Chrome Releases

Release updates from the Chrome team

Stable Channel Update for Desktop

Tuesday, May 5, 2026

The Chrome team is delighted to announce the promotion of Chrome 148 to the stable channel for Windows, Mac and Linux. This will roll out over the coming days/weeks.

Chrome 148.0.7778.96 (Linux) 148.0.7778.96/97 Windows/Mac contains a number of fixes and improvements -- a list of changes is available in the log. Watch out for upcoming Chrome and Chromium blog posts about new features and big efforts delivered in 148.

Security Fixes and Rewards

Note: Access to bug details and links may be kept restricted until a majority of users are updated with a fix. We will also retain restrictions if the bug exists in a third party library that other projects similarly depend on, but haven't yet fixed.

This update includes 127 security fixes. Below, we highlight fixes that were contributed by external researchers. Please see the Chrome Security Page for more information.

Many of our security bugs are detected using AddressSanitizer, MemorySanitizer, UndefinedBehaviorSanitizer, Control Flow Integrity, libFuzzer, or AFL.

[$43000][493747582] **Critical** CVE-2026-7896: Integer overflow in Blink. *Reported by c6eed09fc8b174b0f3eebedcceb1e792 on 2026-03-18*
[N/A][504069514] **Critical** CVE-2026-7897: Use after free in Mobile. *Reported by Google on 2026-04-18*
[N/A][504587882] **Critical** CVE-2026-7898: Use after free in Chromoting. *Reported by Google on 2026-04-20*
[$55000][505481948] **High** CVE-2026-7899: Out of bounds read and write in V8. *Reported by Project WhatForLunch (@pjwhatforlunch) on 2026-04-23*
[$16000][496503799] **High** CVE-2026-7900: Heap buffer overflow in ANGLE. *Reported by Anonymous on 2026-03-26*
[$16000][497724490] **High** CVE-2026-7901: Use after free in ANGLE. *Reported by Syn4pse (@ret2happy) on 2026-03-30*

[$8000][502030575] **High** CVE-2026-7902: Out of bounds memory access in V8. *Reported by JunYoung Park(@candymate) of KAIST Hacking Lab on 2026-04-13*

[TBD][491760376] **High** CVE-2026-7903: Integer overflow in ANGLE. *Reported by heesun on 2026-03-11*

[TBD][492350406] **High** CVE-2026-7904: Out of bounds read in Fonts. *Reported by c6eed09fc8b174b0f3eebedcceb1e792 on 2026-03-13*

[N/A][495259842] **High** CVE-2026-7905: Insufficient validation of untrusted input in Media. *Reported by Google on 2026-03-23*

[N/A][496284584] **High** CVE-2026-7906: Use after free in SVG. *Reported by Google on 2026-03-25*

[N/A][496292089] **High** CVE-2026-7907: Use after free in DOM. *Reported by Google on 2026-03-25*

[N/A][497436531] **High** CVE-2026-7908: Use after free in Fullscreen. *Reported by Google on 2026-03-29*

[N/A][497437113] **High** CVE-2026-7909: Inappropriate implementation in ServiceWorker. *Reported by Google on 2026-03-29*

[N/A][497543810] **High** CVE-2026-7910: Use after free in Views. *Reported by Google on 2026-03-29*

[N/A][497548912] **High** CVE-2026-7911: Use after free in Aura. *Reported by Google on 2026-03-29*

[N/A][497639714] **High** CVE-2026-7912: Integer overflow in GPU. *Reported by Google on 2026-03-30*

[N/A][497936728] **High** CVE-2026-7913: Insufficient policy enforcement in DevTools. *Reported by Google on 2026-03-30*

[N/A][498401609] **High** CVE-2026-7914: Type Confusion in Accessibility. *Reported by Google on 2026-04-01*

[N/A][498454478] **High** CVE-2026-7915: Insufficient data validation in DevTools. *Reported by Google on 2026-04-01*

