INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-19 19:00 UTC

usbliter8: Unpatchable SecureROM Exploit Targets A12/A13 Apple Silicon via USB DMA Buffer Underflow

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0226
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Apple iPhone XS, XS Max, XR, iPhone 11 series, iPhone SE (2nd gen); iPad Air 3rd gen, iPad mini 5th gen, iPad 8th gen; Apple Watch Series 4, 5, SE (1st gen); HomePod mini, all devices using A12, A13, S4, or S5 SoCs
Published	2026-06-19T14:37:41
Discovery Source	Rss

Executive Summary

A public exploit called usbliter8, released June 18, 2026 by the group Paradigm Shift, achieves privileged code execution inside the SecureROM of Apple A12 and A13 silicon, the same immutable boot ROM that anchors the entire iOS trust chain. Because the flaw lives in read-only hardware, Apple cannot patch it; every affected device is permanently compromised at the hardware root of trust for the remainder of its operational life. Organizations that rely on iPhones, iPads, Apple Watches, or HomePod minis built on A12, A13, S4, or S5 chips for sensitive, regulated, or high-assurance work must treat those devices as untrustworthy endpoints with no remediation path short of hardware replacement.

Technical Analysis

usbliter8 is a SecureROM-level exploit targeting a USB Direct Memory Access (DMA) buffer underflow, classified under CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer), CWE-787 (Out-of-bounds Write), and CWE-121 (Stack-based Buffer Overflow), in the boot ROM silicon of Apple's A12 and A13 SoCs, as well as the associated S4 and S5 chips used in Apple Watch and HomePod mini. The attack surface is Device Firmware Update (DFU) mode, a low-level USB recovery interface that operates before the operating system loads and before any software-layer security control can intervene.

The exploit maps squarely to MITRE ATT&CK T1542.003 (Pre-OS Boot: Bootkit), T1200 (Hardware Additions), T1014 (Rootkit), and T1082 (System Information Discovery). DFU mode exploitation also connects to

T1195.003 (Supply Chain Compromise: Compromise Hardware Supply Chain) in scenarios where devices are intercepted and implanted before deployment. Once usbliter8 achieves execution within SecureROM, the attacker controls the foundational layer of the Apple Secure Boot chain, the layer that validates every subsequent firmware and OS component. From that position, persistence (T1542.003) and arbitrary code execution (T1059) become achievable without leaving artifacts detectable by iOS-layer security tools.

The physical access requirement, placing a device in DFU mode, limits opportunistic, remote exploitation. However, this barrier is well within reach of insider threats, device interception during shipping or repair, border crossing scenarios, law enforcement or intelligence agencies, and forensic extraction firms. The public release of a working proof-of-concept by Paradigm Shift on June 18, 2026 is a critical escalation: prior to public availability, exploitation required sophisticated actors with independent research capability. Post-release, the barrier drops to anyone capable of following documented steps.

The closest historical analogue is checkm8, a SecureROM USB DMA vulnerability disclosed in September 2019 by researcher axi0mX, affecting A5 through A11 chips. checkm8 has been operationalized continuously since disclosure, powering jailbreak tools like checkra1n, commercial mobile forensic platforms (Cellebrite, GrayKey), and threat actor toolkits. usbliter8 extends that legacy to the next two chip generations, meaning devices released through 2020 (iPhone 11 series, iPad 8th gen, iPad mini 5th gen, iPad Air 3rd gen, Apple Watch SE 1st gen, HomePod mini) now share the permanent, unremediable trust boundary failure that has defined the checkm8-affected fleet since 2019.

The source material is drawn from The Hacker News reporting (June 2026) and cross-referenced Apple device/SoC compatibility data. No CVE identifier has been assigned; no CVSS vector from Apple is available. The qualitative severity assessment of High and a CVSS base score of 7.5 reflect the permanent, unremediable nature of the flaw and the public availability of a working exploit, weighted against the physical access prerequisite.

