel API, which is used to transport various information across processes, did not check the sending principal but rather accepted the principal being sent. This could have led to privilege escalation attacks.

References

[Bug 1915257](#)

CVE-2025-0238: Use-after-free when breaking lines in text

Reporter Irvan Kurniawan

Impact moderate

Description

Assuming a controlled failed memory allocation, an attacker could have caused a use-after-free, leading to a potentially exploitable crash.

References

[Bug 1915535](#)

CVE-2025-0239: Alt-Svc ALPN validation failure when redirected

Reporter Paul Gerste

Impact moderate

Description

When using Alt-Svc, ALPN did not properly validate certificates when the original server is redirecting to an insecure site.

References

[Bug 1929156](#)

CVE-2025-0240: Compartment mismatch when parsing JavaScript JSON module

Reporter Nils Bars

Impact moderate

Description

Parsing a JavaScript module as JSON could under some circumstances cause cross-compartment access, which may result in a use-after-free.

References

[Bug 1929623](#)

CVE-2025-0241: Memory corruption when using JavaScript Text Segmentation

Reporter Nils Bars

Impact moderate

Description

When segmenting specially crafted text, segmentation would corrupt memory leading to a potentially exploitable crash.

References

[Bug 1933023](#)

CVE-2025-0242: Memory safety bugs fixed in Firefox 134, Thunderbird 134, Firefox ESR 115.19, Firefox ESR 128.6, Thunderbird 115.19, and Thunderbird 128.6

Reporter Andrew McCreight, Tooru Fujisawa, and the Mozilla Fuzzing Team

Impact high

Description

Memory safety bugs present in Firefox 133, Thunderbird 133, Firefox ESR 115.18, Firefox ESR 128.5, Thunderbird 115.18, and Thunderbird 128.5. 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 134, Thunderbird 134, Firefox ESR 115.19, Firefox ESR 128.6, Thunderbird 115.19, and Thunderbird 128.6](#)

CVE-2025-0243: Memory safety bugs fixed in Firefox 134, Thunderbird 134, Firefox ESR 128.6, and Thunderbird 128.6

Reporter Andrew Osmond and the Mozilla Fuzzing Team

Impact moderate

Description

Memory safety bugs present in Firefox 133, Thunderbird 133, Firefox ESR 128.5, and Thunderbird 128.5. 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 134, Thunderbird 134, Firefox ESR 128.6, and Thunderbird 128.6](#)

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](#)

