Apple fixes 2 iOS zero-day vulnerabilities actively used in attacks

bleepingcomputer.com/news/apple/apple-fixes-2-ios-zero-day-vulnerabilities-actively-used-in-attacks/

Lawrence Abrams

By
Lawrence Abrams

- May 3, 2021
- 06:56 PM
- 0

Today, Apple has released security updates that fix two actively exploited iOS zero-day vulnerabilities in the Webkit engine used by hackers to attack iPhones, iPads, iPods, macOS, and Apple Watch devices.

"Apple is aware of a report that this issue may have been actively exploited," the company said in multiple security advisories published today.

Webkit is Apple's browser rendering engine that is required to be used by all mobile web browsers in iOS and other applications that render HTML, such as Apple Mail and the App Store.

These vulnerabilities are tracked as CVE-2021-30665 and CVE-2021-30663, and both allow arbitrary remote code execution (RCE) on vulnerable devices simply by visiting a malicious website.

RCE vulnerabilities are considered the most dangerous as they allow attackers to target vulnerable devices and execute commands on them remotely.

CVE-2021-30665 was discovered by Yang Kang, zerokeeper, and Bian Liang of Qihoo 360 ATA, while CVE-2021-30663 was reported to Apple by a researcher who wishes to remain anonymous.

The list of affected devices includes:

- iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)
- macOS Big Sur
- Apple Watch Series 3 and later

The zero-days were addressed by Apple earlier today in the iOS 14.5.1, iOS 12.5.3, macOS Big Sur 11.3.1, and the watchOS 7.4.1 updates.

iOS 14.5.1 update

This update also resolved a bug that prevented users from seeing App Tracking Transparency prompts within apps.

"This update fixes an issue with App Tracking Transparency where some users who previously disabled Allow Apps to Request to Track in Settings may not receive prompts from apps after re-enabling it," stated Apple in their iOS 14.5.1 release notes.

Apple has been dealing with a stream of actively exploited zero-day vulnerabilities over the past few months, with one fixed in macOS last month and numerous other iOS vulnerabilities fixed in the previous months.

Related Articles:

Apple emergency update fixes zero-day used to hack Macs, Watches

Apple emergency update fixes zero-days used to hack iPhones, Macs

Spring patches leaked Spring4Shell zero-day RCE vulnerability

Cisco urges admins to patch IOS XR zero-day exploited in attacks

Adware Maker Tries to Intimidate Security Firm with Cease and Desist Letters

- Apple
- iOS
- macOS
- Security Update
- Vulnerability
- Zero-Day

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: