

Chrome Releases

Release updates from the Chrome team

Stable Channel Update

Wednesday, July 20, 2016

The Chrome team is delighted to announce the promotion of Chrome 52 to the stable channel for Windows, Mac and Linux. Chrome 52.0.2743.82 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 52.

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 48 security fixes. Below, we highlight fixes that were contributed by external researchers. Please see the Chromium security page for more information.

[$15000][610600] **High** CVE-2016-1706: Sandbox escape in PPAPI. Credit to Pinkie Pie

[$3000][622183] **High** CVE-2016-1707: URL spoofing on iOS. Credit to xisigr of Tencent's Xuanwu Lab

[$500][613949] **High** CVE-2016-1708: Use-after-free in Extensions. Credit to Adam Varsan

[$500][614934] **High** CVE-2016-1709: Heap-buffer-overflow in sfntly. Credit to ChenQin of Topsec Security Team

[$8000][616907] **High** CVE-2016-1710: Same-origin bypass in Blink. Credit to Mariusz Mlynski

[$7500][617495] **High** CVE-2016-1711: Same-origin bypass in Blink. Credit to Mariusz Mlynski

[$3000][618237] **High** CVE-2016-5127: Use-after-free in Blink. Credit to cloudfuzzer

[$7500][619166] **High** CVE-2016-5128: Same-origin bypass in V8. Credit to Anonymous

[$5000][620553] **High** CVE-2016-5129: Memory corruption in V8. Credit to Jeonghoon Shin

[$2000][623319] **High** CVE-2016-5130: URL spoofing. Credit to Wadih Matar

[$3500][623378] **High** CVE-2016-5131: Use-after-free in libxml. Credit to Nick Wellnhofer

[$1000][607543] **Medium** CVE-2016-5132: Limited same-origin bypass in Service Workers. Credit to Ben Kelly

[$1000][613626] **Medium** CVE-2016-5133: Origin confusion in proxy authentication. Credit to Patch Eudor

[$500][593759] **Medium** CVE-2016-5134: URL leakage via PAC script. Credit to Alex Chapman and Paul Stone of Context Information Security

[$500][605451] **Medium** CVE-2016-5135: Content-Security-Policy bypass. Credit to ShenYeYinJiu of Tencent Security Response Center, TSRC

[$1000][625393] **Medium** CVE-2016-5136: Use after free in extensions. Credit to Rob Wu

[$1000][625945] **Medium** CVE-2016-5137: History sniffing with HSTS and CSP. Credit to Xiaoyin Liu

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.

As usual, our ongoing internal security work was responsible for a wide range of fixes:

[629852] CVE-2016-1705: Various fixes from internal audits, fuzzing and other initiatives.

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

Interested in switching release channels? Find out how. 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.

Krishna Govind
Google Chrome



Labels: Stable updates



Google

Google · Privacy · Terms