Find out how to install malicious code on iPhone even when it is powered off

In one of the first security analyzes of the Find My functionality on iOS, security researchers have uncovered a new attack surface.

In one of the first security analyzes of the Find My functionality on iOS, security researchers have uncovered a new attack surface. Specifically, hackers can tamper with firmware and upload malicious code to the Bluetooth chip, which operates even when the iPhone is powered off.

This mechanism takes advantage of the fact that wireless chips related to Bluetooth, Near Field Communication (NFC), and ultra-wideband (UWB) will continue to work when iOS has turned off iPhone and entered standby mode. Low Power Mode (LPM) energy storage.

This is the solution that Apple came up with to enable features like Find My and support Express Card transactions even when the iPhone is powered off. In addition, all three wireless chips have direct access to the security magnetic section. Therefore, on iPhone models that support find even when powered off, the wireless chips cannot be abused even when the device is turned off, posing a new threat model.

The LPM feature, introduced by Apple last year with iOS 15, makes it possible to find your device using Find My even when the battery is dead or the power is off. Currently, iPhone models that support UWB include iPhone 11, iPhone 12, and iPhone 13.

When you power off these iPhone models, you'll get a message that says: iPhone can still be found after powering off. Find My helps locate this iPhone when it's lost or stolen, even when it's in power reserve mode or when it's powered off."

The researchers said Apple was not strict in the implementation of LPM. Sometimes the process of launching Find My ads also fails during power off. Furthermore, they discovered the Bluetooth firmware had no digital signature or encryption at all.

By taking advantage of the above loopholes, hackers with privileged access can create malicious code that can execute on the iPhone's Bluetooth chip even when it is powered off.

However, to be able to compromise firmware hackers must be able to interact with the firmware via the operating system, modify the firmware image or execute code on the LPM-enabled chip over the network by exploiting vulnerabilities such as BrakTooth,

The new attack method and vulnerabilities were responsibly reported by the researchers to Apple, but the Apple side remained silent and did not respond. Therefore, the research team presented their findings at the ACM Conference on Security and Privacy under the framework of the International Mobile and Wireless Networks (WiSec 2022) event that just took place.

Researchers believe that when designing LPM, Apple only cares about functionality and ignores security. Therefore, Apple needs to make adjustments to ensure user safety.