Menlo Security

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

Menlo Labs Threat Bulletin

Bulletin: 2021-004

Date: 05/11/2021

Name: Microsoft Patch Tuesday

Classification: Browser Zero Day

Summary

Microsoft issued fixes for a total of 56 vulnerabilities in May's patch Tuesday release.

- 6 out of the 56 vulnerabilities patched, have been given a rating of "Exploitation More Likely" by Microsoft. This rating is given to vulnerabilities that Microsoft thinks will be exploited by bad actors
- 3 out of the 6 vulnerabilities deemed as "Exploitation more likely", have been given a severity rating of ***Critical,*** Microsoft's most severe rating.

Technical Details

Menlo protects customers against the vulnerabilities in the table below. Of utmost importance is CVE-2021-26419. Customers using IE11 are affected by this vulnerability. This is a flaw in the JScript engine, that allows for unsafe command execution. A user's endpoint can get exploited by visiting a malicious web page.

*A quick note about CVE-2021-31170 and CVE-2021-31188. Elevation of privilege vulnerabilities are usually chained with browser exploits to compromise endpoints. Past elevation of privilege exploits like CVE-2021-28310, which was patched in April by Microsoft, was chained with a Chrome browser 0-day exploit, by the BITTER APT group to compromise endpoints. Menlo labs predicts that these two vulnerabilities might also be used in the same fashion.

Menlo Labs Threat Bulletin

CVE	Severity	Impact	Description	In the wild exploitation
CVE-2021-26419	Critical	Remote Code Execution	Scripting Engine Memory Corruption Vulnerability	Exploitation more likely
*CVE-2021-31170	Important	Elevation of Privilege	Windows Graphics Component Elevation of Privilege Vulnerability	Exploitation More Likely
*CVE-2021-31188	Important	Elevation of Privilege	Windows Graphics Component Elevation of Privilege Vulnerability	Exploitation More Likely

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 executes 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 protects all devices—including mobile.

Menlo Labs is actively monitoring for any IOCs and will update the platform, once additional details about the threats are available.