Action Checklist

1. Step 1: Assess exposure, inventory every Apple device in your fleet and identify those running A12, A13, S4, or S5 silicon: iPhone XS, XS Max, XR, iPhone 11/11 Pro/11 Pro Max, iPhone SE (2nd gen), iPad Air 3rd gen, iPad mini 5th gen, iPad 8th gen, Apple Watch Series 4/5/SE (1st gen), and HomePod mini. Cross-reference against CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory).
2. Step 2: Classify affected devices by sensitivity tier, identify which of the inventoried devices access regulated data, sensitive systems, or serve in high-assurance roles (executive devices, privileged admin workstations, BYOD with corporate email/VPN). Apply AC-3 (Access Enforcement) and AC-6 (Least Privilege) to restrict these devices' access to sensitive resources until a hardware replacement plan is in place.
3. Step 3: Enforce physical security controls, because exploitation requires DFU mode access, treat physical custody of affected devices as a security control. Revise device handling policies: prohibit unescorted device repair, flag devices sent for third-party service, and implement chain-of-custody logging for devices that leave organizational premises. Reference NIST SP 800-53 PE (Physical and Environmental Protection) controls for incident handling context.
4. Step 4: Update mobile device management (MDM) posture, enforce MDM enrollment attestation checks and consider revoking access to sensitive resources from affected-SoC devices that cannot be verified as uncompromised. Review AC-17 (Remote Access) and AC-19 (Access Control for Mobile Devices) for policy alignment.

5. Step 5: Revise threat model and risk register, add usbliter8 to your hardware root-of-trust threat scenarios. Map to MITRE ATT&CK T1542.003, T1200, and T1014. Document that the affected device fleet has no software remediation path and that risk acceptance or hardware replacement are the only disposition options.

6. Step 6: Communicate device replacement posture to leadership, brief CISOs and relevant business owners that affected devices cannot be made compliant through patching. Frame the decision as a hardware lifecycle acceleration, not a vendor failure response. Include total fleet count, replacement cost estimate, and timeline.

7. Step 7: Monitor for follow-on tooling, track public repositories, jailbreak community forums, and mobile forensics vendor announcements for usbliter8-based tools analogous to checkra1n. A working public exploit is a precursor to operationalized toolkits. Assign a threat intelligence owner to this watch item per AU-6 (Audit Record Review, Analysis, and Reporting).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if MDM telemetry or network logs reveal any affected A12/A13 device exhibiting post-exploitation indicators (anomalous DFU enumeration, supervision status change, or C2-pattern outbound traffic) AND that device was used to access regulated data (PII, PHI, PCI) — this combination triggers breach notification assessment obligations under HIPAA, state privacy laws, and PCI-DSS Requirement 12.10.
Recovery Notes	Recovery for usbliter8-affected devices is hardware-dependent: there is no software recovery path that restores a trusted boot state, because the SecureROM flaw is immutable. For devices that must remain in service pending replacement, 'recovery' means verifying that compensating controls from Steps 2–4 remain enforced (access restrictions, MDM posture, physical custody controls) and establishing a 90-day re-attestation cadence. Post-replacement, verify that incoming devices use A14 silicon or later (iPhone 12 series and newer) by cross-referencing MDM hardware model identifiers against Apple's SoC documentation before restoring access to sensitive resources.

Forensic Artifacts	Apple MDM enrollment and compliance state export (timestamped CSV of device UDID, hardware model, last check-in, supervision status, and OS version) captured before any MDM policy changes — anomalous supervision status changes post-usbliter8 disclosure are a primary indicator of exploitation | Windows System Event Log entries from Apple Mobile Device Service (source: 'AppleMobileDeviceService', channel: System) on any Windows host used for device management — DFU mode USB enumeration produces a distinct device class event that differs from normal iTunes sync and indicates a potential usbliter8 exploitation attempt | Network firewall or proxy session logs for affected device IP addresses covering 30 days prior to June 18, 2026 (usbliter8 public release date) — focus on outbound connections to non-corporate IPs on ports 443/80 from device IP ranges, which may reveal C2 activity from implants installed before public disclosure | Physical access control system (PACS) badge logs for device storage rooms, IT repair areas, or MDM management workstations — because usbliter8 exploitation requires physical USB access, PACS logs are the primary evidence source for establishing when and by whom a device may have been physically accessed for exploitation | VPN concentrator session logs filtered by affected device UDID or certificate CN for the 60 days preceding disclosure — a device compromised via usbliter8 and implanted with a persistent payload may show session anomalies (unusual connection hours, anomalous data volumes, or connections from geolocation inconsistent with the assigned user) that predate the public exploit release, suggesting earlier private exploitation by Paradigm Shift or affiliated actors

Per-Action IR Details

Step 1: Assess exposure — inventory every Apple device in your fleet and identify those running A12, A13, S4, or S5 silicon: iPhone XS, XS Max, XR, iPhone 11/11 Pro/11 Pro Max, iPhone SE (2nd gen), iPad Air 3rd gen, iPad mini 5th gen, iPad 8th gen, Apple Watch Series 4/5/SE (1st gen), and HomePod mini. Cross-reference against CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory).

