Chrome Releases

Release updates from the Chrome team

Stable Channel Update for Desktop

Tuesday, April 7, 2020

The Chrome team is delighted to announce the promotion of Chrome 81 to the stable channel for Windows, Mac and Linux. This will roll out over the coming days/weeks.

Chrome 81.0.4044.92 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 81.

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

[$7500][1019161] **High** CVE-2020-6454: Use after free in extensions. *Reported by Leecraso and Guang Gong of Alpha Lab, Qihoo 360 on 2019-10-29*
[$5000][1043446] **High** CVE-2020-6423: Use after free in audio. *Reported by Anonymous on 2020-01-18*
[$3000][1059669] **High** CVE-2020-6455: Out of bounds read in WebSQL. *Reported by Nan Wang(@eternalsakura13) and Guang Gong of Alpha Lab, Qihoo 360 on 2020-03-09*

[$2000][1040325] **High** CVE-2020-6419: Out of bounds read and write in V8. *Reported by David Manouchehri on 2020-01-09*
[$N/A] [1066893] **High** CVE-2020-6572: Use after free in media. *Reported by Anonymous on 2020-04-01*
[$2000][1031479] **Medium** CVE-2020-6430: Type Confusion in V8. *Reported by Avihay Cohen @ SeraphicAlgorithms on 2019-12-06*
[$2000][1040755] **Medium** CVE-2020-6456: Insufficient validation of untrusted input in clipboard. *Reported by Michał Bentkowski of Securitum on 2020-01-10*

[$1000][852645] **Medium** CVE-2020-6431: Insufficient policy enforcement in full screen. *Reported by Luan Herrera (@lbherrera_) on 2018-06-14*
[$1000][965611] **Medium** CVE-2020-6432: Insufficient policy enforcement in navigations. *Reported by David Erceg on 2019-05-21*
[$1000][1043965] **Medium** CVE-2020-6433: Insufficient policy enforcement in extensions. *Reported by David Erceg on 2020-01-21*
[$500][1048555] **Medium** CVE-2020-6434: Use after free in devtools. *Reported by HyungSeok Han (DaramG) of Theori on 2020-02-04*
[$N/A][1032158] **Medium** CVE-2020-6435: Insufficient policy enforcement in extensions. *Reported by Sergei Glazunov of Google Project Zero on 2019-12-09*
[$TBD][1034519] **Medium** CVE-2020-6436: Use after free in window management. *Reported by Igor Bukanov from Vivaldi on 2019-12-16*
[$500][639173] **Low** CVE-2020-6437: Inappropriate implementation in WebView. *Reported by Jann Horn on 2016-08-19*
[$500][714617] **Low** CVE-2020-6438: Insufficient policy enforcement in extensions. *Reported by Ng Yik Phang on 2017-04-24*
[$500][868145] **Low** CVE-2020-6439: Insufficient policy enforcement in navigations. *Reported by remkoboonstra on 2018-07-26*
[$500][894477] **Low** CVE-2020-6440: Inappropriate implementation in extensions. *Reported by David Erceg on 2018-10-11*
[$500][959571] **Low** CVE-2020-6441: Insufficient policy enforcement in omnibox. *Reported by David Erceg on 2019-05-04*
[$500][1013906] **Low** CVE-2020-6442: Inappropriate implementation in cache. *Reported by B@rMey on 2019-10-12*
[$500][1040080] **Low** CVE-2020-6443: Insufficient data validation in developer tools. *Reported by @lovasoa (Ophir LOJKINE) on 2020-01-08*
[$N/A][922882] **Low** CVE-2020-6444: Uninitialized Use in WebRTC. *Reported by mlfbrown on 2019-01-17*
[$N/A][933171] **Low** CVE-2020-6445: Insufficient policy enforcement in trusted types. *Reported by Jun Kokatsu, Microsoft Browser Vulnerability Research on 2019-02-18*
[$N/A][933172] **Low** CVE-2020-6446: Insufficient policy enforcement in trusted types. *Reported by Jun Kokatsu, Microsoft Browser Vulnerability Research on 2019-02-18*
[$N/A][991217] **Low** CVE-2020-6447: Inappropriate implementation in developer tools. *Reported by David Erceg on 2019-08-06*
[$N/A][1037872] **Low** CVE-2020-6448: Use after free in V8. *Reported by Guang Gong of Alpha Lab, Qihoo 360 on 2019-12-26*

Thanks also to Hosein Askari for identifying a vulnerability with the Chromium website.

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:

- [1067891] Various fixes from internal audits, fuzzing and other initiatives

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.

Thank you,
Prudhvikumar Bommana

Labels: Desktop Update , Stable updates