Google fixes one more Chrome zero-day exploited at Pwn2Own

Date: 04th April 2024 | Severity: High

Summary

Google has fixed another zero-day vulnerability in the Chrome browser, which was exploited by security researchers during the Pwn2Own hacking contest last month. Tracked as CVE-2024-3159, this high-severity security flaw is caused by an out-of-bounds read weakness in the Chrome V8 JavaScript engine.

Attack Vectors

Remote attackers can exploit the vulnerability usingcrafted HTML pages to gain access to data beyond the memory buffer via heap corruption, which can provide them with sensitive information or trigger a crash. Palo Alto Networks security researchers Edouard Bochin and Tao Yan demoed the zero-day on the second day of Pwn2Own Vancouver 2024 to defeat V8 hardening. Their double-tap exploit allowed them to execute arbitrary code on Google Chrome and Microsoft Edge, earning them a $42,500 award.

One week ago, Google fixed two more Chrome zero-days exploited at Pwn2Own Vancouver 2024. The first, a high- severity type confusion weakness (CVE-2024-2887) in the WebAssembly (Wasm) open standard, was targeted by Manfred Paul's double-tap RCE exploit that targeted both Chrome and Edge. The second, a use-after-free (UAF) weakness in the WebCodecs API (CVE-2024-2886), was also exploited by KAIST Hacking Lab's Seunghyun Lee to gain remote code execution on both Chromium web browsers.

Indicator of Compromise

Not Applicable

Recommendation

Google has now fixed the zero-day in the Google Chrome stable channel version 123.0.6312.105/.106/.107 (Windows and Mac) and 123.0.6312.105 (Linux), which will roll out worldwide over the coming days.

We strongly recommended to update Google Chrome to latest version.

Reference Links

https://securityaffairs.com/161445/hacking/google-chrome-zero-day-pwn2own.html

https://www.bleepingcomputer.com/news/security/google-fixes-one-more-chrome-zero-day-exploited-at-pwn2own/