

Menu

Mozilla Security



Mozilla Foundation Security Advisory 2026-33

Security Vulnerabilities fixed in Thunderbird 150

Announced April 21, 2026

Impact high

Products Thunderbird

Fixed in Thunderbird 150

In general, these flaws cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail, but are potentially risks in browser or browser-like contexts.

CVE-2026-6746: Use-after-free in the DOM: Core & HTML component

Reporter Evyatar Ben Asher, Keane Lucas, Nicholas Carlini, Newton Cheng, Daniel Freeman, Alex Gaynor, and Joel Weinberger using Claude from Anthropic

Impact high

References

[Bug 2014596](#)

CVE-2026-6747: Use-after-free in the WebRTC component

Reporter Nan Wang

Impact high

References

[Bug_2021769](#)

CVE-2026-6748: Uninitialized memory in the Audio/Video: Web Codecs component

Reporter Inseo An

Impact high

References

[Bug_2022604](#)

CVE-2026-6749: Information disclosure due to uninitialized memory in the Graphics: Canvas2D component

Reporter Inseo An

Impact high

References

[Bug_2022610](#)

CVE-2026-6750: Privilege escalation in the Graphics: WebRender component

Reporter choeseyeong

Impact high

References

[Bug_2023407](#)

CVE-2026-6751: Uninitialized memory in the Audio/Video: Web Codecs component

Reporter Joren Afman

Impact high

References

[Bug_2025883](#)

CVE-2026-6752: Incorrect boundary conditions in the WebRTC component

Reporter jmwebdevelopement

Impact high

References

[Bug_2027499](#)

CVE-2026-6753: Incorrect boundary conditions in the WebRTC component

Reporter jmwebdevelopement

Impact high

References

[Bug_2027501](#)

CVE-2026-6754: Use-after-free in the JavaScript Engine component

Reporter Xuehao Guo

Impact high

References

[Bug_2027541](#)

CVE-2026-6755: Mitigation bypass in the DOM: postMessage component

Reporter paranoidmoth

Impact moderate

References

[Bug_1880429](#)

CVE-2026-6757: Invalid pointer in the JavaScript: WebAssembly component

Reporter Evyatar Ben Asher, Keane Lucas, Nicholas Carlini, Newton Cheng, Daniel Freeman, Alex Gaynor, and Joel Weinberger using Claude from Anthropic

Impact moderate

References

[Bug_2013588](#)

CVE-2026-6758: Use-after-free in the JavaScript: WebAssembly component

Reporter Evyatar Ben Asher, Keane Lucas, Nicholas Carlini, Newton Cheng, Daniel Freeman, Alex Gaynor, and Joel Weinberger using Claude from Anthropic

Impact moderate

References

[Bug_2013619](#)

CVE-2026-6759: Use-after-free in the Widget: Cocoa component

Reporter Steven Michaud

Impact moderate

References

[Bug_2016164](#)

CVE-2026-6760: Mitigation bypass in the Networking: Cookies component

Reporter Richard Belisle

Impact moderate

References

[Bug_2016923](#)

CVE-2026-6761: Privilege escalation in the Networking component

Reporter kiyong

Impact moderate

References

[Bug_2017857](#)

CVE-2026-6762: Spoofing issue in the DOM: Core & HTML component

Reporter Farras Givari

Impact moderate

References

[Bug_2021080](#)

CVE-2026-6763: Mitigation bypass in the File Handling component

Reporter Tomoya Nakanishi

Impact moderate

References

[Bug_2021666](#)

CVE-2026-6764: Incorrect boundary conditions in the DOM: Device Interfaces component

Reporter Florian

Impact moderate

References

[Bug_2022162](#)

CVE-2026-6765: Information disclosure in the Form Autofill component

Reporter ABDULAZIZ ALASAIQAH

Impact moderate

References

[Bug_2022419](#)

CVE-2026-6766: Incorrect boundary conditions in the Libraries component in NSS

Reporter Haruto Kimura

Impact moderate

References

[Bug_2023207](#)

CVE-2026-6767: Other issue in the Libraries component in NSS

Reporter Haruto Kimura

Impact moderate

References

[Bug_2023209](#)

CVE-2026-6768: Mitigation bypass in the Networking: Cookies component

Reporter Satoki Tsuji

Impact moderate

References

[Bug_2023615](#)

