INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-19 13:53 UTC

Apple A12/A13 BootROM Unpatchable Exploit and Beats Bluetooth Eavesdropping Flaw Expose Layered Hardware Attack Surface

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0336
Type	CVE Vulnerability
CVE ID	CVE-2025-20701, CVE-2025-20700, CVE-2025-20702
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.0340 (87th percentile)
Affected Products	Apple Beats Studio Buds (Airoha Bluetooth Audio SDK); Apple iPhone/iPad devices with A12 and A13 chips (SecureROM/BootROM); Jabra devices using Airoha SDK (patched December 2025)
Published	2026-06-19T02:36:09
Discovery Source	Rss

Executive Summary

Two Apple hardware-layer vulnerabilities have been disclosed, together exposing a layered attack surface across consumer audio devices and iPhones and iPads with A12 and A13 chips. The Bluetooth flaw (CVE-2025-20701, CVSS 8.8) allows a physically proximate attacker to access the microphone on Beats Studio Buds without completing Bluetooth pairing, enabling covert eavesdropping. More critically, a separately disclosed BootROM exploit ('usbliter8'; CVE assignment pending) targets A12/A13 devices at the silicon level, is permanently unpatchable via software, and threatens secure boot chain integrity, cryptographic key storage, and biometric authentication, representing a durable, device-lifetime risk for any organization deploying these devices in sensitive environments.

Technical Analysis

Two distinct vulnerability clusters are present. First, CVE-2025-20701 (CVSS 8.8, CWE-306/CWE-863) is a missing authentication and authorization bypass in the Airoha Bluetooth Audio SDK. It affects Beats Studio Buds and Jabra devices using the same SDK. A physically adjacent, unauthenticated attacker can access the device microphone without completing Bluetooth pairing. Jabra issued patches in December 2025; Apple's

patch status for Beats Studio Buds should be confirmed against the Apple Security Advisory at support.apple.com/en-us/100100. CVE-2025-20700 and CVE-2025-20702 are part of the same Airoha SDK cluster; authoritative CVSS scores for each should be cross-referenced at nvd.nist.gov/vuln/detail/cve-2025-20702 and cve.org. Second, a separate BootROM vulnerability affects all Apple A12 and A13 chip devices (iPhone XS through iPhone 11 generation and corresponding iPad models). A published proof-of-concept exploit named 'usbliter8' enables arbitrary code execution at the SecureROM layer, the lowest firmware execution environment, before any OS-level or software security control initializes. Because BootROM is mask ROM, burned into silicon at fabrication, no software update can remediate this vulnerability. The attack path extends toward the Secure Enclave Processor (SEP), potentially undermining cryptographic key storage, biometric authentication (Face ID, Touch ID), and secure boot chain integrity. This exploit lineage is historically associated with checkm8 (A5-A11); extension to A12/A13 is a significant surface expansion. CVE assignment for the BootROM component is not confirmed in the source data; the CVE-2025-20700/20701/20702 cluster appears primarily associated with Airoha SDK. CWE-119 and CWE-120 (buffer overflow variants) are consistent with BootROM exploit mechanics. MITRE ATT&CK techniques mapped: T1542 (Pre-OS Boot), T1542.001 (System Firmware), T1011 (Exfiltration over Bluetooth), T1200 (Hardware Additions), T1557 (Adversary-in-the-Middle), T1552.004 (Private Keys), T1091 (Replication through Removable Media), T1195 (Supply Chain Compromise), T1040 (Network Sniffing). EPSS score is 0.034 (87th percentile), indicating elevated exploitation probability relative to the broader CVE population. Not currently on CISA KEV.

