Mphasis
The Next Applied

Zero-day Vulnerability in Chrome

Severity: High

Date: 17th Aug 2022

Description

Google has released a security update for the Chrome browser that addresses close to a dozen vulnerabilities, including a zero-day flaw that is being exploited in the wild.

The security update is currently rolling out for Windows, Mac, and Linux. Users who have automatic updates turned on should receive it in the coming days/weeks.

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-2022-2856) is described as a high-severity security issue due to “insufficient validation of untrusted input in Intents,” a feature that enables launching applications and web services directly from a web page.

Bad input validation in software can serve as a pathway to overriding protections or exceeding the scope of the intended functionality, potentially leading to buffer overflow, directory traversal, SQL injection, cross-site scripting, null byte injection, and more.

Fifth zero-day patched in 2022

The current Chrome update addresses the fifth zero-day vulnerability in Google Chrome this year that is actively exploited by threat actors:

The previous four were:

- CVE-2022-2294 – July 4
- CVE-2022-1364 – April 14
- CVE-2022-1096 – March 25
- CVE-2022-0609 – February 14 (exploited by North Korean hackers in phishing campaigns)

Fix

Strongly recommended to update Google Chrome to latest version.

Reference Links

- https://www.bleepingcomputer.com/news/security/google-fixes-fifth-chrome-zero-day-bug-exploited-this-year/
- https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html