Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert

August 18, 2022 TLP: White Report: 202208181500

Apple Fixes Two Zero Day Exploits

Executive Summary

Apple has released a security update fixing two zero-day common vulnerability and exposures (CVE) that they state are being actively exploited. It is unknown as to how these bugs were discovered outside of the reports from an anonymous researcher. The exploits can grant an attacker remote code execution (RCE) and kernel level privileges on a device. A device compromised from these exploits could be subjected to data access to an unauthorized user, location retrieval, internet tracking, and much more. With the increasing use of iOS devices in the healthcare sector, it is strongly encouraged to update your devices immediately. Over the course of this year, Apple has released updates to fix seven total zero-day exploits.

Report

Apple has released two emergency security updates to fix zero-day vulnerabilities that hackers have been able to exploit on iPhones, iPads, and Macs. Currently the devices that are affected by both vulnerabilities are iPhone 6s and later, Macs that run macOS Monterey, all iPad Pro models, iPad Air 2 and later, iPad 5th generation and on, iPad mini 4 and later, and the 7th generation of iPod touch.

Apple and Healthcare

iOS devices have gained popularity recently within the healthcare sector due to their ability to be utilized as multipurpose platform. The iOS devices can be used by care teams to provide secure internal communication, medication administration, ultrasound imaging, mobile documentation of sensitive patient information, and multiple other tasks. Cyberthreat actors can leverage the zero-day exploitations to compromise these iOS devices in the healthcare sector.

The Exploits

CVE-2022-32893: This exploit is in WebKit, which is a part of Apple's browser engine and primarily resides in Safari. This vulnerability can lead to the execution of arbitrary code. According to Apple this could be exploited by remotely visiting a malicious website.

CVE-2022-32894: This vulnerability is in the operating system's Kernel that could be abused to execute arbitrary code with the highest privileges. A malware on the kernel would be able to essentially give an attacker full control of the device.

How to Update

Apple has already published advisories for the vulnerabilities on their webpage. To update your device:

On iPhone or iPad: Settings > General > Software Update

On Mac: Apple menu > About this Mac > Software Update

References

Abrams, Lawrence. "Apple security update fix 2 zero-days used to hack iphones, macs" bleepingcomputer. August 17, 2022. Apple security updates fix 2 zero-days used to hack iPhones, Macs (bleepingcomputer.com)

Lakshmanan, Ravie. “Apple Releases Security Updates to Patch Two New Zero-Day Vulnerabilities” thehackernews. August 17, 2022. https://thehackernews.com/2022/08/apple-releases-security-updates-to.html

Ducklin, Paul. “Apple patches double zero-day in browser and kernel – update now!” nakedsecurity. August 18, 2022. https://nakedsecurity.sophos.com/2022/08/18/apple-patches-double-zero-day-in-browser-and-kernel-update-now/

Apple. “The future of healthcare is in your hands”. https://www.apple.com/healthcare/

Apple. “Deploying iPhone for Clinical Communication and Nursing Care”. Deploying iPhone for Clinical Communication and Nursing Care April 2022 (apple.com)

Gupata, Dileep. “iOS App development for Healthcare – Advanced Features & Cost”. Appinventiv. July 22, 2022. https://appinventiv.com/blog/ios-app-development-cost-for-healthcare/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback