UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO)

New York State Intelligence Center

Intelligence Bulletin

IAU@nysic.ny.gov
1-866-48-NYSIC (866-486-9742)

November 21, 2024 **NYSIC-IB-24-23**

(U) iOS 18 - Inactivity Reboot After 72 Hours in Locked State - UPDATE

(U) SUMMARY:

(U) The "Inactivity Reboot" feature in iOS 18.1, which triggers an automatic device restart after 72 hours of inactivity, introduces challenges for law enforcement in seizing, analyzing, and preserving digital evidence. This enhancement to data security has operational, forensic, and legal implications, which may require updated strategies to mitigate its impact.

(U//FOUO) It is critically important that law enforcement secure legal authority swiftly when seeking access to electronic devices to ensure the admissibility of evidence and protection of constitutional rights. Exceptions are limited to exigent circumstances where probable cause exists that the device contains evidence of a crime and immediate action is necessary.

(U) DETAILS:

(U) Beginning with iOS 18.0,[A] Apple[USBUS] added an inactivity reboot timer into the operating system. An iPhone running iOS 18.1 will automatically reboot if it remains in a locked state and is not unlocked for 72 hours, a situation that could occur while a phone is being stored prior to forensic evaluation.[1]

(U) Operational Implications for Field Personnel

(U) Law enforcement personnel involved in seizing iPhone devices are directly impacted by the iOS 18 inactivity reboot. The 72-hour inactivity reboot necessitates swift action to secure and process devices. Without timely imaging or unlocking, devices restart and revert to the "Before First Unlock" (BFU) phase.[2] The BFU state significantly limits access to data and requires advanced forensic tools to bypass.

(U) Implications for Digital Forensics Professionals

(U) The post-reboot encryption state restricts access to device contents, placing additional burdens on forensic examiners.[3] Tools capable of expedited data acquisition, such as GrayKey, may now be increasingly leveraged for digital forensics. Examiners may also leverage resources like the shutdown log file (shutdown.log) within the iOS file system to identify and timestamp reboots. This log, located at /private/var/db/diagnostics, provides essential information about reboot events, and assists in reconstructing device activity.[4]

(U) Legal Considerations

(U//FOUO) The reboot feature amplifies the distinction between seizure (securing a device) and search (accessing its contents). While seizing a device prevents its loss or destruction, the reboot feature could render it effectively inaccessible without appropriate warrants or user cooperation. This highlights the critical importance of securing legal authority swiftly. Where exigent circumstances exist, the phone may be unlocked and extracted without consent or a warrant. This is only permissible where probable cause exists that the device contains evidence of a crime, and articulable circumstances exist that make it impossible to obtain a warrant for the contents of the phone within 72 hours.

[A] (U) Apple introduced the inactivity reboot timer into the code of iOS 18.0, which was originally tied to 7 days of inactivity. Now, in iOS 18.1, the timer is 72 hours (3 days).

Requirements: NY-SIN / HSEC-SIN 4.8, 5.8, 8.8

UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO)

(U) RECOMMENDATIONS:

(U//FOUO) To mitigate the challenges posed by the iOS 18 inactivity reboot, law enforcement agencies may consider the following:

- (U//FOUO) *Policy updates* – review and amend standard operating procedures for digital evidence handling, emphasizing the urgency of data imaging within 72 hours of seizure.
- (U//FOUO) *Legal collaboration* – work closely with legal teams to address potential evidentiary challenges, particularly regarding timely warrants for device unlocking and extraction.

(U//FOUO) The iOS 18 inactivity reboot reinforces Apple's commitment to user data security while complicating law enforcement efforts to retrieve digital evidence. The New York State Police Computer Forensic Lab (CFL) and statewide Computer Crimes Units (CCUs) can assist with the imaging and extraction of cellular devices. Law enforcement are encouraged to call their local CFL or CCU in advance to verify the availability of an extraction tool. Members with additional questions may contact the CFL at NYSPCCU@troopers.ny.gov.

(U) Endnotes:

---

[1] (U) Website | Magnet Forensics | 13 November 2024 | "Understanding the security impacts of iOS 18's inactivity reboot" | https://www.magnetforensics.com/blog/understanding-the-security-impacts-of-ios-18s-inactivity-reboot/ | UNCLASSIFIED.
[2] (U) Website | Dataconomy | 13 November 2024 | "Law enforcement faces challenges with iPhones' automatic rebooting | https://dataconomy.com/2024/11/13/law-enforcement-faces-challenges-with-iphones-automatic-rebooting/ | UNCLASSIFIED.
[3] (U) Ibid.
[4] (U) Website | Magnet Forensics | 13 November 2024 | "Understanding the security impacts of iOS 18's inactivity reboot" | https://www.magnetforensics.com/blog/understanding-the-security-impacts-of-ios-18s-inactivity-reboot/ | UNCLASSIFIED.