# Chrome 112 Patches 16 Security Flaws

**Google this week announced the release of Chrome 112 in the stable channel with patches for 16 vulnerabilities, including 14 reported by external researchers.**

Of the externally reported flaws, two are rated ‘high severity’, nine have a severity rating of ‘medium’, while the remaining three are low-severity issues.

The most severe of these is a heap buffer overflow bug in Visuals. Tracked as CVE-2023-1810, the vulnerability earned the reporting researcher a $5,000 bug bounty reward.

“CVE-2023-1810 can allow a compromised renderer to register multiple things with the same FrameSinkId, violating ownership assumptions,” Action1 VP Mike Walters said in an emailed comment.

Next in line is a use-after-free flaw in Frames, which is tracked as CVE-2023-1811, and for which Google awarded a $3,000 bug bounty. The issue, Walters says, could lead to a crash or malicious code execution.

Next in line is a use-after-free flaw in Frames, which is tracked as CVE-2023-1811, and for which Google awarded a $3,000 bug bounty.

The resolved medium-severity vulnerabilities include out-of-bounds memory access, inappropriate implementation, insufficient validation of untrusted input, use-after-free, incorrect security UI, insufficient policy enforcement, out-of-bounds read, and heap buffer overflow issues.

Impacted Chrome components include DOM Bindings, Extensions, Safe Browsing, Networking APIs, Picture In Picture, Intents, Vulkan, Accessibility, and Browser History.

The three low-severity flaws addressed with the Chrome 112 release impact the WebShare, Navigation, FedCM components.

Google says it has paid roughly $26,000 in bug bounty rewards for the reported vulnerabilities, but the final amount might be higher, as the internet giant has yet to determine the amount to be handed out for two of the bugs.

Per Google’s policies, no rewards will be issued for two other vulnerabilities, which were reported by Microsoft researchers.

Google makes no mention of any of these vulnerabilities being exploited in attacks.

The latest Chrome iteration is now rolling out as version 112.0.5615.49/50 for Windows and as version 112.0.5615.49 for Linux and macOS.

**Related:** Chrome 111 Update Patches High-Severity Vulnerabilities

**Related:**Google Discontinuing Chrome Tool for Removing Unwanted Software

**Related:** Chrome 111 Patches 40 Vulnerabilities

https://www.securityweek.com/chrome-112-patches-16-security-flaws/