Action Checklist

1. Step 1: Containment. Identify all Beats Studio Buds and Jabra devices using the Airoha Bluetooth Audio SDK in your environment. Restrict use of Airoha-based audio devices in proximity to sensitive conversations, executive meetings, board rooms, and secure facilities until patch status is confirmed. For A12/A13 devices (iPhone XS, XS Max, XR, 11, 11 Pro, 11 Pro Max, and iPad equivalents) used in high-sensitivity roles, enforce a physical access policy: devices should not be left unattended with untrusted USB access, consistent with NIST AC-6 (Least Privilege).
2. Step 2: Detection. For the Bluetooth flaw, audit Bluetooth pairing logs on managed mobile devices for unexpected connection attempts to Beats or Airoha-SDK devices. Query MDM (Mobile Device Management) platforms for Bluetooth device pairing events involving unrecognized peripheral MAC addresses near sensitive locations. For the BootROM exploit, check for USB-based device interactions on A12/A13 devices using endpoint management telemetry; the 'usbliter8' PoC requires physical USB access, so USB connection logs are the primary indicator. Review AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting) controls to confirm Bluetooth and USB events are being captured. Reference CIS 8.2 (Collect Audit Logs) to verify logging is enabled across managed mobile assets.
3. Step 3: Eradication. For CVE-2025-20701/20700/20702 (Airoha SDK/Beats): apply available Apple firmware updates to Beats Studio Buds per the Apple Security Advisory (support.apple.com/en-us/100100). Jabra users should confirm December 2025 patch deployment. Cross-reference patch availability and version numbers against NVD records for CVE-2025-20702 (nvd.nist.gov/vuln/detail/cve-2025-20702). For the BootROM vulnerability: no software patch exists. Eradication for affected A12/A13 devices requires hardware controls; enforce physical device custody policies, disable USB access where possible via MDM configuration profiles, and evaluate device replacement for roles requiring high-assurance security (consistent with NIST AC-6, Least Privilege).

4. Step 4: Recovery. After applying Beats and Jabra firmware updates, re-pair devices and verify firmware version strings match vendor-published patched versions. Monitor Bluetooth pairing activity for 14 days post-patch to detect any anomalous re-pairing attempts. For A12/A13 devices, validate that MDM enrollment and configuration profiles enforcing USB restrictions are active and reporting compliance. Review NIST AU-9 (Protection of Audit Information) to ensure audit logs from this investigation period are preserved and tamper-protected. Confirm CIS 7.3 (Automated Operating System Patch Management) processes have updated all eligible Apple devices to the latest iOS/iPadOS release.

5. Step 5: Post-Incident. Conduct a Bluetooth peripheral inventory audit; many organizations do not track consumer audio devices as managed assets despite their proximity to sensitive conversations. This exposure maps to a gap in CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), which should be extended to include Bluetooth peripherals and IoT-class devices in sensitive environments. Evaluate whether A12/A13 devices in privileged or high-sensitivity roles should be replaced with A14 or later hardware as part of the next device refresh cycle. Review mobile device policy (NIST AC-6) to include explicit controls on Bluetooth peripheral authorization in secure areas. Document the BootROM unpatchability as a hardware risk exception requiring compensating controls, consistent with a risk acceptance process under NIST AC-6 and your GRC framework.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal counsel if any forensic evidence suggests a Beats Studio Buds CVE-2025-20701 microphone access event or 'usbliter8' USB interaction occurred in proximity to a sensitive conversation or on a device with access to PII, PHI, or regulated data, as this may trigger breach notification obligations under HIPAA, GDPR, or applicable state privacy law.
Recovery Notes	Recovery for the Airoha Bluetooth flaw (CVE-2025-20701/20700/20702) is confirmed when all Beats Studio Buds and Jabra devices report patched firmware versions matching Apple and Jabra vendor advisories, and 14 days of post-patch Bluetooth pairing monitoring shows no anomalous Airoha-class peripheral connections near sensitive areas. For A12/A13 BootROM vulnerability recovery, there is no patch-based resolution — recovery is defined as MDM-enforced USB Restricted Mode active and reporting compliance on 100% of in-scope devices, with hardware risk exceptions formally documented and accepted. Sustain monitoring indefinitely for A12/A13 devices in privileged roles, as the BootROM flaw remains exploitable for the hardware lifetime and any future physical access incident reopens the attack surface.

Forensic Artifacts	iOS Bluetooth pairing database at /private/var/mobile/Library/Preferences/com.apple.MobileBluetooth.devices.plist — records all historical pairing attempts including incomplete and rejected pairings, which is the primary artifact for CVE-2025-20701's pre-pairing microphone access vector on Beats Studio Buds | usbmuxd connection log on macOS management hosts ('log show --predicate "process == \"usbmuxd\"") — captures USB device serial numbers and connection timestamps that would evidence a 'usbliter8' BootROM exploit attempt against A12/A13 devices connected to a management machine | MDM Bluetooth pairing event telemetry — peripheral MAC address records from Jamf, Intune, or Apple Configurator showing unrecognized Airoha OUI devices (Airoha Technology Corp MAC prefixes) paired or connection-attempted near sensitive facility locations during the incident window | Beats Studio Buds firmware version string captured via the Beats iOS/Android companion app device settings screen — pre- and post-patch version strings establish whether CVE-2025-20701/20700/20702 were present during any suspected eavesdropping window | Apple Configurator 2 or Xcode Organizer device connection history on IT admin workstations — records USB-connected iDevice serial numbers and connection timestamps, providing a host-side forensic counterpart to usbmuxd logs for corroborating or ruling out 'usbliter8' physical access attempts on A12/A13 devices