CVE-2026-6769: Privilege escalation in the Debugger component

Reporter Tomoya Nakanishi

Impact moderate

References

[Bug_2023753](#)

CVE-2026-6770: Other issue in the Storage: IndexedDB component

Reporter Dai

Impact moderate

References

[Bug_2024220](#)

CVE-2026-6771: Mitigation bypass in the DOM: Security component

Reporter Rayhan Hanaputra

Impact moderate

References

[Bug_2025067](#)

CVE-2026-6772: Incorrect boundary conditions in the Libraries component in NSS

Reporter sseehra

Impact moderate

References

[Bug_2026089](#)

CVE-2026-6773: Denial-of-service due to integer overflow in the Graphics: WebGPU component

Reporter Richard Belisle

Impact low

References

[Bug_2015959](#)

CVE-2026-6774: Mitigation bypass in the DOM: Security component

Reporter lebr0nli

Impact low

References

[Bug_2016915](#)

CVE-2026-6775: Incorrect boundary conditions in the WebRTC component

Reporter Nan Wang

Impact low

References

[Bug_2021768](#)

CVE-2026-6776: Incorrect boundary conditions in the WebRTC: Networking component

Reporter Nan Wang

Impact low

References

[Bug_2021770](#)

CVE-2026-6777: Other issue in the Networking: DNS component

Reporter b00rito

Impact low

References

[Bug_2022726](#)

CVE-2026-6778: Invalid pointer in the Audio/Video: Playback component

Reporter chanhokim

Impact low

References

[Bug_2022746](#)

CVE-2026-6779: Other issue in the JavaScript Engine component

Reporter Gary Kwong

Impact low

References

[Bug_2023343](#)

CVE-2026-6780: Denial-of-service in the Audio/Video: Playback component

Reporter LatticeBased

Impact low

References

[Bug_2025179](#)

CVE-2026-6781: Denial-of-service in the Audio/Video: Playback component

Reporter LatticeBased

Impact low

References

[Bug_2025583](#)

CVE-2026-6782: Information disclosure in the IP Protection component

Reporter Yuki Umemura

Impact low

References

[Bug_2026571](#)

CVE-2026-6783: Incorrect boundary conditions, integer overflow in the Audio/Video: Playback component

Reporter crixer

Impact low

References

[Bug_2027564](#)

CVE-2026-7321: Sandbox escape due to incorrect boundary conditions in the WebRTC: Networking component

Reporter The Mozilla Fuzzing Team

Impact moderate

References

[Bug 2029461](#)

CVE-2026-6784: Memory safety bugs fixed in Firefox 150 and Thunderbird 150

Reporter Ben Visness, Brian Grinstead, Christian Holler, Dimi Lee, Jens Stutte, Jim Mathies, John Schanck, Jon Coppeard, Karl Tomlinson, Maurice Dauer, Nika Layzell, Randell Jesup, Tom Schuster and the Mozilla Fuzzing Team

Impact high

Description

Memory safety bugs present in Firefox 149 and Thunderbird 149. 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 150 and Thunderbird 150](#)

CVE-2026-6785: Memory safety bugs fixed in Firefox ESR 115.35, Firefox ESR 140.10, Thunderbird ESR 140.10, Firefox 150 and Thunderbird 150

Reporter Andrew McCreight, Ashley Zebrowski, Brian Grinstead, Christian Holler, Maurice Dauer, Tom Schuster and the Mozilla Fuzzing Team

Impact high

Description

Memory safety bugs present in Firefox ESR 115.34, Firefox ESR 140.9, Thunderbird ESR 140.9, Firefox 149 and Thunderbird 149. 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 ESR 115.35, Firefox ESR 140.10, Thunderbird ESR 140.10, Firefox 150 and Thunderbird 150](#)

CVE-2026-6786: Memory safety bugs fixed in Firefox ESR 140.10, Thunderbird ESR 140.10, Firefox 150 and Thunderbird 150

Reporter Alex Franchuk, Andrew McCreight, Brian Grinstead, Christian Holler, Jan de Mooij, Maurice Dauer, Sebastian Hengst, Tom Schuster and the Mozilla Fuzzing Team

Impact high

Description

Memory safety bugs present in Firefox ESR 140.9, Thunderbird ESR 140.9, Firefox 149 and Thunderbird 149. 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 ESR 140.10, Thunderbird ESR 140.10, Firefox 150 and Thunderbird 150](#)

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

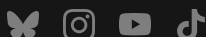
MDN

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