Mozilla Foundation Security Advisory 2026-13

Security Vulnerabilities fixed in Firefox 148

Announced February 24, 2026

Impact high

Products Firefox

Fixed in Firefox 148

CVE-2026-2757: Incorrect boundary conditions in the WebRTC: Audio/Video component

Reporter Igor Morgenstern

Impact high

References

Bug 2001637

CVE-2026-2794: Information disclosure due to uninitialized memory in Firefox and Firefox Focus for Android

Reporter Steven Julian

Impact high

References

Bug 2008365

CVE-2026-2758: Use-after-free in the JavaScript: GC component

Reporter Gary Kwong

Impact high

References

Bug 2009608

CVE-2026-2759: Incorrect boundary conditions in the Graphics: ImageLib component

Reporter Steven Julian

Impact high

References

Bug 2010933

CVE-2026-2795: Use-after-free in the JavaScript: GC component

Reporter x0e

Impact high

References

Bug 2010940

CVE-2026-2760: Sandbox escape due to incorrect boundary conditions in the Graphics: WebRender component

Reporter Oskar L

Impact high

References

Bug 2011062

CVE-2026-2761: Sandbox escape in the Graphics: WebRender component

Reporter Oskar L

Impact high

References

Bug 2011063

CVE-2026-2762: Integer overflow in the JavaScript: Standard Library component

Reporter André Bargull

Impact high

References

Bug 2011649

CVE-2026-2763: Use-after-free in the JavaScript Engine 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 2012018

CVE-2026-2764: JIT miscompilation, use-after-free in the JavaScript Engine: JIT 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 2012608

CVE-2026-2796: JIT miscompilation 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 high

References

Bug 2013165

CVE-2026-2797: Use-after-free in the JavaScript: GC 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 2013561

CVE-2026-2765: Use-after-free in the JavaScript Engine 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 2013562

CVE-2026-2766: Use-after-free in the JavaScript Engine: JIT 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 2013583

CVE-2026-2767: Use-after-free in the JavaScript: WebAssembly component

Reporter Sajeeb Lohani

Impact high

References

Bug 2013741

CVE-2026-2768: Sandbox escape in the Storage: IndexedDB component

Reporter Sajeeb Lohani

Impact high

References

Bug 2014101

CVE-2026-2798: Use-after-free in the DOM: Core & HTML component

Reporter Sajeeb Lohani

Impact high

References

Bug 2014136

CVE-2026-2769: Use-after-free in the Storage: IndexedDB 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 2014550

CVE-2026-2799: 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 2014551

CVE-2026-2770: Use-after-free in the DOM: Bindings (WebIDL) 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 2014585

CVE-2026-2771: Undefined behavior 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 2014593

CVE-2026-2772: Use-after-free in the Audio/Video: Playback 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 2014827

CVE-2026-2773: Incorrect boundary conditions in the Web Audio 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 2014832

CVE-2026-2774: Integer overflow in the Audio/Video 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 2014883

CVE-2026-2775: Mitigation bypass in the DOM: HTML Parser 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 2015199

CVE-2026-2776: Sandbox escape due to incorrect boundary conditions in the Telemetry component in External Software

Reporter Sajeeb Lohani

Impact high

References

Bug 2015266

CVE-2026-2777: Privilege escalation in the Messaging System component

Reporter Richard Belisle

Impact high

References

Bug 2015305

CVE-2026-2778: Sandbox escape due to incorrect boundary conditions in the DOM: Core & HTML component

Reporter Sajeeb Lohani

Impact high

References

Bug 2016358

CVE-2026-2779: Incorrect boundary conditions in the Networking: JAR component

Reporter Alex Mayorga

Impact moderate

References

Bug 1164141

CVE-2026-2800: Spoofing issue in the WebAuthn component in Firefox for Android

Reporter hafiizh & kang ali

Impact moderate

References

Bug 1988145

CVE-2026-2780: Privilege escalation in the Netmonitor component

Reporter RyotaK of GMO Flatt Security Inc.

Impact moderate

References

Bug 2007829

CVE-2026-2781: Integer overflow in the Libraries component in NSS

Reporter Clay Ver Valen

Impact moderate

References

Bug 2009552

CVE-2026-2801: Incorrect boundary conditions in the JavaScript: WebAssembly component

Reporter Kanaru Sato

Impact moderate

References

Bug 2009901

CVE-2026-2782: Privilege escalation in the Netmonitor component

Reporter Cody

Impact moderate

References

Bug 2010743

CVE-2026-2783: Information disclosure due to JIT miscompilation in the JavaScript Engine: JIT component

Reporter x0e

Impact moderate

References

Bug 2010943

CVE-2026-2802: Race condition in the JavaScript: GC component

Reporter Gary Kwong

Impact moderate

References

Bug 2011069

CVE-2026-2803: Information disclosure, mitigation bypass in the Settings UI component

Reporter Skywarp

Impact moderate

References

Bug 2012012

CVE-2026-2784: Mitigation bypass in the DOM: Security component

Reporter D. Santos

Impact moderate

References

Bug 2012984

CVE-2026-2785: Invalid pointer in the JavaScript Engine 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 2013549

CVE-2026-2804: 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 2013584

CVE-2026-2786: Use-after-free in the JavaScript Engine 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 2013612

CVE-2026-2805: Invalid pointer 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 moderate

References

Bug 2014549

CVE-2026-2787: Use-after-free in the DOM: Window and Location 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 2014560

CVE-2026-2788: Incorrect boundary conditions in the Audio/Video: GMP 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 2014824

CVE-2026-2789: Use-after-free in the Graphics: ImageLib 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 2015179

CVE-2026-2806: Uninitialized memory in the Graphics: Text component

Reporter Zijie Zhao

Impact low

References

Bug 2006199

CVE-2026-2790: Same-origin policy bypass in the Networking: JAR component

Reporter Surya Dev Singh

Impact low

References

Bug 2008426

CVE-2026-2791: Mitigation bypass in the Networking: Cache component

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

Impact low

References

Bug 2015220

CVE-2026-2807: Memory safety bugs fixed in Firefox 148 and Thunderbird 148

Reporter Agi Sferro, Andrew McCreight, Randell Jesup, Tom Schuster

Impact high

Description

Memory safety bugs present in Firefox 147 and Thunderbird 147. 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 148 and Thunderbird 148

CVE-2026-2792: Memory safety bugs fixed in Firefox ESR 140.8, Thunderbird ESR 140.8, Firefox 148 and Thunderbird 148

Reporter Andrew McCreight, Maurice Dauer, Olli Pettay, Ryan Hunt

Impact high

Description

Memory safety bugs present in Firefox ESR 140.7, Thunderbird ESR 140.7, Firefox 147 and Thunderbird 147. 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 140.8, Thunderbird ESR 140.8, Firefox 148 and Thunderbird 148

CVE-2026-2793: Memory safety bugs fixed in Firefox ESR 115.33, Firefox ESR 140.8, Thunderbird ESR 140.8, Firefox 148 and Thunderbird 148

Reporter Andrew McCreight, Christian Holler

Impact high

Description

Memory safety bugs present in Firefox ESR 115.32, Firefox ESR 140.7, Thunderbird ESR 140.7, Firefox 147 and Thunderbird 147. 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 115.33, Firefox ESR 140.8, Thunderbird ESR 140.8, Firefox 148 and Thunderbird 148

Mozilla Ads

Add trust to your ad buy.

Learn more →

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