MENLO SECURITY

☎ 650-614-1705
🌐 www.menlosecurity.com
✉ support@menlosecurity.com

Menlo Labs Threat Bulletin

Bulletin: 2021-007

Date: 09/14/2021

Name: Apple iOS & Google Chrome Zero Day Exploits

Classification: Zero Day Exploits

Summary

- Apple has issued a critical security update to two specific vulnerabilities that affects Apple's iPhone, iPad & Mac operating systems. These vulnerabilities are also being actively exploited in the wild.
- Google has also issued a patch for 11 Chrome related vulnerabilities, out of which two of them are confirmed to be exploited in the wild.

Technical Details

Apple Vulnerabilities:

- From the Apple security bulletin, it was found that the one zero day exploit was triggered due to a bug in the Core Graphics system component, which can be triggered within the context of applications like iMessage or maliciously crafted PDF documents.
- Another zero day vulnerability exists in the WebKit engine which is also actively being exploited in the wild. This vulnerability is due to a memory management bug that could lead to arbitrary code execution. Webkit is the engine for the default Safari Browser on all Apple operating systems.

CVE	Severity	Description	Exploited in the Wild
CVE-2021-30860	HIGH	Integer Overflow bug in CoreGraphics	YES, Confirmed by Apple
CVE-2021-30858	HIGH	Use after free bug in WebKit	YES, Confirmed by Apple

Menlo Labs Threat Bulletin

- From a research article published by Citizen Lab, it is learnt that the Core Graphics exploit is being distributed via iMessages, but the Apple security bulletin states that this specific vulnerability can be exploited via maliciously crafted PDF files.
- As of now, additional details are being gathered for these two exploits, and an additional advisory will be issued as needed.

Google Chrome Vulnerabilities:

- For the Google Chrome vulnerabilities, 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-2021-30625	HIGH	Use after free in Selection API	TBD
CVE-2021-30626	HIGH	Out of bounds memory access in ANGLE	TBD
CVE-2021-30627	HIGH	Type Confusion in Blink layout	TBD
CVE-2021-30628	HIGH	Stack buffer overflow in ANGLE	TBD
CVE-2021-30629	HIGH	Use after free in Permissions	TBD
CVE-2021-30630	HIGH	Inappropriate implementation in Blink	TBD
CVE-2021-30631	HIGH	Type Confusion in Blink layout	TBD
CVE-2021-30632	HIGH	Out of bounds write in V8	YES, Confirmed by Google
CVE-2021-30633	HIGH	Use after free in Indexed DB API	YES, Confirmed by Google

Menlo Labs Threat Bulletin

Menlo Protection

Customers using the Menlo Cloud Security Platform are protected against browser zero day vulnerabilities (Like the WebKit 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 users device. Menlo protects all devices—including mobile.

For the iOS zero day vulnerability in the CoreGraphics component that lets attackers craft malicious PDF documents, the Document Isolation solution can help protect against such document borne zero day exploits.