

- [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](#)



Chrome 97 Patches 37 Vulnerabilities

By [Ionut Arghire](#) on January 05, 2022

[Tweet](#)



Google this week announced the release of Chrome 97 in the stable channel with a total of 37 security fixes, including 24 for vulnerabilities reported by external researchers.

Of the 24 externally reported security flaws, one is rated critical severity, 10 high severity, 10 medium, and three low. The most common types of vulnerabilities are use-after-free (seven bugs), and improper implementation (eight issues).

The most severe is CVE-2022-0096, a use-after-free issue in Storage that could be exploited to execute code in the context of the browser.

Five of the 10 high-severity flaws addressed with this Chrome release are use-after-free errors affecting components such as screen capture, sign-in, SwiftShader, PDF, and Autofill.

The other five are an inappropriate implementation in DevTools, type confusion in V8, and heap buffer overflows in Bookmarks, V8, and ANGLE.

Half of the medium-severity issues are improper implementation bugs, affecting components such as navigation, Autofill, Blink, and compositing.

The remaining flaws include a use-after-free in File Manager API, incorrect security UI in Autofill and Browser UI, out-of-bounds memory access in Web Serial, and uninitialized-use in File API.

The low-severity errors fixed in this Chrome release include a policy bypass in Service Workers and inappropriate implementations in WebShare and passwords.

Google made no mention in its [advisory](#) of any of the addressed vulnerabilities being exploited in malicious attacks.

To date, the Internet search giant has paid a total of \$54,000 in bug bounty rewards to the reporting researchers. However, the company has yet to share details on over half of the bounty payouts.

The latest browser release is now rolling out to Windows, Mac, and Linux machines as Chrome 97.0.4692.71.

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

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

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

 view counter

[Tweet](#)



[RSS](#)



Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

[Zloader Banking Malware Exploits Microsoft Signature Verification](#)

[VMware Plugs Security Holes in Workstation, Fusion and ESXi](#)

[Chrome 97 Patches 37 Vulnerabilities](#)

[Google Patches 48 Vulnerabilities With First Set of 2022 Android Updates](#)

[Broward Health Data Breach Impacts 1.3 Million People](#)

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

sponsored links

 view counter

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

 view counter

[2022 Singapore/APAC ICS Cyber Security Conference\]](#)

 view counter

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

 view counter

 **Tags:**

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

Search

Get the Daily Briefing

BRIEFING

Business Email Address

Subscribe