Per-Action IR Details

Step 1: Containment — Identify all Beats Studio Buds and Jabra devices using the Airoha Bluetooth Audio SDK in your environment. Restrict use of Airoha-based audio devices in proximity to sensitive conversations, executive meetings, board rooms, and secure facilities until patch status is confirmed. For A12/A13 devices (iPhone XS, XS Max, XR, 11, 11 Pro, 11 Pro Max, and iPad equivalents) used in high-sensitivity roles, enforce a physical access policy: devices should not be left unattended with untrusted USB access, consistent with NIST AC-19 (Access Control for Mobile Devices).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Choosing a Containment Strategy based on the type of incident; physical access vector and unpatchable BootROM require immediate environmental controls rather than software-only response.

Controls: NIST AC-19 (Access Control for Mobile Devices), NIST AC-3 (Access Enforcement), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Export MDM (e.g., Jamf, Intune) device inventory filtered by model identifiers for iPhone XS/XR/11-series (model strings: iPhone11,x; iPhone12,x) to produce an A12/A13 asset list. For Bluetooth peripheral discovery without enterprise tooling, run 'bluetoothctl devices' on Linux or 'system_profiler SPBluetoothDataType' on macOS in conference room areas to enumerate paired and recently seen Airoha-class peripherals. Post physical signage and email directive banning Beats/Jabra use in boardrooms and SCIFs immediately — no tooling required.

Evidence: Before enforcing USB restriction profiles via MDM (which alters device configuration state), capture: (1) current MDM enrollment and compliance status snapshot for all A12/A13 devices; (2) list of all currently paired Bluetooth peripherals from MDM inventory or device-level 'system_profiler SPBluetoothDataType' output, preserving MAC addresses of any unrecognized Airoha SDK devices; (3) iOS Bluetooth pairing database located at /private/var/mobile/Library/Preferences/com.apple.MobileBluetooth.devices.plist on jailbroken or forensic-image-accessible devices — this records all historical pairings including incomplete or rejected ones relevant to CVE-2025-20701's pre-pairing microphone access vector.

Step 2: Detection — For the Bluetooth flaw, audit Bluetooth pairing logs on managed mobile devices for unexpected connection attempts to Beats or Airoha-SDK devices. Query MDM (Mobile Device Management) platforms for Bluetooth pairing events involving unrecognized peripheral MAC addresses near sensitive locations. For the BootROM exploit, check for USB-based device interactions on A12/A13 devices using endpoint management telemetry; the 'usbliter8' PoC requires physical USB access, so USB connection logs

are the primary indicator. Review AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting) controls to confirm Bluetooth and USB events are being captured. Reference CIS 8.2 (Collect Audit Logs) to verify logging is enabled across managed mobile assets.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Analyzing indicators of compromise across log sources to distinguish benign activity from exploitation attempts; the physical-proximity and USB-only attack vectors narrow the detection surface to location-correlated pairing anomalies and physical access events.

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: For Bluetooth anomaly detection without a SIEM: export MDM Bluetooth pairing event logs to a CSV and use a Python one-liner ('import pandas as pd; df=pd.read_csv("bt_events.csv"); print(df[df["device_name"].str.contains("Beats|Studio|Jabra", case=False, na=False)])') to surface Airoha-related pairing events. For USB BootROM exploit detection on macOS hosts used to manage A12/A13 devices, enable and review system_log with 'log show --predicate "subsystem == \"com.apple.usbd\"" --last 7d' to identify unexpected USB enumeration events. Deploy a Sigma rule matching on USB connection events to iDevices outside approved charging contexts (Sigma category: file_event or process_creation on the management host spawning libimobiledevice or ideviceinfo processes unexpectedly).

Evidence: This is a detection/analysis step that does not itself alter live state, but analysts must preserve evidence before any downstream action: (1) Export raw MDM Bluetooth pairing event logs with timestamps and peripheral MAC addresses before MDM policy changes flush them; (2) On macOS management hosts, collect 'log show --predicate "process == \"usbmuxd\"" --last 30d' output to identify any 'usbliter8'-style USB enumeration sessions targeting A12/A13 devices — usbmuxd handles iPhone USB multiplexing and would reflect BootROM-level USB interactions; (3) Capture Apple Configurator or Xcode Organizer device connection history if present on IT admin machines, as these logs record USB device serial numbers and connection timestamps that would evidence physical BootROM exploit attempts.

