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

Menlo Labs Threat Bulletin

Bulletin: 2022-02

Date: 02/15/2022

Name: Apple Webkit & Google Chrome Zero Day Exploits

Classification: Browser Zero Day Exploits

Summary

Apple (WebKit):

- Apple has issued a security advisory for a critical WebKit vulnerability that affects Safari Browsers across all platforms. This vulnerability is actively being exploited in the wild.
- The CISA has also added this Zero Day vulnerability to its known vulnerability catalog.

Google (Chromium):

- Google has issued security patches for 11 Chrome related vulnerabilities, out of which one of them is actively being exploited in the wild.
- The above Chrome vulnerability also affects other Chromium based browsers like Microsoft Edge & Brave.
- Microsoft has acknowledged the vulnerability and is currently working on a Security Patch for the Edge browser.
- The CISA has also issued an awareness report regarding this vulnerability.

Technical Details

Apple WebKit vulnerability:

- As of now, there is no specific detail about how this vulnerability is being exploited. Apple's security advisory states: "Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited."

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

Menlo Labs Threat Bulletin

CVE	Severity	Description	Exploited in the Wild
CVE-2022-22620	HIGH	Use after free bug in WebKit	YES, Confirmed by Apple, CISA.gov

Google Chrome Vulnerabilities:

- For the Google Chrome vulnerability that is actively being exploited, at this time the exact infection mechanism has not been disclosed by Google. Below is a table, listing all the HIGH severity vulnerabilities, with associated CVEs patched by Google.

CVE	Severity	Description	Exploited in the Wild
CVE-2022-0603	HIGH	Use after free in File Manager	TBD
CVE-2022-0604	HIGH	Heap buffer overflow in Tab Groups	TBD
CVE-2022-0605	HIGH	Use after free in Webstore API	TBD
CVE-2022-0606	HIGH	Use after free in ANGLE	TBD
CVE-2022-0607	HIGH	Use after free in GPU	TBD
CVE-2022-0608	HIGH	Integer overflow in Mojo	TBD
CVE-2022-0609	HIGH	Use after free in Animation	YES, Confirmed by Google

- Going by the bug description for CVE-2022-0609, the vulnerability could be exploited upon visiting a malicious page that uses Javascript to trigger the vulnerability.

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

Menlo Labs Threat Bulletin

Menlo Protection

Customers using the Menlo Cloud Security Platform are protected against browser zero day vulnerabilities (Like the WebKit/Chrome vulnerability mentioned above) 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 user's device. Menlo can protect all devices—including mobile.