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establish IR capability and asset visibility before incidents occur; accurate asset inventory is a prerequisite for scoping any hardware-rooted compromise.

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: Query your MDM platform (Jamf Free/Apple Configurator) for device model and SoC identifiers: run `profiles list` on enrolled devices or export MDM inventory to CSV and filter for model identifiers A1920, A2097, A2160, A2217, A2111 (iPhone XS/XR/11 family) and equivalent iPad/Watch model strings. For unmanaged BYOD, collect self-reported device model via a one-page attestation form distributed by email.

Evidence: No live-state alteration occurs in this step; however, capture the MDM enrollment roster and device hardware model/UDID export before any containment actions are taken — this roster is the baseline scope document for the entire incident and must not be modified by subsequent MDM policy pushes. Preserve a timestamped CSV export of the MDM inventory as a forensic artifact.

Step 2: Classify affected devices by sensitivity tier — identify which of the inventoried devices access regulated data, sensitive systems, or serve in high-assurance roles (executive devices, privileged admin workstations, BYOD with corporate email/VPN). Apply AC-3 (Access Enforcement) and AC-6 (Least Privilege) to restrict these devices' access to sensitive resources until a hardware replacement plan is in place.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Select and implement a containment strategy that limits further damage; for a permanent hardware-rooted vulnerability with no patch path, access restriction is the primary containment lever.

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 3.3 (Configure Data Access Control Lists)

Compensating: For teams without a NAC solution, use conditional access rules in Microsoft Entra ID (free tier) or Google Workspace device policies to block OAuth token issuance to devices whose MDM-reported hardware model matches affected SoC families. Alternatively, create a network VLAN segment for affected devices using pfSense firewall rules that permit only outbound internet access and deny routing to internal RFC 1918 ranges.

Evidence: Before revoking VPN certificates or MDM access tokens for affected devices, capture: (1) active VPN session logs showing source device UDID and connection timestamps from your VPN concentrator; (2) Microsoft Entra ID or Okta sign-in logs filtered by device hardware model for the 30 days preceding the usbliter8 disclosure (June 18, 2026) — look for anomalous off-hours authentications or access to privileged resources that may indicate prior exploitation; (3) MDM compliance state snapshot for all affected devices showing last check-in time and policy posture before any policy changes are pushed.

Step 3: Enforce physical security controls — because exploitation requires DFU mode access, treat physical custody of affected devices as a security control. Revise device handling policies: prohibit unescorted device repair, flag devices sent for third-party service, and implement chain-of-custody logging for devices that leave organizational premises. Reference NIST IR family controls for incident handling context.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Containment for usbliter8 must address the physical attack vector; DFU mode exploitation requires USB cable attachment to the target device, making physical custody the operative security boundary.

Controls: NIST AC-3 (Access Enforcement), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Implement a paper-based chain-of-custody log (device UDID, custodian name, departure/return timestamp, purpose) for any affected device leaving the premises. For repair scenarios, require the accompanying staff member to remain present during any USB connection event. Use a tamper-evident USB port blocker (commercially available, under $5/unit) on devices in storage or repair queues to provide a physical indicator of unauthorized DFU mode attempts.

Evidence: Because DFU mode exploitation via usbliter8 leaves no persistent iOS-layer log (the attack occurs below the OS in SecureROM), the primary forensic indicator of physical access is external: review physical access control system (PACS) badge logs for server rooms or device storage areas around the time of any suspected exploitation. If available, pull USB connection event logs from any Windows host used for device management — look for Apple Mobile Device (AMD) driver events (Windows Event Log, System channel, source 'AppleMobileDeviceService') indicating DFU mode enumeration, which presents as a distinct USB device class distinct from normal iTunes sync mode.

Step 4: Update mobile device management (MDM) posture — enforce MDM enrollment attestation checks and consider revoking access to sensitive resources from affected-SoC devices that cannot be verified as uncompromised. Review AC-17 (Remote Access) and AC-19 (Access Control for Mobile Devices) for policy alignment.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: MDM attestation enforcement is the principal software-layer containment mechanism available when the hardware root of trust is compromised; it limits blast radius by removing network trust granted to potentially exploited devices.