Step 3: Eradication — For CVE-2025-20701/20700/20702 (Airoha SDK/Beats): apply available Apple firmware updates to Beats Studio Buds per the Apple Security Advisory (support.apple.com/en-us/100100). Jabra users should confirm December 2025 patch deployment. Cross-reference patch availability and version numbers against NVD records for CVE-2025-20702 (nvd.nist.gov/vuln/detail/cve-2025-20702). For the BootROM vulnerability: no software patch exists. Eradication for affected A12/A13 devices requires hardware controls — enforce physical device custody policies, disable USB access where possible via MDM configuration profiles, and evaluate device replacement for roles requiring high-assurance security (consistent with NIST AC-19 and AC-6, Least Privilege).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Eliminating components of the incident; for the Airoha Bluetooth flaw this means firmware remediation, while the unpatchable A12/A13 BootROM requires acknowledging that software eradication is impossible and substituting hardware lifecycle controls as the eradication equivalent.

Controls: NIST AC-19 (Access Control for Mobile Devices), NIST AC-6 (Least Privilege), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams without enterprise patch management: use Apple Configurator 2 (free, macOS App Store) to push supervised MDM configuration profiles that set 'allowUSBRestrictedMode = false' (enforces USB Restricted Mode) on all A12/A13 devices, blocking the physical USB vector required by 'usbliter8' without requiring a SIEM. For Beats firmware patching at scale, use Jamf Pro's free tier or ABM-enrolled devices with an MDM restriction profile — verify patched firmware version string via MDM hardware inventory query post-update. For Jabra devices, use Jabra Direct (free) to confirm December 2025 patch deployment by checking firmware version against Jabra's published advisory version number.

Evidence: Before pushing MDM configuration profiles (which alter device USB restriction state) and before any device retirement/replacement (which destroys hardware evidence): (1) Capture full MDM hardware inventory snapshot for all A12/A13 devices including current iOS version, supervision status, and USB restriction mode state; (2) If any A12/A13

device is suspected of having been physically accessed with 'usbliter8', acquire a logical or filesystem backup via Cellebrite UFED or open-source idevicebackup2 BEFORE MDM profile changes, as post-exploit persistence mechanisms may exist in the user partition; (3) Document current Beats Studio Buds firmware version strings (retrievable via the Beats app under device settings) before applying firmware updates, to establish a pre-patch baseline for the incident record.

Step 4: Recovery — After applying Beats and Jabra firmware updates, re-pair devices and verify firmware version strings match vendor-published patched versions. Monitor Bluetooth pairing activity for 14 days post-patch to detect any anomalous re-pairing attempts. For A12/A13 devices, validate that MDM enrollment and configuration profiles enforcing USB restrictions are active and reporting compliance. Review NIST AU-9 (Protection of Audit Information) to ensure audit logs from this investigation period are preserved and tamper-protected. Confirm CIS 7.3 (Automated Operating System Patch Management) processes have updated all eligible Apple devices to the latest iOS/iPadOS release.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restoring systems to normal operation and verifying that systems are functioning normally; for a hardware-layer vulnerability with no patch, recovery validation centers on confirming compensating control effectiveness rather than patch verification alone.

Controls: NIST AU-9 (Protection Of Audit Information), NIST AC-19 (Access Control for Mobile Devices), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Without a SIEM for 14-day post-patch Bluetooth monitoring: configure a free osquery schedule on macOS management endpoints with a query on the 'bluetooth_info' or equivalent table to log all Bluetooth pairing events daily ('SELECT * FROM bluetooth_info;') and diff outputs across days to detect new unrecognized Airoha-class peripheral MAC addresses. For MDM compliance verification without an enterprise platform, use Apple Business Manager's free device management reports or run 'ideviceinfo -k ProductVersion' via libimobiledevice on each enrolled device to confirm iOS version and 'ideviceinfo -k HardwareModel' to confirm A12/A13 model scope. Store all 14-day monitoring logs in a write-once location (S3 with Object Lock, or a read-only NFS share) to satisfy AU-9 tamper-protection without a commercial SIEM.

