KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New Google Chrome zero-day CVE-2022-2856 weaponized

Tracker ID: TN0827 **Date:** 22/Aug/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Google published Chrome desktop browser upgrades to address a high-severity zero-day vulnerability which is being actively exploited in the wild. CVE-2022-2856 has been identified as an instance of inadequate validation of untrusted input in “Intents”. It has yet to be assigned a vulnerability score.

Chrome processes user input using "intents"; if the browser does not correctly validate this input, an attacker can submit a customized input (for example, a post in a website's comments section) that the application did not intend. The intent feature enables the deployment of web services and apps directly from websites. Poor input validation can allow for the circumvention of security measures or the augmentation of intended functionality, potentially allowing for buffer overflow, directory traversal, SQL injection, cross-site scripting, null byte injection, and other privacy violations.

The latest patch also addresses ten more security flaws, the most of which are use-after-free vulnerabilities in various components such as FedCM, SwiftShader, ANGLE, and Blink. A heap buffer overflow vulnerability in downloads was also fixed. Automatic upgrades for Windows, Mac, and Linux are now being delivered in stages, but everyone may update manually.

This is the fifth zero-day vulnerability in Chrome that Google has fixed since the beginning of the year. CVE-2022-0609: Use-after-free in Animation, CVE-2022-1096: Type misunderstanding in V8, CVE-2022-1364: Type confusion in V8, and CVE-2022-2294: Heap buffer overflow in WebRTC.

Affected Products and Versions

- Google Chrome browser versions prior to 104.0.5112.102 Mac and Linux.
- Google Chrome browser versions prior to 104.0.5112.102/101 for Windows.

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-2856	High	NA

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New Google Chrome zero-day CVE-2022-2856 weaponized

Tracker ID: TN0827 **Date:** 22/Aug/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Recommendations

- Update Chrome to its latest version, 104.0.5112.101 for Mac and Linux and 104.0.5112.102/101 for Windows, to be rolled out over the coming days.Immediately identify the vulnerable instances and apply the vendor-provided fixes as soon as possible.

References

- Stable Channel Update for Desktop, Google, 16th August 2022, External Link (chromereleases.googleblog.com)
- Ravie Lakshmanan, New Google Chrome Zero-Day Vulnerability Being Exploited in the Wild, Hacker News, 17th August 2022, External Link (thehackernews.com)
- Dark Reading Staff, Google Chrome Zero-Day Found Exploited in the Wild, Dark Reading, 18th August 2022, External Link (darkreading.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia