# Chrome Releases

Release updates from the Chrome team

# Stable Channel Update for Desktop

Tuesday, April 7, 2026

The Chrome team is delighted to announce the promotion of Chrome 147 to the stable channel for Windows, Mac and Linux. This will roll out over the coming days/weeks.

Chrome 147.0.7727.55 (Linux) 147.0.7727.55/56 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 147.

## 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 multiple security fixes. Please see the Chrome Security Page for more information.

[$43000][493319454] **Critical** CVE-2026-5858: Heap buffer overflow in WebML. *Reported by c6eed09fc8b174b0f3eebedcceb1e792 on 2026-03-17*
[$43000][494158331] **Critical** CVE-2026-5859: Integer overflow in WebML. *Reported by Anonymous on 2026-03-19*
[$11000][486495143] **High** CVE-2026-5860: Use after free in WebRTC. *Reported by c6eed09fc8b174b0f3eebedcceb1e792 on 2026-02-22*
[$3000][486927780] **High** CVE-2026-5861: Use after free in V8. *Reported by 5shain on 2026-02-23*
[TBD][470566252] **High** CVE-2026-5862: Inappropriate implementation in V8. *Reported by Google on 2025-12-21*
[TBD][484527367] **High** CVE-2026-5863: Inappropriate implementation in V8. *Reported by Google on 2026-02-14*
[TBD][490642831] **High** CVE-2026-5864: Heap buffer overflow in WebAudio. *Reported by Syn4pse on 2026-03-08*
[TBD][491884710] **High** CVE-2026-5865: Type Confusion in V8. *Reported by Project WhatForLunch (@pjwhatforlunch) on 2026-03-12*
[TBD][492218537] **High** CVE-2026-5866: Use after free in Media. *Reported by c6eed09fc8b174b0f3eebedcceb1e792 on 2026-03-13*

[TBD][492668885] **High** CVE-2026-5867: Heap buffer overflow in WebML. *Reported by Syn4pse on 2026-03-14*

[TBD][493256564] **High** CVE-2026-5868: Heap buffer overflow in ANGLE. *Reported by cinzinga on 2026-03-16*

[TBD][493708165] **High** CVE-2026-5869: Heap buffer overflow in WebML. *Reported by c6eed09fc8b174b0f3eebedcceb1e792 on 2026-03-18*

[TBD][495534710] **High** CVE-2026-5870: Integer overflow in Skia. *Reported by Google on 2026-03-23*

[TBD][495679730] **High** CVE-2026-5871: Type Confusion in V8. *Reported by Google on 2026-03-24*

[TBD][496281816] **High** CVE-2026-5872: Use after free in Blink. *Reported by Google on 2026-03-25*

[TBD][496301615] **High** CVE-2026-5873: Out of bounds read and write in V8. *Reported by Google on 2026-03-25*

[$11000][485397279] **Medium** CVE-2026-5874: Use after free in PrivateAI. *Reported by Krace on 2026-02-18*

[$4000][430198264] **Medium** CVE-2026-5875: Policy bypass in Blink. *Reported by Lyra Rebane (rebane2001) on 2025-07-08*

[$2000][41485206] **Medium** CVE-2026-5876: Side-channel information leakage in Navigation. *Reported by Lyra Rebane (rebane2001) on 2023-12-18*

[TBD][333024273] **Medium** CVE-2026-5877: Use after free in Navigation. *Reported by Cassidy Kim(@cassidy6564) on 2024-04-05*

[TBD][365089001] **Medium** CVE-2026-5878: Incorrect security UI in Blink. *Reported by Shaheen Fazim on 2024-09-06*

[TBD][40073848] **Medium** CVE-2026-5879: Insufficient validation of untrusted input in ANGLE. *Reported by parkminchan, working for SSD Labs Korea on 2023-10-01*

[TBD][424995036] **Medium** CVE-2026-5880: Incorrect security UI in browser UI. *Reported by Anonymous on 2025-06-14*

[TBD][454162508] **Medium** CVE-2026-5881: Policy bypass in LocalNetworkAccess. *Reported by asnine on 2025-10-22*

[TBD][480993682] **Medium** CVE-2026-5882: Incorrect security UI in Fullscreen. *Reported by Anonymous on 2026-02-02*

[TBD][482958590] **Medium** CVE-2026-5883: Use after free in Media. *Reported by sherkito on 2026-02-09*

[TBD][484547633] **Medium** CVE-2026-5884: Insufficient validation of untrusted input in Media. *Reported by xmzyshypnc on 2026-02-15*

[TBD][485203823] **Medium** CVE-2026-5885: Insufficient validation of untrusted input in WebML. *Reported by Bryan Bernhart on 2026-02-17*

[TBD][485397283] **Medium** CVE-2026-5886: Out of bounds read in WebAudio. *Reported by c6eed09fc8b174b0f3eebedcceb1e792 on 2026-02-18*

[TBD][486079015] **Medium** CVE-2026-5887: Insufficient validation of untrusted input in Downloads. *Reported by daffainfo on 2026-02-20*

