Mphasis
The Next Applied

Zero-day Vulnerability in Chrome

Severity: High | Date: 5th Jul 2022

Description

Google has released Chrome 103.0.5060.114 for Windows users to address a high-severity zero-day vulnerability exploited by attackers in the wild, the fourth Chrome zero-day patched in 2022.

The 103.0.5060.114 version is rolling out worldwide in the Stable Desktop channel, with Google saying that it is a matter of days or weeks until it reaches the entire userbase.

This update was available immediately by checking for new updates by going into Chrome menu > Help > About Google Chrome.

Impact

The zero-day bug fixed (tracked as CVE-2022-2294) is a high severity heap-based buffer overflow weakness in the WebRTC (Web Real-Time Communications) component.

The impact of successful heap overflow exploitation can range from program crashes and arbitrary code execution to bypassing security solutions if code execution is achieved during the attack.

Although Google says this zero-day vulnerability was exploited in the wild, the company is yet to share technical details or an any info regarding these incidents.

“Access to bug details and links may be kept restricted until a majority of users are updated with a fix,” Google said.

Fix

Strongly recommended to update Google Chrome to latest version as soon as update available.

Reference Links

https://www.bleepingcomputer.com/news/security/google-patches-new-chrome-zero-day-flaw-exploited-in-attacks