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

Menlo Labs Threat Bulletin

Bulletin: 2021-003

Date: 04/21/2021

Name: Zero day protection

Classification: Browser Zero Day

Summary

It's been a busy April for both Google and Microsoft. Google issued a patch for 7 browser vulnerabilities, out of which one is confirmed to be exploited in the wild. Google has not yet published additional details or IOCs in this specific attack.

Microsoft on the other hand issued a total of 109 patches. In addition to fixes for Exchange server vulnerabilities, exploited by the HAFNIUM group, Microsoft fixed one critical Escalation of Privilege vulnerability that is being exploited in the wild.

Technical Details

CHROME

The browser zero days are primarily affecting Chrome browsers, however, since Microsoft Edge is also now based on Chrome, Edge users are vulnerable to these flaws. Below is a table, listing all the HIGH severity vulnerabilities with associated CVEs patched by Google

CVE	Severity	Description	In the wild exploitation
CVE-2021-21222	High	Heap buffer overflow in V8	TBD
CVE-2021-21223	High	Integer overflow in Mojo	TBD
CVE-2021-21224	High	Type Confusion in V8	Yes. Confirmed by Google
CVE-2021-21225	High	Out of bounds memory access in V8	TBD
CVE-2021-21226	High	Use after free in navigation	TBD

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

Menlo Labs Threat Bulletin

BITTER APT GROUP

Kaspersky's research team has attributed the Windows EOP vulnerability (***CVE-2021-28310***) as being used by the Bitter APT group, in targeted attacks. Their research indicates that this vulnerability is used in conjunction with browser 0 days to compromise endpoints.

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 update the platform once additional details about the threat are available.