[TBD][486506202] **Medium** CVE-2026-5888: Uninitialized Use in WebCodecs. *Reported by Identified by the Octane Security Team: Giovanni Vignone, Paolo Gentry, Robert van Eijk on 2026-02-22*

[TBD][486906037] **Medium** CVE-2026-5889: Cryptographic Flaw in PDFium. *Reported by mlafon on 2026-02-23*

[TBD][487259772] **Medium** CVE-2026-5890: Race in WebCodecs. *Reported by Casper Woudenberg on 2026-02-24*

[TBD][487471101] **Medium** CVE-2026-5891: Insufficient policy enforcement in browser UI. *Reported by Tianyi Hu on 2026-02-25*

[TBD][487568011] **Medium** CVE-2026-5892: Insufficient policy enforcement in PWAs. *Reported by Tianyi Hu on 2026-02-25*

[TBD][487768771] **Medium** CVE-2026-5893: Race in V8. *Reported by QYmag1c on 2026-02-26*

[$1000][481882038] **Low** CVE-2026-5894: Inappropriate implementation in PDF. *Reported by Povcfe of Tencent Security Xuanwu Lab on 2026-02-05*

[TBD][374285495] **Low** CVE-2026-5895: Incorrect security UI in Omnibox. *Reported by Renwa Hiwa @RenwaX23 on 2024-10-18*

[TBD][40064543] **Low** CVE-2026-5896: Policy bypass in Audio. *Reported by Luan Herrera (@lbherrera_) on 2023-05-13*

[TBD][419921726] **Low** CVE-2026-5897: Incorrect security UI in Downloads. *Reported by Farras Givari on 2025-05-24*

[TBD][470295118] **Low** CVE-2026-5898: Incorrect security UI in Omnibox. *Reported by saidinahikam032 on 2025-12-19*

[TBD][474817168] **Low** CVE-2026-5899: Incorrect security UI in History Navigation. *Reported by Islam Rzayev on 2026-01-11*

[TBD][475265304] **Low** CVE-2026-5900: Policy bypass in Downloads. *Reported by Luan Herrera (@lbherrera_) on 2026-01-13*

[TBD][479673903] **Low** CVE-2026-5901: Policy bypass in DevTools. *Reported by Povcfe of Tencent Security Xuanwu Lab on 2026-01-29*

[TBD][483109205] **Low** CVE-2026-5902: Race in Media. *Reported by Luke Francis on 2026-02-10*

[TBD][483771899] **Low** CVE-2026-5903: Policy bypass in IFrameSandbox. *Reported by @Ciarands on 2026-02-11*

[TBD][483851888] **Low** CVE-2026-5904: Use after free in V8. *Reported by Zhenpeng (Leo) Lin at depthfirst on 2026-02-12*

[TBD][483899628] **Low** CVE-2026-5905: Incorrect security UI in Permissions. *Reported by daffainfo on 2026-02-12*

[TBD][484082189] **Low** CVE-2026-5906: Incorrect security UI in Omnibox. *Reported by mohamedhesham9173 on 2026-02-13*

[TBD][484665123] **Low** CVE-2026-5907: Insufficient data validation in Media. *Reported by Luke Francis on 2026-02-15*
[TBD][485115554] **Low** CVE-2026-5908: Integer overflow in Media. *Reported by Ameen Basha M K & Mohammed Yasar B on 2026-02-17*
[TBD][485203821] **Low** CVE-2026-5909: Integer overflow in Media. *Reported by Mohammed Yasar B & Ameen Basha M K on 2026-02-17*
[TBD][485212874] **Low** CVE-2026-5910: Integer overflow in Media. *Reported by Ameen Basha M K & Mohammed Yasar B on 2026-02-17*
[TBD][485785246] **Low** CVE-2026-5911: Policy bypass in ServiceWorkers. *Reported by lebr0nli of National Yang Ming Chiao Tung University, Dept. of CS, Security and Systems Lab on 2026-02-19*
[TBD][486498791] **Low** CVE-2026-5912: Integer overflow in WebRTC. *Reported by c6eed09fc8b174b0f3eebedcceb1e792 on 2026-02-22*
[TBD][487195286] **Low** CVE-2026-5913: Out of bounds read in Blink. *Reported by Vitaly Simonovich on 2026-02-24*
[TBD][490023239] **Low** CVE-2026-5914: Type Confusion in CSS. *Reported by Syn4pse on 2026-03-05*
[TBD][494341335] **Low** CVE-2026-5915: Insufficient validation of untrusted input in WebML. *Reported by ningxin.hu@intel.com on 2026-03-20*
[TBD][490139441] **Low** CVE-2026-5918: Inappropriate implementation in Navigation. *Reported by Google on 2026-03-05*
[TBD][483423893] **Low** CVE-2026-5919: Insufficient validation of untrusted input in WebSockets. *Reported by Richard Belisle on 2026-02-10*

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.

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

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 , Stable updates