[N/A][498720754] **High** CVE-2026-7916: Insufficient data validation in InterestGroups. *Reported by Google on 2026-04-01*

[N/A][498752242] **High** CVE-2026-7917: Use after free in Fullscreen. *Reported by Google on 2026-04-02*

[N/A][498780188] **High** CVE-2026-7918: Use after free in GPU. *Reported by Google on 2026-04-02*

[N/A][498832921] **High** CVE-2026-7919: Use after free in Aura. *Reported by Google on 2026-04-02*

[N/A][498989348] **High** CVE-2026-7920: Use after free in Skia. *Reported by Google on 2026-04-02*

[N/A][499062376] **High** CVE-2026-7921: Use after free in Passwords. *Reported by Google on 2026-04-02*

[N/A][499449324] **High** CVE-2026-7922: Use after free in ServiceWorker. *Reported by Google on 2026-04-04*
[N/A][500080194] **High** CVE-2026-7923: Out of bounds write in Skia. *Reported by Google on 2026-04-06*
[N/A][500087204] **High** CVE-2026-7924: Uninitialized Use in Dawn. *Reported by Google on 2026-04-06*
[N/A][501833981] **High** CVE-2026-7925: Use after free in Chromoting. *Reported by Google on 2026-04-12*
[TBD][502249087] **High** CVE-2026-7926: Use after free in PresentationAPI. *Reported by anonymous on 2026-04-14*
[N/A][502830119] **High** CVE-2026-7927: Type Confusion in Runtime. *Reported by Google on 2026-04-15*
[N/A][504612429] **High** CVE-2026-7928: Use after free in WebRTC. *Reported by Google on 2026-04-20*
[N/A][504660052] **High** CVE-2026-7929: Use after free in MediaRecording. *Reported by Google on 2026-04-20*
[TBD][434825208] **Medium** CVE-2026-7930: Insufficient validation of untrusted input in Cookies. *Reported by Satoki on 2025-07-29*
[TBD][474338157] **Medium** CVE-2026-7931: Insufficient validation of untrusted input in iOS. *Reported by Qadhafy Muhammad Tera on 2026-01-08*
[TBD][481634116] **Medium** CVE-2026-7932: Insufficient policy enforcement in Downloads. *Reported by Povcfe of Tencent Security Xuanwu Lab on 2026-02-04*
[TBD][488585490] **Medium** CVE-2026-7933: Out of bounds read in WebCodecs. *Reported by heapracer (@heapracer) on 2026-03-01*
[N/A][489023922] **Medium** CVE-2026-7934: Insufficient validation of untrusted input in Popup Blocker. *Reported by Google on 2026-03-02*
[TBD][489624550] **Medium** CVE-2026-7935: Inappropriate implementation in Speech. *Reported by Qadhafy Muhammad Tera on 2026-03-04*
[TBD][490485402] **Medium** CVE-2026-7936: Object lifecycle issue in V8. *Reported by Christian Holler on 2026-03-07*
[TBD][491766258] **Medium** CVE-2026-7937: Insufficient policy enforcement in DevTools. *Reported by lebr0nli of National Yang Ming Chiao Tung University, Dept. of CS, Security and Systems Lab on 2026-03-11*
[TBD][492735384] **Medium** CVE-2026-7938: Use after free in CSS. *Reported by c6eed09fc8b174b0f3eebedcceb1e792 on 2026-03-15*
[TBD][492963096] **Medium** CVE-2026-7939: Inappropriate implementation in SanitizerAPI. *Reported by s3zer0 on 2026-03-15*
[TBD][493631402] **Medium** CVE-2026-7940: Use after free in V8. *Reported by sakana on 2026-03-17*
[TBD][493955234] **Medium** CVE-2026-7941: Insufficient validation of untrusted input in Mobile. *Reported by Adithya Kotian on 2026-03-19*

