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

Menlo Labs Threat Bulletin

Bulletin: 2022-011

Date: 07/06/2022

Name: Chrome 0 Days

Classification: Browser Zero Day - CVE-2022-2294

Summary

Google issued patches for 2 high severity browser vulnerabilities, out of which one is confirmed to be exploited in the wild. The 103.0.5060.114 version addresses these vulnerabilities. On 6th July 2022, Microsoft released a Security Update Guide addressing the same vulnerabilities as Microsoft Edge ingests chromium.

Google has not yet published additional details or IOCs for the in the wild exploitation and attacks leveraging the vulnerabilities disclosed.

Technical Details

Infection Vector

The browser zero days are primarily affecting Chrome browsers. Below is a table, listing all the HIGH severity vulnerabilities, with associated CVEs patched by Google.

CVE	Severity	Description	In the wild exploitation

CVE-2022-2294	High	Heap overflow in WebRTC	Yes. Confirmed by Google Threat Analysis Group.
CVE-2022-2295	High	Type confusion in V8	TBD

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 executed in the Menlo Isolation Cloud, which means that any malicious JavaScript executes in an isolated browser, running in Menlo's cloud-based isolation platform - Not on the users device. Menlo protects all devices—including mobile.

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