iOS vulnerability that let you jailbreak your iPhone is once again dead

reader comments

56 with 48 posters participating

Share this story

The iOS vulnerability that made it possible for users and hackers to jailbreak fully up-to-date iPhones and iPads is no more, following an update Apple released on Monday that patches the highly unusual bug.

The security advisory accompanying the release of iOS version 12.4.1 says it patches a kernel vulnerability that allows malicious apps to execute code that runs with the highest of privileges. (The use-after-free vulnerability was first fixed in iOS 12.3.) Then, last weekend, researchers noticed that version 12.4, released in June, was once again vulnerable. Jailbreak enthusiasts—who like the freedom that such vulnerabilities permit—quickly capitalized on the Apple developer mistake by releasing exploits that worked on fully patched devices.

Jailbreaking phones allows users to do all kinds of things that aren’t normally possible, including installing unauthorized apps. But that freedom can potentially work to the favor of malicious hackers. Jailbreaking may weaken iOS protections that prevent an app from reading or modifying another app’s data.

Jailbreaking can also allow malicious apps to silently install spyware. In 2016, a malicious attack known as Pegasus that was delivered by text message used a then-secret jailbreak vulnerability to install stealthy malware on iOS devices targeted by the United Arab Emirates government.

Over the years, publicly known jailbreaks have grown increasingly rare. The jailbreak discovered last weekend was all the more unusual because it was the result of a flaw Apple developers already knew of and, indeed, had already fixed. That vulnerability—tracked as CVE-2019-8605—was originally found by Google researcher Ned Williamson. Somehow, the same flaw appears also to have been reintroduced into macOS version 10.14.6, according to an advisory that was published on Monday for a supplemental update of the OS.

Apple's Monday advisories credited a jailbreak researcher who goes by the handle Pwn20wnd with the discovery of the bug regression in both iOS and macOS. On Twitter, the researcher confirmed the mobile update effectively killed the jailbreak. While the researcher advised people to "Stay on iOS 12.4!" Ars recommends everyone update as soon as possible.

https://arstechnica.com/?p=1558201