[N/A][495363705] **Medium** CVE-2026-7942: Integer overflow in ANGLE. *Reported by Google on 2026-03-23*
[TBD][495373657] **Medium** CVE-2026-7943: Insufficient validation of untrusted input in ANGLE. *Reported by 86ac1f1587b71893ed2ad792cd7dde32 on 2026-03-23*
[N/A][495783187] **Medium** CVE-2026-7944: Insufficient validation of untrusted input in Persistent Cache. *Reported by Google on 2026-03-24*
[N/A][495802788] **Medium** CVE-2026-7945: Insufficient validation of untrusted input in COOP. *Reported by Google on 2026-03-24*
[N/A][496016840] **Medium** CVE-2026-7946: Insufficient policy enforcement in WebUI. *Reported by Google on 2026-03-25*
[N/A][496169594] **Medium** CVE-2026-7947: Insufficient validation of untrusted input in Network. *Reported by Google on 2026-03-25*
[N/A][496193452] **Medium** CVE-2026-7948: Race in Chromoting. *Reported by Google on 2026-03-25*
[N/A][496206134] **Medium** CVE-2026-7949: Out of bounds read in Skia. *Reported by Google on 2026-03-25*
[N/A][496259890] **Medium** CVE-2026-7950: Out of bounds read and write in GFX. *Reported by Google on 2026-03-25*
[TBD][496266456] **Medium** CVE-2026-7951: Out of bounds write in WebRTC. *Reported by soft.connect.fr on 2026-03-26*
[N/A][496279876] **Medium** CVE-2026-7952: Insufficient policy enforcement in Extensions. *Reported by Google on 2026-03-25*
[N/A][496379792] **Medium** CVE-2026-7953: Insufficient validation of untrusted input in Omnibox. *Reported by Google on 2026-03-26*
[N/A][496380960] **Medium** CVE-2026-7954: Race in Shared Storage. *Reported by Google on 2026-03-26*
[N/A][496441232] **Medium** CVE-2026-7955: Uninitialized Use in GPU. *Reported by Google on 2026-03-26*
[N/A][496463315] **Medium** CVE-2026-7956: Use after free in Navigation. *Reported by Google on 2026-03-26*
[N/A][496607380] **Medium** CVE-2026-7957: Out of bounds write in Media. *Reported by Google on 2026-03-26*
[N/A][496632973] **Medium** CVE-2026-7958: Inappropriate implementation in ServiceWorker. *Reported by Google on 2026-03-26*
[N/A][496645205] **Medium** CVE-2026-7959: Inappropriate implementation in Navigation. *Reported by Google on 2026-03-26*
[N/A][497007825] **Medium** CVE-2026-7960: Race in Speech. *Reported by Google on 2026-03-27*
[N/A][497008295] **Medium** CVE-2026-7961: Insufficient validation of untrusted input in Permissions. *Reported by Google on 2026-03-27*

