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

Menlo Labs Threat Bulletin

Bulletin: 2023—02

Date: 27/04/2023

Name: Chrome 0 Days

Classification: Browser Zero Days

Summary

Google recently issued two stable channel updates addressing 10 security fixes of which two CVE's - CVE-2023-2033 and CVE-2023-2136, are confirmed to be exploited in the wild. The Stable channel 112.0.5615.137/138 for Windows, 112.0.5615.137 for Mac and 112.0.5615.165 for Linux addresses this vulnerability.

The details of the vulnerabilities are as follows

- CVE-2023-2033 - Type confusion in V8 in Google Chrome prior to 112.0.5615.121 that allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
- CVE-2023-2136 - Integer overflow in Skia (2D graphics library) in Google Chrome prior to 112.0.5615.137 that allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

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-2023-2033	High	Type Confusion in V8	Yes. Confirmed by Google Threat Analysis Group.
CVE-2023-2136	High	Integer overflow in Skia	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 usually protected against such vulnerabilities by design! With Menlo, when a user visits a website via the isolation platform (including IOS and Android mobile devices), all active content is executed in the Menlo cloud-based isolation platform - Not on the user's 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. Menlo labs is actively monitoring for any further intel and will send updates, once additional details are identified.