Security Advisory 2021-049

Multiple Zero-Day Vulnerabilities in Apple Products

September 14, 2021 — v1.0

TLP:WHITE

History:

- *14/09/2021 — v1.0 – Initial publication*

Summary

On September 13, Apple has released multiple security updates to address two zero-day vulnerabilities tracked as CVE-2021-30858 and CVE-2021-30860 in multiple products [1]. An attacker could exploit these vulnerabilities to take control of an affected device [2]. One vulnerability is known to be used to install the Pegasus spyware on iPhones [3] and Apple is aware of a report that this issue may have been actively exploited [1].

Technical Details

Both vulnerabilities allow maliciously crafted documents to execute commands when opened on vulnerable devices.

CVE-2021-30860 - CoreGraphics

The CVE-2021-30860 CoreGraphics vulnerability is an integer overflow bug discovered by Citizen Lab that allows threat actors to create malicious PDF documents that execute commands when opened in iOS and macOS [3]. The exploit, which called `FORCEDENTRY`, targets Apple's image rendering library, and was effective against Apple iOS, MacOS and WatchOS devices [4].

CVE-2021-30858 - WebKit

The CVE-2021-30858 is a WebKit use after free vulnerability allowing hackers to create maliciously crafted web page that execute commands when visiting them on iPhones and macOS. Apple states that this vulnerability was disclosed anonymously [3].

Products Affected

The vulnerabilities affect:

- iPhones with iOS versions prior to 14.8;
- Mac computers with operating system versions prior to OSX Big Sur 11.6 and Catalina Security Update 2021-005;
- Apple Watches prior to watchOS 7.6.2;
- Safari with versions prior to 14.1.2.

Recommendations

Apple has released software updates addressing the vulnerabilities [1].

CERT-EU recommends updating vulnerable software as soon as possible.

References

[1] https://support.apple.com/en-us/HT201222

[2] https://us-cert.cisa.gov/ncas/current-activity/2021/09/13/apple-releases-security-updates-address-cve-2021-30858-and-cve

[3] https://www.bleepingcomputer.com/news/apple/apple-fixes-ios-zero-day-used-to-deploy-nso-iphone-spyware/

[4] https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/