[N/A][497081987] **Medium** CVE-2026-7962: Insufficient policy enforcement in DirectSockets. *Reported by Google on 2026-03-28*
[N/A][497250399] **Medium** CVE-2026-7963: Inappropriate implementation in ServiceWorker. *Reported by Google on 2026-03-28*
[N/A][497254383] **Medium** CVE-2026-7964: Insufficient validation of untrusted input in FileSystem. *Reported by Google on 2026-03-28*
[N/A][497255035] **Medium** CVE-2026-7965: Insufficient validation of untrusted input in DevTools. *Reported by Google on 2026-03-28*
[N/A][497341787] **Medium** CVE-2026-7966: Insufficient validation of untrusted input in SiteIsolation. *Reported by Google on 2026-03-29*
[N/A][497365545] **Medium** CVE-2026-7967: Insufficient validation of untrusted input in Navigation. *Reported by Google on 2026-03-29*
[N/A][497432281] **Medium** CVE-2026-7968: Insufficient validation of untrusted input in CORS. *Reported by Google on 2026-03-29*
[N/A][497450574] **Medium** CVE-2026-7969: Integer overflow in Network. *Reported by Google on 2026-03-29*
[N/A][497487462] **Medium** CVE-2026-7970: Use after free in TopChrome. *Reported by Google on 2026-03-29*
[N/A][497529290] **Medium** CVE-2026-7971: Inappropriate implementation in ORB. *Reported by Google on 2026-03-29*
[N/A][497546281] **Medium** CVE-2026-7972: Uninitialized Use in GPU. *Reported by Google on 2026-03-29*
[N/A][497565944] **Medium** CVE-2026-7973: Integer overflow in Dawn. *Reported by Google on 2026-03-29*
[N/A][497649372] **Medium** CVE-2026-7974: Use after free in Blink. *Reported by Google on 2026-03-30*
[N/A][497735587] **Medium** CVE-2026-7975: Use after free in DevTools. *Reported by Google on 2026-03-30*
[N/A][497736679] **Medium** CVE-2026-7976: Use after free in Views. *Reported by Google on 2026-03-30*
[N/A][497821223] **Medium** CVE-2026-7977: Inappropriate implementation in Canvas. *Reported by Google on 2026-03-30*
[N/A][497828892] **Medium** CVE-2026-7978: Inappropriate implementation in Companion. *Reported by Google on 2026-03-30*
[N/A][497849876] **Medium** CVE-2026-7979: Inappropriate implementation in Media. *Reported by Google on 2026-03-30*
[N/A][497859275] **Medium** CVE-2026-7980: Use after free in WebAudio. *Reported by Google on 2026-03-30*
[N/A][497926602] **Medium** CVE-2026-7981: Out of bounds read in Codecs. *Reported by Google on 2026-03-30*

[N/A][497952533] **Medium** CVE-2026-7982: Uninitialized Use in WebCodecs. *Reported by Google on 2026-03-30*
[N/A][497975608] **Medium** CVE-2026-7983: Out of bounds read in Dawn. *Reported by Google on 2026-03-31*
[N/A][498277368] **Medium** CVE-2026-7984: Use after free in ReadingMode. *Reported by Google on 2026-03-31*
[N/A][498352423] **Medium** CVE-2026-7985: Use after free in GPU. *Reported by Google on 2026-03-31*
[N/A][498396238] **Medium** CVE-2026-7986: Insufficient policy enforcement in Autofill. *Reported by Google on 2026-04-01*
[N/A][498696266] **Medium** CVE-2026-7987: Use after free in WebRTC. *Reported by Google on 2026-04-01*
[N/A][498753456] **Medium** CVE-2026-7988: Type Confusion in WebRTC. *Reported by Google on 2026-04-02*
[N/A][498765082] **Medium** CVE-2026-7989: Insufficient data validation in DataTransfer. *Reported by Google on 2026-04-02*
[N/A][498892267] **Medium** CVE-2026-7990: Insufficient validation of untrusted input in Updater. *Reported by Google on 2026-04-02*
[N/A][499065126] **Medium** CVE-2026-7991: Use after free in UI. *Reported by Google on 2026-04-02*
[N/A][499067529] **Medium** CVE-2026-7992: Insufficient validation of untrusted input in UI. *Reported by Google on 2026-04-02*
[N/A][499099003] **Medium** CVE-2026-7993: Insufficient validation of untrusted input in Payments. *Reported by Google on 2026-04-03*
[N/A][499116954] **Medium** CVE-2026-7994: Inappropriate implementation in Chromoting. *Reported by Google on 2026-04-03*
[N/A][501745798] **Medium** CVE-2026-7995: Out of bounds read in AdFilter. *Reported by Google on 2026-04-11*
[TBD][484547631] **Low** CVE-2026-7996: Insufficient validation of untrusted input in SSL. *Reported by heesun on 2026-02-15*
[TBD][487960705] **Low** CVE-2026-7997: Insufficient validation of untrusted input in Updater. *Reported by ochkofficial on 2026-02-26*
[TBD][491676472] **Low** CVE-2026-7998: Insufficient validation of untrusted input in Dialog. *Reported by Tianyi Hu on 2026-03-11*
[TBD][493099941] **Low** CVE-2026-7999: Inappropriate implementation in V8. *Reported by Taisic Yun (@taisic) of Theori on 2026-03-16*
[TBD][494464734] **Low** CVE-2026-8000: Insufficient validation of untrusted input in ChromeDriver. *Reported by Ryan Jupp - HAAO on 2026-03-20*
[TBD][494764371] **Low** CVE-2026-8001: Use after free in Printing. *Reported by c6eed09fc8b174b0f3eebedcceb1e792 on 2026-03-21*

