Google Patches Second Chrome Zero-Day Vulnerability of 2023

Google on Tuesday announced patches for another zero-day vulnerability found in the Chrome browser.

Tracked as CVE-2023-2136, the security defect is described as a high-severity integer overflow issue in Skia. The bug was reported by Google Threat Analysis Group researcher Clement Lecigne and, per Google's policy, no monetary reward was issued for it.

"Google is aware that an exploit for CVE-2023-2136 exists in the wild," the internet giant notes in its advisory.

CVE-2023-2136 is the second zero-day vulnerability resolved in Chrome this year, after CVE-2023-2033, a type confusion issue in the V8 JavaScript engine, was addressed with an emergency patch last week.

The latest Chrome 112 update includes eight security fixes, five of which address vulnerabilities reported by external researchers, including four bugs rated 'high' severity.

Google says it handed out $20,000 in bug bounty rewards to the reporting researchers.

Based on the paid reward, the most severe of the externally reported security defects are CVE-2023-2133 and CVE-2023-2134, two out-of-bounds memory access issues in the Service Worker API.

Out-of-bounds access bugs occur when the area outside of array

bounds is accessed, which could lead to unexpected behavior, such as crashes and data leaks.

Both vulnerabilities were reported by Rong Jian, who received a total of $16,000 for the findings.

The third externally reported high-severity issue addressed with this Chrome update is CVE-2023-2135, a use-after-free bug in DevTools. Security researcher Cassidy Kim received a $3,000 bug bounty reward for finding this flaw.

Google handed out a $1,000 reward for CVE-2023-2137, a medium-severity heap-buffer overflow in SQLite, which was reported by 360 Vulnerability Research Institute's Nan Wang and Guang Gong.

The new Chrome iteration is rolling out as version 112.0.5615.137 for Mac and as versions 112.0.5615.137/138 for Windows. A new Chrome for Linux release will arrive soon.

Related: CISA Adds Chrome, macOS Bugs to Known Exploited Vulnerabilities Catalog

Related: Chrome 112 Patches 16 Security Flaws

Related: Chrome 111 Update Patches High-Severity Vulnerabilities

Google Patches Second Chrome Zero-Day Vulnerability of 2023