Apple reveals two iOS zero-day vulnerabilities that allow attackers to access fully patched devices

4 May 2021, by Sarah Katz

Apple mobile iOS. Credit: Unsplash

One week after Apple carried out its largest iOS and iPad update since September 2020's version 14.0 release, the company has followed up with a new patch for two zero-day vulnerabilities that let hackers execute malicious code on fully updated devices. Additionally, the new release of 14.5.1 also mitigates issues with a bug in the recent App Tracking Transparency feature included in the previous version.

Both of these vulnerabilities are located in the browser engine Webkit, which provides web content for App Store, Mail and Safari as well as other various apps running on iOS, Linux and macOS. Apple described this attack as the processing of maliciously crafted web content resulting in arbitrary code execution. As of now, these two zero-days have been patched.

So far, Apple has issued a notice that these vulnerabilities may have already been exploited. The company has also announced that the second zero-day was discovered by Chinese security research firm Qihoo 360, whereas an anonymous source reported the first vulnerability. At this time, Apple has yet to offer details regarding who is carrying out the exploits or who faces a risk of exploitation.

Google's Project Zero vulnerability research team has assessed that these three new vulnerabilities make the total number of seven actively exploited Apple zero-days. In fact, out of 22 zero-days discovered in 2021 alone, nearly 33 percent have targeted Apple mobile OS. This makes iOS the software most targeted by zero-day after Chrome.

Since these vulnerabilities have been patched, Facebook has taken some issue due to the new security restrictions not allowing the Facebook app to track user activity across other installed applications without explicit user permission. Furthermore, another bug may cause graying out of the App Tracking Transparency toggle in the settings menu, even after users have updated to iOS 14.5.1.

Overall, Apple security and vulnerability research teams emphasize that these types of zero-days pose such a threat to both defenders and users due to the lack of knowledge surrounding their presence. After all, if hackers manage to execute evil code or access a privileged system before incident responders and researchers even realize the vulnerabilities in question exist, the attackers can steal a plethora of data, causing potentially immeasurable damage.

Alongside patches for the discovered vulnerabilities, Apple has also confirmed a patch for the App Tracking Transparency feature bug. This fix will enable users to once again opt out of ad tracking on their Apple devices.

More information: support.apple.com/en-us/HT212336
support.apple.com/en-us/HT212335
support.apple.com/en-us/HT212339

APA citation: Apple reveals two iOS zero-day vulnerabilities that allow attackers to access fully patched devices (2021, May 4) retrieved 11 May 2021 from https://techxplore.com/news/2021-05-apple-reveals-ios-zero-day-vulnerabilities.html