

- [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 101 Update Patches High-Severity Vulnerabilities

By [Ionut Arghire](#) on May 11, 2022

Share

Tweet

推荐 0



Google this week announced the release of a Chrome browser update that resolves a total of 13 vulnerabilities, including nine that were reported by external researchers.

Of the externally reported security holes, seven are use-after-free bugs - these types of vulnerabilities could lead to arbitrary code execution.

Based on severity ratings and the currently listed bug bounties, the most important of these flaws is CVE-2022-1633, a high-severity use-after-free in Sharesheet that was reported by Khalil Zhani, who was awarded a \$5,000 reward for the find.

The same researcher reported CVE-2022-1634, a high-severity use-after-free in Browser UI, for which he was awarded \$3,000.

CVE-2022-1635, a high-severity use-after-free in Permission Prompts, which was reported by an anonymous researcher, also qualified for a \$3,000 bug bounty payout.

As per Google's policies, however, CVE-2022-1636, a high-severity use-after-free in Performance APIs, reported by Microsoft's Seth Brenith, is not eligible for a reward.

Google notes in its [advisory](#) that it has yet to determine the bug bounties to be handed out for four other high-severity vulnerabilities resolved with this Chrome update.

These include CVE-2022-1637 (inappropriate implementation in Web Contents), CVE-2022-1638 (Heap buffer overflow in V8 Internationalization), CVE-2022-1639 (use-after-free in ANGLE), and CVE-2022-1640 (use-after-free in Sharing).

The ninth vulnerability resolved with this browser update and the seventh use-after-free in the batch is rated “medium severity.” Tracked as CVE-2022-1641, the bug was awarded a \$5,000 bounty reward, Google says.

The latest Chrome iteration is now rolling out to Windows, Mac and Linux users as version 101.0.4951.64. Google made no mention of any of these vulnerabilities being exploited in attacks.

Related: [Chrome 101 Patches 30 Vulnerabilities](#)

Related: [Chrome 100 Update Patches High-Severity Vulnerabilities](#)

Related: [Chrome Browser Gets Major Security Update](#)

[Share](#)[Tweet](#)[推荐 0](#)

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

[Iran-Linked OilRig APT Caught Using New Backdoor](#)
[devOcean Emerges From Stealth With Cloud-Native Security Operations Platform](#)
['IceApple' Post-Exploitation Framework Created for Long-Running Operations](#)
[Ukrainian Sentenced to US Prison for Selling Hacked Credentials](#)
[Organizations in Europe Targeted With New 'Nerbian' RAT](#)

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

sponsored links

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

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

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

Tags:

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

Get the Daily Briefing

BRIEFING

