Menlo Labs Threat Bulletin

Bulletin: 2023—019

Date: 09/13/2023

Name: CVE-2023-4863

Classification: Browser 0 day

Summary

Google fixed a critical Heap Buffer Overflow vulnerability in Chrome. This vulnerability is tracked as CVE-2023-4863

Infection Vector

The vulnerability is in a component known as WebP. WebP is a modern image format that provides superior lossless and lossy compression for images on the web. With WebP, web developers are able to create richer and smaller images without compromising on the performance of the website.

This component is natively supported by Google Chrome, Safari, Firefox, Edge and the Opera browser. This browser zero day potentially affects all browsers. It is critical for admins to expedite the patching of this vulnerability.

There is speculation that this vulnerability is connected to the recent BLASTPASS exploit chain, reported by Citizen Lab. The report by Citizen Lab notes that the BLASTPASS exploit drops the sophisticated Pegasus malware and attributes it to the NSO group. The Pegasus malware and the NSO group have been linked to attacks conducted by various countries to spy on journalists and other persons of interest.

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.