1 650.614.1705
support@menlosecurity.com
www.menlosecurity.com

Menlo labs.

Menlo Labs Threat Bulletin

Bulletin: 2022—016

Date: 04/11/2022

Name: Chrome 0 Days

Classification: Browser Zero Day - CVE-2022-3723

Summary

Google recently issued a patch for a high severity browser vulnerability - CVE-2022-3723, which is confirmed to be exploited in the wild. The Stable channel 107.0.5304.87 for Mac and Linux, and 107.0.5304.87/.88 for Windows, addresses this vulnerability.

This high severity vulnerability is caused by a type confusion vulnerability in the Chromium V8 JavaScript engine.

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-2022-3723	High	Type Confusion in V8	Yes. Confirmed by Google.

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 disrupt the exploit chain needed to take advantage of it.