650-614-1705
www.menlosecurity.com
support@menlosecurity.com

Menlo Labs Threat Bulletin

Bulletin: 2022-05

Date: 03/28/2022

CVE: CVE-2022-1096

Classification: Browser Zero Day Exploits

Summary

- Google issued an emergency patch CVE-2022-1096, for a browser 0 day
- The vulnerability is reported to be used by attackers in the wild for active exploitation
- Websites isolated by the Menlo Platform are completely protected from this threat

Technical Details

Google issued an emergency patch on March 26th for a high severity vulnerability. According to various open source threat intelligence sources, the vulnerability is actively being used in attacks.

The vulnerability is a type confusion in the Chrome V8 JavaScript engine. Type confusion vulnerabilities are caused when sufficient validation or verification on the type of object, passed to a piece of code is not done. According to CWE, when the program accesses the resource using an incompatible type, this could trigger logical errors because the resource does not have expected properties. In languages without memory safety, such as C and C++, type confusion can lead to out-of-bounds memory access.

Menlo Protection

Customers using the Menlo Cloud Security Platform are protected against browser zero day 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

650-614-1705
www.menlosecurity.com
support@menlosecurity.com

Menlo Labs Threat Bulletin

any malicious JavaScript executes in an isolated browser, running in Menlo's cloud-based isolation platform - not on the user's device. Menlo can protect all devices—including mobile.

Menlo labs will continue to research this vulnerability and will provide an update if we find additional intelligence.