Controls: NIST AC-17 (Remote Access), NIST AC-19 (Access Control For Mobile Devices), CIS 6.2 (Establish an Access Revoking Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: In Jamf Pro or Jamf Now (free tier supports up to 3 devices; use School Manager free enrollment for larger fleets temporarily), create a smart group scoped to affected device model identifiers and push a configuration profile that removes Wi-Fi and VPN payloads. For Microsoft 365 environments, use Intune compliance policies (free with M365 Business Basic) to mark affected hardware models as non-compliant, which blocks Conditional Access to Exchange Online and SharePoint automatically.

Evidence: Before revoking MDM enrollment certificates or pushing profile removal, capture: (1) the full MDM command queue and device compliance state report — a compromised device whose SecureROM is backdoored may report false MDM compliance states, so preserve the pre-revocation attestation response payload as evidence of potential integrity subversion; (2) network flow logs (NetFlow or firewall session table) for affected devices' IP addresses for the 72 hours preceding this action, focusing on connections to non-corporate IP ranges that could indicate C2 beaconing established via a post-usbliter8 implant.

Step 5: Revise threat model and risk register — add usbliter8 to your hardware root-of-trust threat scenarios. Map to MITRE ATT&CK T1542.003, T1200, and T1014. Document that the affected device fleet has no software remediation path and that risk acceptance or hardware replacement are the only disposition options.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons-learned and threat model updates are post-incident activities that institutionalize knowledge from an incident; documenting an unpatchable hardware vulnerability formally closes the remediation decision loop.

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Maintain the risk register as a shared spreadsheet (Google Sheets or Confluence page) with columns for: threat name, CVE/identifier, affected asset list (linked to the MDM inventory export from Step 1), disposition decision (accept/replace/retire), decision owner, and review date. For usbliter8 specifically, the 'patch ETA' field should be documented as 'N/A — hardware root-of-trust vulnerability, no vendor patch possible' to prevent future analysts from treating it as a pending patch item.

Evidence: No live-state alteration in this step; however, the risk register entry should reference and link to the preserved forensic artifacts from Steps 1–4 as supporting documentation. The ATT&CK technique mappings (T1542.003 — Bootkit, T1200 — Hardware Additions, T1014 — Rootkit) are referenced here for threat modeling context only and do not constitute defensive controls.

Step 6: Communicate device replacement posture to leadership — brief CISOs and relevant business owners that affected devices cannot be made compliant through patching. Frame the decision as a hardware lifecycle acceleration, not a vendor failure response. Include total fleet count, replacement cost estimate, and timeline.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Effective post-incident communication to leadership is required to drive resource allocation decisions; for usbliter8, the permanent nature of the vulnerability means this communication triggers a capital expenditure decision, not a patch cycle.

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Prepare a one-page executive brief using the MDM inventory CSV from Step 1 as the data source. Include three columns: device type, count of affected units, and estimated replacement cost (reference Apple Business pricing or your carrier contract). For timeline, use the CIS v8.1 remediation process cadence as a baseline: critical-risk devices (executive, privileged admin) within 30 days; standard fleet within 90 days; BYOD/low-sensitivity within 180 days.

Evidence: No volatile evidence capture required for this step. Retain the executive brief and any written risk acceptance decisions as formal records — if a regulated device (one handling PII, PHI, or payment card data) is accepted as a known risk rather than replaced, that decision may constitute a compliance disclosure obligation under HIPAA, PCI-DSS, or applicable state breach notification law and should be documented with legal counsel's review.

Step 7: Monitor for follow-on tooling — track public repositories, jailbreak community forums, and mobile forensics vendor announcements for usbliter8-based tools analogous to checkra1n. A working public exploit is a precursor to operationalized toolkits. Assign a threat intelligence owner to this watch item per AU-6 (Audit Record Review, Analysis, and Reporting).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Ongoing threat intelligence monitoring for derivative tooling is a post-incident requirement; the checkra1n precedent (which operationalized the checkm8 SecureROM exploit into a one-click jailbreak tool within weeks) establishes that usbliter8 will almost certainly be weaponized into forensic and implant toolkits.

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Configure free GitHub RSS feeds or use github.com/search?q=usbliter8&type=repositories with a weekly manual review cadence. Set Google Alerts for 'usbliter8', 'A12 jailbreak', and 'Paradigm Shift exploit' to catch forum discussions and researcher posts. Monitor /r/jailbreak, iH8sn0w Twitter/X, and the #jailbreak channel in public security Discord servers. For MDM-enrolled devices, enable Jamf's built-in OS version compliance reporting to detect if any affected device is rebooted into a modified firmware state (post-exploitation devices may show anomalous activation lock or supervision status changes).

