

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)
> Security (<https://www.bleepingcomputer.com/news/security/>)
> Emergency Google Chrome update fixes zero-day exploited in the wild

Emergency Google Chrome update fixes zero-day exploited in the wild

By **Sergiu Gatlan** (<https://www.bleepingcomputer.com/author/sergiu-gatlan/>)
September 24, 2021 01:33 PM 1



Google has released Chrome 94.0.4606.61 for Windows, Mac, and Linux, an emergency update addressing a high-severity zero-day vulnerability exploited in the wild.



"Google is aware that an exploit for CVE-2021-37973 exists in the wild," the browser vendor revealed in today's security advisory (https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_24.html).

This Chrome update has started rolling out worldwide to the Stable desktop channel and will be available to all users over the following days and weeks.



The update was available immediately when BleepingComputer manually checked for new updates from Chrome menu > Help > About Google Chrome.

The web browser will also check for new updates and automatically update itself after the next launch.

Details regarding ongoing attacks not disclosed

The zero-day security flaw fixed today was reported the day the first Google Chrome 94 stable release was published, on September 21, by Clément Lecigne from Google TAG, with assistance from Sergei Glazunov and Mark Brand from Google Project Zero.

The bug, tracked as CVE-2021-37973, is a use after free (<https://cwe.mitre.org/data/definitions/416.html>) weakness in Portals, Google's new web page navigation system for Chrome.

Successful exploitation of this vulnerability can let attackers execute arbitrary code on computers running unpatched Chrome versions.

Even though Google said it detected in the wild attacks abusing CVE-2021-37973, the company did not share additional info regarding these incidents.



"Access to bug details and links may be kept restricted until a majority of users are updated with a fix," Google said.

"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."



Chrome users should have enough time to install the security update to prevent exploitation attempts until more info is available.

Eleventh zero-day fixed this year

With this bug, Google has patched 11 zero-day vulnerabilities in the Chrome web browser since the start of 2021.

The other Chrome zero-day bugs Google 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
- CVE-2021-30632 and CVE-2021-30633
(<https://www.bleepingcomputer.com/news/google/google-patches-10th-chrome-zero-day-exploited-in-the-wild-this-year/>) - September 13th

Because these security bugs are all known to have been abused by threat actors in the wild, installing all Google Chrome updates is strongly recommended as soon as they are available.

Related Articles:

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

Cisco: Firewall manager RCE bug is a zero-day, patch incoming
(<https://www.bleepingcomputer.com/news/security/cisco-firewall-manager-rce-bug-is-a-zero-day-patch-incoming/>)

Researcher drops three iOS zero-days that Apple refused to fix
(<https://www.bleepingcomputer.com/news/security/researcher-drops-three-ios-zero-days-that-apple-refused-to-fix/>)

New macOS zero-day bug lets attackers run commands remotely
(<https://www.bleepingcomputer.com/news/apple/new-macos-zero-day-bug-lets-attackers-run-commands-remotely/>)

New Windows security updates break network printing
(<https://www.bleepingcomputer.com/news/security/new-windows-security-updates-break-network-printing/>)

