

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
 - [Cloud Security](#)
 - [Identity & Access](#)
 - [Data Protection](#)
 - [Network Security](#)
 - [Application Security](#)
- ▼ [Security Strategy](#)
 - [Risk Management](#)
 - [Security Architecture](#)
 - [Disaster Recovery](#)
 - [Training & Certification](#)
 - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Vulnerabilities](#)



Google Patches Serious Use-After-Free Vulnerabilities in Chrome

By [Ionut Arghire](#) on December 07, 2021

Share

Tweet

推荐 9



Google on Monday announced the rollout of a new security update for Chrome, to address 20 vulnerabilities in the browser, including 16 reported by external researchers.

Of these 16 security errors, 15 are rated *high severity*. Nearly half of them are use-after-free bugs affecting various components of the browser.

The most severe of these issues affects the web apps component. Tracked as CVE-2021-4052, it was reported by Wei Yuan of MoyunSec VLab, who received a \$15,000 bug bounty payout for the finding.

Next in line is CVE-2021-4053, a security hole in Chrome's UI component, which earned the reporting researcher \$10,000.

The [latest Chrome update](#) also addresses an incorrect security UI in autofill (CVE-2021-4054) and a heap buffer overflow in extensions (CVE-2021-4055), for which Google awarded the reporting researchers \$5,000 and \$1,000 bug bounty rewards, respectively.

The internet search company has yet to disclose the monetary rewards awarded for the remaining eleven high-severity issues that were addressed with this browser update and which were reported externally.

Of these, five were use-after-free vulnerabilities patched in components such as API, developer tools, screen capture, autofill, and window manager.

The remaining flaws include heap buffer overflows (in ANGLE and BFCache), type confusion (in loader and V8), insufficient data validation in loader, and integer underflow in ANGLE.

Google also addressed an issue described as “insufficient validation of untrusted input in new tab page.” Tracked as CVE-2021-4068 and considered *low severity*, the bug brought the reporting researcher a \$500 reward.

The latest Chrome release is now rolling out to Windows, Mac and Linux users as version 96.0.4664.93. Google also announced that the extended stable channel for Windows and Mac was updated to version 96.0.4664.93 as well.

Related: [Chrome 96 Plugs High-Risk Browser Flaws](#)

Related: [Chrome 95 Update Patches Exploited Zero-Days, Flaws Disclosed at Tianfu Cup](#)

Related: [Google Patches 19 Vulnerabilities in Chrome 95 Browser Refresh](#)

[Share](#)[Tweet](#)[推荐 9](#)[RSS](#)

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

[Android Security Updates Patch 46 Vulnerabilities](#)

[Grip Security Raises \\$25 Million to Secure SaaS Applications](#)

[Microsoft Seizes Domains Used by China-Linked APT 'Nickel'](#)

[Firefox 95 Rolls Out With New 'RLBox' Isolation Feature](#)

[Google Patches Serious Use-After-Free Vulnerabilities in Chrome](#)

[2021 ICS Cyber Security Conference | USA \[Hybrid: Oct. 25-28\]](#)

sponsored links

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

[2021 CISO Forum: September 21-22 - A Virtual Event](#)

[2021 Singapore/APAC ICS Cyber Security Conference \[Virtual: June 22-24\]](#)

Tags:

[NEWS & INDUSTRY](#) [Vulnerabilities](#)

Get the Daily Briefing

BRIEFING

