

Forum: [Hack Forums](#)

Thread: [Critical Chrome Vulnerability Earns Researcher \\$43,000](#)

MadScientist - September 14, 2025, 8:34 am

Google this week rolled out a Chrome update that fixes two security defects reported by external researchers, including a critical-severity bug in the browser's Serviceworker component, for which a \$43,000 bug bounty reward was paid.

Tracked as CVE-2025-10200 and reported by Looben Yang, the critical flaw is described as a use-after-free issue. These types of memory corruption vulnerabilities appear when the program attempts to access memory that has been freed.

By timing memory operations, attackers can exploit use-after-free bugs to place malicious code in the freed memory, potentially achieving arbitrary code execution and complete system compromise.

The latest Chrome update also resolves CVE-2025-10201, a high-severity inappropriate implementation in Mojo, for which Google handed out a \$30,000 reward. This flaw was reported to Google by Sahan Fernando and an anonymous researcher.

While these may seem like significant rewards, Google recently paid out a \$250,000 bug bounty for a Chrome vulnerability that can be exploited to escape the web browser's sandbox.

Google makes no mention of either of the newly patched vulnerabilities being exploited in the wild, but users are advised to update their browsers as soon as possible.

The Chrome update is rolling out as versions 140.0.7339.127/.128 for Windows, versions 140.0.7339.132/.133 for macOS, and 140.0.7339.127 for Linux.

Source - <https://www.securityweek.com/critical-chrome-vulnerability-earns-researcher-43000/>