Evidence: For this monitoring step, establish a baseline before any derivative toolkit is released: snapshot the current iOS version distribution across all affected-SoC devices from MDM, and record the expected activation lock and supervision status for each enrolled device. If a usbliter8-based toolkit emerges (analogous to checkra1n), the forensic indicators to watch for on potentially exploited devices include: (1) unexpected changes in MDM supervision status; (2) Apple Mobile Device logs on management hosts showing DFU-mode USB enumeration outside of authorized maintenance windows; (3) network traffic from affected device IP addresses to known jailbreak repository CDN ranges (e.g., Cydia/Sileo infrastructure IPs) captured via firewall or proxy logs.

Detection Guidance

Detection of active usbliter8 exploitation is constrained by the attack's pre-OS execution context, by the time iOS boots, the compromise may already be established below the observable stack. However, several detection and hunting opportunities exist.

Physical access indicators: Monitor for unexpected device reboots into DFU mode (visible as a device that is unresponsive and not recognized as a normal iOS device by connected management systems). If your MDM platform reports a device as 'unenrolled' or 'unrecognized' after a period of normal enrollment, treat it as a potential tampering indicator.

MDM attestation gaps: Apple's MDM framework can attest device integrity state. After exploitation, a device may fail Device Enrollment Program (DEP) attestation or present an unexpected device identifier. Review MDM enrollment logs (AU-2: Event Logging) for devices that re-enroll unexpectedly or with changed hardware identifiers.

Jailbreak artifact detection: Post-exploitation, usbliter8-based jailbreaks will likely install persistence mechanisms analogous to checkra1n artifacts, look for unexpected processes, filesystem modifications outside the iOS sandbox, or SSH server presence detectable via network scanning. Mobile threat defense (MTD) solutions (CrowdStrike Falcon for Mobile, Jamf Protect, Lookout) should be tuned to flag known jailbreak indicators on enrolled devices.

DFU-mode USB traffic: In controlled environments where devices are connected to managed USB hubs or charging stations, monitor for USB traffic patterns consistent with DFU mode enumeration (device presenting as Apple Mobile Device [DFU Mode] in USB device logs).

D3FEND countermeasures to apply: D3-SFA (System File Analysis), monitor for unexpected filesystem changes post-boot; D3-LAM (Local Account Monitoring), watch for new or unexpected local accounts on managed devices; D3-UAP (User Account Permissions), audit permission changes on affected devices.

CIS 8.2 (Collect Audit Logs) should be verified as active across MDM platforms and MTD solutions covering the affected device fleet. NIST AU-6 (Audit Record Review, Analysis, and Reporting) should drive periodic review of

MDM enrollment and device health attestation logs for anomalies.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`usbliter8`	Public proof-of-concept exploit tool released by Paradigm Shift on June 18, 2026, leveraged via physical DFU mode USB access to achieve privileged code execution within Apple SecureROM on A12/A13/S4/S5 SoCs	HIGH
TOOL	`Pending — refer to The Hacker News (https://thehackernews.com/2026/06/unpatchable-usbliter8-exploit-breaks.html) and Paradigm Shift's public release materials for published exploit hashes and supporting tool indicators`	Exploit binaries, supporting scripts, and any associated payload hashes published by Paradigm Shift at time of release — values not present in provided source material	LOW

Framework Mappings

MITRE-ATTACK

- **T1200** — Hardware Additions
- **T1014** — Rootkit
- **T1195.003** — Compromise Hardware Supply Chain
- **T1059** — Command and Scripting Interpreter
- **T1195** — Supply Chain Compromise
- **T1542.003** — Bootkit
- **T1082** — System Information Discovery

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A01:2021** — Broken Access Control

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1200	Hardware Additions	Initial-Access
T1014	Rootkit	Defense-Evasion
T1195.003	Compromise Hardware Supply Chain	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1195	Supply Chain Compromise	Initial-Access
T1542.003	Bootkit	Persistence
T1082	System Information Discovery	Discovery

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/unpatchable-usbliter8-exploit-bre...	T3
Apple Watch and iPhone compatibility	https://support.apple.com/en-us/118490	T3

Source	URL	Tier
List of Apple's mobile device codes types a.k.a. machine ids ... - GitHub	https://gist.github.com/adamawolf/3048717	T3
iOS version by device - iOS Ref	https://iosref.com/ios	T3
Here's the compatibility list for Apple's newly announced OSs - Reddit	https://www.reddit.com/r/apple/comments/1l7dfuy/heres_the_compatibi...	T3

Generated 2026-06-19 19:00 UTC by TJS Security Command Center