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

Menlo Labs Threat Bulletin

Bulletin: 2022—012

Date: 24/08/2022

Name: Chrome 0 Days

Classification: Browser Zero Day - CVE-2022-2856

Summary

Google recently issued a patch for a high severity browser vulnerability - CVE-2022-2856, which is confirmed to be exploited in the wild. The Stable channel 104.0.5112.101 for Mac and Linux and 104.0.5112.102/101 for Windows addresses this vulnerability.

Google has not yet published additional details or IOCs for the in the wild exploitation or disclosed details around attacks leveraging the 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-2022-2856	High	Insufficient validation of untrusted input in Intents	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.

For this specific browser 0 day, Menlo labs has confirmed that the issue is prevented as long as customers did not add "intent://" to the list of 'External Application Links". Intent is a linking replacement feature for URI schemes to start an activity in another app.

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