

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)
> Google (<https://www.bleepingcomputer.com/news/google/>)
> Google patches 10th Chrome zero-day exploited in the wild this year

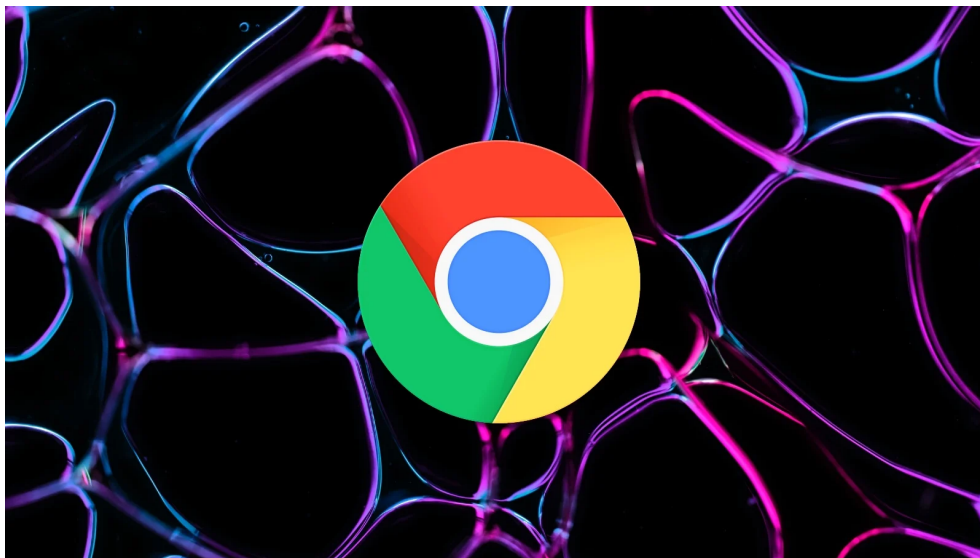
Google patches 10th Chrome zero-day exploited in the wild this year

By
Lawrence Abrams
(<https://www.bleepingcomputer.com/author/lawrence-abrams/>)

September 13, 2021

06:12 PM

1

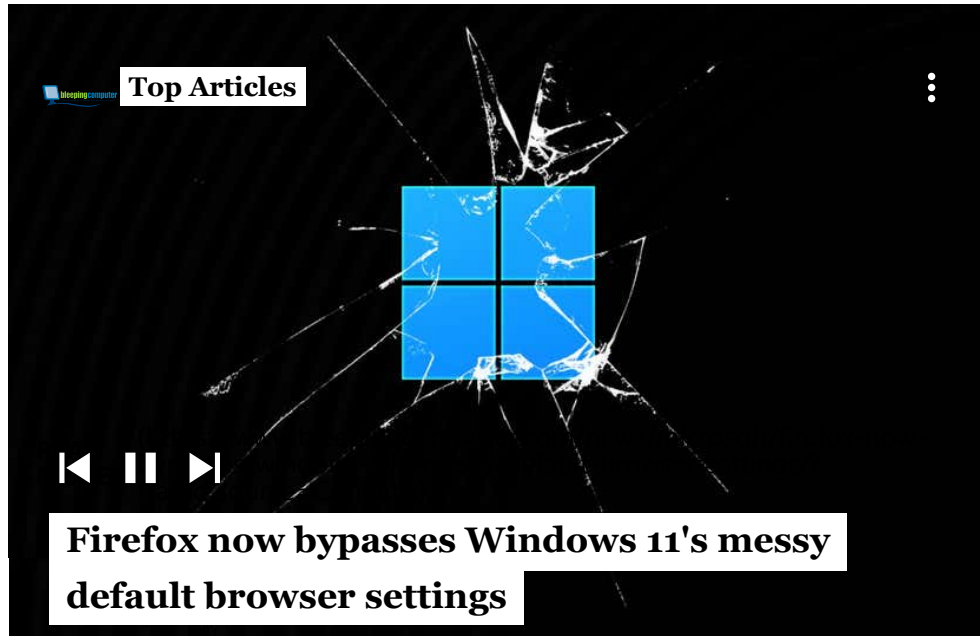


Google has released Chrome 93.0.4577.82 for Windows, Mac, and Linux to fix eleven security vulnerabilities, two of them being zero-days exploited in the wild.



"Google is aware that exploits for CVE-2021-30632 and CVE-2021-30633 exist in the wild," the company revealed in the release notes for the new Chrome version.

The update is currently rolling out worldwide in the Stable desktop channel, and Google states it will become available to everyone over the next few days.



The update was available immediately when BleepingComputer performed a manual check for new updates (**Chrome menu > Help > About Google Chrome**).

Google Chrome will also automatically check for new updates the next time you restart the browser.

Tenth zero-day fixed in 2021

The two zero-day vulnerabilities fixed today were disclosed to Google on September 8th, 2021, and are both memory bugs.

The CVE-2021-30632 is an out-of-bounds write in the V8 JavaScript engine, and the CVE-2021-30633 bug is a use-after-free bug in the Indexed DB API.

While these bugs often lead to browser crashes, threat actors can sometimes exploit them to perform remote code execution, sandbox escapes, and other malicious behavior.

While Google has disclosed that both bugs have been exploited in the wild, they have not shared further information regarding the attacks.

With these two vulnerabilities, Google has now patched a total of ten zero-day vulnerabilities in Chrome in 2021.

Other vulnerabilities fixed this year are:

- CVE-2021-21148
(<https://www.bleepingcomputer.com/news/security/google-fixes-chrome-zero-day-actively-exploited-in-the-wild/>) - February 4th, 2021
- CVE-2021-21166
(<https://www.bleepingcomputer.com/news/security/google-fixes-second-actively-exploited-chrome-zero-day-bug-this-year/>) - March 2nd, 2021
- CVE-2021-21193
(<https://www.bleepingcomputer.com/news/security/google-fixes-second-actively-exploited-chrome-zero-day-this-month/>) - March 12th, 2021
- CVE-2021-21220
(<https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop.html>) - April 13th, 2021
- CVE-2021-21224
(<https://www.bleepingcomputer.com/news/security/google-fixes-exploited-chrome-zero-day-dropped-on-twitter-last-week/>) - April 20th, 2021
- CVE-2021-30551
(<https://www.bleepingcomputer.com/news/security/google-fixes-sixth-chrome-zero-day-exploited-in-the-wild-this-year/>) - June 9th, 2021
- CVE-2021-30554
(<https://www.bleepingcomputer.com/news/security/google-fixes-seventh-chrome-zero-day-exploited-in-the-wild-this-year/>) - June 17th, 2021
- CVE-2021-30563
(<https://www.bleepingcomputer.com/news/security/google-patches-8th-chrome-zero-day-exploited-in-the-wild-this-year/>) - July 15th, 2021



As these vulnerabilities are known to have been exploited in the wild, it is strongly advised that all Google Chrome update to the latest version immediately.