[N/A][495779613] **Low** CVE-2026-8002: Use after free in Audio. *Reported by Google on 2026-03-24*
[N/A][495985532] **Low** CVE-2026-8003: Insufficient validation of untrusted input in TabGroups. *Reported by Google on 2026-03-25*
[N/A][496189510] **Low** CVE-2026-8004: Insufficient policy enforcement in DevTools. *Reported by Google on 2026-03-25*
[N/A][496298665] **Low** CVE-2026-8005: Insufficient validation of untrusted input in Cast. *Reported by Google on 2026-03-25*
[N/A][496373088] **Low** CVE-2026-8006: Insufficient policy enforcement in DevTools. *Reported by Google on 2026-03-26*
[N/A][496399759] **Low** CVE-2026-8007: Insufficient validation of untrusted input in Cast. *Reported by Google on 2026-03-26*
[N/A][496426191] **Low** CVE-2026-8008: Inappropriate implementation in DevTools. *Reported by Google on 2026-03-26*
[N/A][496555077] **Low** CVE-2026-8009: Inappropriate implementation in Cast. *Reported by Google on 2026-03-26*
[N/A][496624084] **Low** CVE-2026-8010: Insufficient validation of untrusted input in SiteIsolation. *Reported by Google on 2026-03-26*
[N/A][496626029] **Low** CVE-2026-8011: Insufficient policy enforcement in Search. *Reported by Google on 2026-03-26*
[N/A][496628298] **Low** CVE-2026-8012: Inappropriate implementation in MHTML. *Reported by Google on 2026-03-26*
[N/A][497427430] **Low** CVE-2026-8013: Insufficient validation of untrusted input in FedCM. *Reported by Google on 2026-03-29*
[N/A][497490364] **Low** CVE-2026-8014: Inappropriate implementation in Preload. *Reported by Google on 2026-03-29*
[N/A][497548558] **Low** CVE-2026-8015: Inappropriate implementation in Media. *Reported by Google on 2026-03-29*
[N/A][497695401] **Low** CVE-2026-8016: Use after free in WebRTC. *Reported by Google on 2026-03-30*
[N/A][497722578] **Low** CVE-2026-8017: Side-channel information leakage in Media. *Reported by Google on 2026-03-30*
[N/A][498292657] **Low** CVE-2026-8018: Insufficient policy enforcement in DevTools. *Reported by Google on 2026-03-31*
[N/A][498353173] **Low** CVE-2026-8019: Insufficient policy enforcement in WebApp. *Reported by Google on 2026-03-31*
[N/A][498382925] **Low** CVE-2026-8020: Uninitialized Use in GPU. *Reported by Google on 2026-04-01*
[N/A][498417031] **Low** CVE-2026-8021: Script injection in UI. *Reported by Google on 2026-04-01*

[N/A][499194407] **Low** CVE-2026-8022: Inappropriate implementation in MHTML. *Reported by Google on 2026-04-03*

We would also like to thank all security researchers that worked with us during the development cycle to prevent security bugs from ever reaching the stable channel.

Interested in switching release channels? Find out how here. If you find a new issue, please let us know by filing a bug. The community help forum is also a great place to reach out for help or learn about common issues.

Srinivas Sista
Google Chrome

Labels: Desktop Update , Extended Stable updates , Stable updates