MENLO SECURITY

1 650.614.1705 ☎
support@menlosecurity.com ✉
www.menlosecurity.com 🌐

Menlo labs.

Menlo Labs Threat Bulletin

Bulletin: 2022—014

Date: 07/09/2022

Name: Chrome 0 Days

Classification: Browser Zero Day - CVE-2022-3075

Summary

Google recently issued a patch for a high severity browser vulnerability - CVE-2022-3075, which is confirmed to be exploited in the wild. The Stable channel 105.0.5195.102 for Windows, Mac and Linux addresses this vulnerability.

This high severity vulnerability is caused by insufficient data validation in Mojo, a collection of runtime libraries used for inter-process communication.

Google has not yet published additional details or IOCs for the in the wild exploitation or disclosed details around attacks leveraging the vulnerability. Google also has currently restricted access to bug details of this vulnerability.

Infection Vector

The browser zero day is primarily affecting Chrome browsers. However, since Microsoft Edge is also now based on Chrome, Edge users are also vulnerable to these same flaws.

The table below lists details of the HIGH severity vulnerability and associated CVE patched by Google.

CVE	Severity	Description	In the wild exploitation
CVE-2022-3075	High	Insufficient data validation in Mojo.	Yes. Confirmed by Google Threat Analysis Group.

Menlo Recommendations

Menlo recommends all Chrome / Edge browser users upgrade to the latest version of the stable channel update.

Menlo Protection

Customers using the Menlo Cloud Security Platform are protected against such vulnerabilities by design! With Menlo, when a user visits a website via the isolation platform, all active content is fetched and executed in the Menlo cloud-based isolation platform - Not on the users device. Menlo protects all devices—including mobile.

Based on the information available, the Menlo isolation platform would likely disrupt the exploit chain needed to take advantage of it.

Menlo labs is actively monitoring for any associated IOCs and will send updates, once additional details about the exploit is identified.