Mozilla Foundation Security Advisory 2025-09

Security Vulnerabilities fixed in Firefox ESR 128.7

Announced February 4, 2025

Impact high

Products Firefox ESR

Fixed in Firefox ESR 128.7

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 low

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 low

Description

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

References

Bug 1940804

CVE-2025-1016: 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

Donate

Visit Mozilla Corporation's not-for-profit parent, Mozilla Foundation.

Website Privacy Notice

Cookies

Legal

Community Participation Guidelines

About this site

Mozilla