Cops are concerned after iPhone units are mysteriously rebooting so they can't be unlocked

Alan Friedman ⋮ 5-6 minutes ⋮ 11/8/2024

This is a strange story. Multiple iPhone units, sent to a forensic lab on October 3rd, 2024, rebooted themselves leaving law enforcement officials concerned about a new security feature that

Apple might have included with

iOS 18. These stored devices, which have been collected as evidence in certain cases, had been disconnected for some time from a cellular network and were all running iOS 18. One of the iPhone units was in Airplane Mode and another one was unable to receive electrical signals since it was placed inside a Faraday cage.

Because the reboots make it harder to unlock these iPhones, law enforcement officials, according to a

document obtained by 404 Media, say that the rebooting could be part of a new security feature. The theory is once an iPhone is disconnected from a cellular network for a period of time, they will now automatically reboot. Once an iPhone is rebooted, it is considered to be more secure against the machines used by law enforcement that use brute force and other techniques to figure out the passcode to unlock the phone. Once unlocked, law enforcement officials can comb through the data inside the device.

"The purpose of this notice is to spread awareness of a situation involving iPhones, which is causing iPhone devices to reboot in a short period of time (observations are possibly within 24 hours) when removed from a cellular network."-Police document

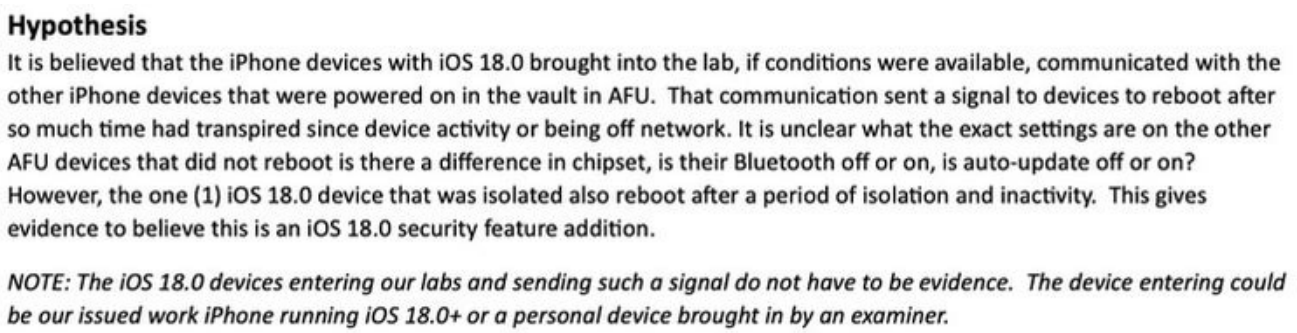
The document was obtained by 404 Media from a mobile forensics source. The document was corroborated by a second mobile forensics source who had already seen the same document and sent 404 Media a small portion of it for verification purposes.

According to this document, a digital forensics lab had a number of iPhone units in After First Unlock (AFU) state. This means that since the last tine the phone was powered on, the device had been unlocked (presumably by the owner of the device) using a passcode at least once. It is easier for law enforcement to use password cracking tools like the Cellebrite machines to unlock an iPhone if it is in the AFU state.

After the reboot, these iPhone units went into a Before First Unlock (BFU) state and current technology prevents iPhones in this state from being cracked open wtih a Cellebrite or similar type of machine.

The document also has one hypothesis that states the iPhone models with iOS 18 installed communicated with other iPhone models held by the same forensic lab in a vault. That communication was a signal to other iPhone units not updated to iOS 18 in the AFU state

telling them to reboot after being cut off a cellular network for a predetermined time period. This signal could come from iPhone devices running iOS 18 and later that are being used as evidence in police cases, but also with the personal iPhone models owned by forensic examiners that run iOS 18 and later.



Hypothesis

It is believed that the iPhone devices with iOS 18.0 brought into the lab, if conditions were available, communicated with the other iPhone devices that were powered on in the vault in AFU. That communication sent a signal to devices to reboot after so much time had transpired since device activity or being off network. It is unclear what the exact settings are on the other AFU devices that did not reboot is there a difference in chipset, is their Bluetooth off or on, is auto-update off or on? However, the one (1) iOS 18.0 device that was isolated also reboot after a period of isolation and inactivity. This gives evidence to believe this is an iOS 18.0 security feature addition.

NOTE: The iOS 18.0 devices entering our labs and sending such a signal do not have to be evidence. The device entering could be our issued work iPhone running iOS 18.0+ or a personal device brought in by an examiner.

The hypothesis from a leaked law enforcement document about iPhone units held for forensic analysis. | Image credit-404 Media

If true, this would be a brilliant move by Apple to enhance the security of iPhones being held by law enforcement. By having the units running iOS 18 and later held by law enforcement signal other iPhone models to reboot, even the personal iPhones owned by forensic examiners could be used to block police, the FBI, and other alphabet soup agencies unlock a person's iPhone with the intent of running through the owner's personal data looking for evidence.

"That is utterly bizarre and amazing. The idea that phones should reboot periodically after an extended period with no network is absolutely brilliant and I'm amazed if indeed Apple did it on purpose."-Matthew Green, cryptographer, associate professor at Johns Hopkins University

The law enforcement document ended with a recommendation. Labs trying to extract data from iPhone units in the AFU state that have not yet been updated to iOS 18 should be isolated and not exposed to iPhone devices that have been updated to iOS 18 or later to prevent them from receiving the signal to reboot.

There is no definitive proof that Apple has created a security system in iOS 18 that reboots iPhone units removed from a cellular network and sends signals to other iPhone units to reboot. However, there is also a common sense explanation. Last month, several

iPhone 16 Pro and

iPhone 16 Pro Max users

complained about their devices rebooting randomly. This bug was exterminated with the iOS 18.1 update.

View Full Bio

Alan, an ardent smartphone enthusiast and a veteran writer at PhoneArena since 2009, has witnessed and chronicled the transformative years of mobile technology. Owning iconic phones from the original iPhone to the iPhone 15 Pro Max, he has seen smartphones evolve into a global phenomenon. Beyond smartphones, Alan has covered the emergence of tablets, smartwatches, and smart speakers.