Evidence: Recovery verification must confirm prior evidence preservation is complete before closing the investigation window: (1) Confirm all Bluetooth pairing event logs and MDM compliance snapshots captured during detection and containment phases are archived in a tamper-evident store per NIST AU-9 — these are the forensic baseline for any future litigation or regulatory inquiry; (2) Retain usbmuxd and Apple Configurator connection history logs from the investigation period for a minimum of 90 days to support post-incident analysis of any 'usbliter8' USB access events that surface later; (3) Document final firmware version strings for all Beats Studio Buds and Jabra devices post-patch as a recovery validation artifact — mismatched strings between MDM inventory and vendor advisory are a recovery failure indicator.

Step 5: Post-Incident — Conduct a Bluetooth peripheral inventory audit; many organizations do not track consumer audio devices as managed assets despite their proximity to sensitive conversations. This exposure maps to a gap in CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) extended to peripheral and IoT-class devices. Evaluate whether A12/A13 devices in privileged or high-sensitivity roles should be replaced with A14 or later hardware as part of the next device refresh cycle. Review mobile device policy (NIST AC-19) to include explicit controls on Bluetooth peripheral authorization in secure areas. Document the BootROM unpatchability as a hardware risk exception requiring compensating controls, consistent with a risk acceptance process under NIST AC-6 and your GRC framework.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned, policy updates, and improving future detection; the unpatchable nature of the A12/A13 BootROM flaw and the consumer-device blind spot exposed by CVE-2025-20701 both represent systemic gaps requiring policy and inventory program changes, not just one-time remediation.

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), NIST AC-19 (Access Control for Mobile Devices), NIST AC-6 (Least Privilege), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: To build a Bluetooth peripheral inventory without enterprise tooling: deploy a recurring weekly cron job using 'hcitool scan' (Linux) or 'system_profiler SPBluetoothDataType' (macOS) from a dedicated scanning host in each secure area, outputting discovered peripheral MAC addresses and device names to a CSV. Cross-reference discovered MACs against an IEEE OUI lookup for Airoha Technology Corp (OUI: lookup via 'curl https://api.macvendors.com/') to flag Airoha-SDK devices automatically. Document hardware risk exceptions for A12/A13 BootROM unpatchability using a free GRC template (e.g., NIST SP 800-30 Appendix I risk acceptance form) stored in a version-controlled repository.

Evidence: Post-incident documentation must capture: (1) Final asset inventory of all Airoha-SDK Bluetooth peripherals discovered during the incident, including MAC addresses, locations, and patch status — this becomes the baseline for the new peripheral inventory program; (2) MDM compliance report showing all A12/A13 devices with USB Restricted Mode enforced, serving as evidence of compensating control implementation for the BootROM risk exception; (3) Formal risk acceptance document for A12/A13 BootROM unpatchability signed by the asset owner and CISO, with documented compensating controls, retained as a GRC artifact for the next audit cycle.

Detection Guidance

For CVE-2025-20701 (Airoha Bluetooth bypass): monitor Bluetooth peripheral pairing logs via MDM for unexpected connection attempts from unregistered device MAC addresses. Look for Bluetooth audit events where a device registers a microphone session without a completed pairing handshake. Physical proximity is required, so detections near conference rooms, executive areas, or secure zones carry higher priority. For the BootROM 'usbliter8' exploit: physical USB connection is required for exploitation. Query endpoint management and MDM platforms for USB device connection events on A12/A13 device inventory. Flag any USB connection events on these devices in restricted areas or outside of authorized IT workflows. Behavioral indicators include unexpected device reboots, DFU (Device Firmware Update) mode activation events, or iCloud account de-association following physical device access. No network-based IOCs are expected given the physical-access requirement. For the Bluetooth flaw, affected device firmware versions should be tracked; for the BootROM exploit, physical USB connection events are the primary indicator. Reference NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs) to verify mobile device USB and Bluetooth events are captured in your log pipeline.

Framework Mappings

MITRE-ATTACK

- **T1542** — Pre-OS Boot
- **T1011** — Exfiltration Over Other Network Medium
- **T1542.001** — System Firmware
- **T1200** — Hardware Additions
- **T1557** — Adversary-in-the-Middle
- **T1552.004** — Private Keys
- **T1091** — Replication Through Removable Media
- **T1195** — Supply Chain Compromise
- **T1040** — Network Sniffing

NIST-800-53R5

- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-3** — Access Enforcement
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation
- **AT-2** — Literacy Training and Awareness
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control
- **A03:2021** — Injection

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.1** — Establish an Access Granting Process
- **6.8** — Define and Maintain Role-Based Access Control
- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1542	Pre-OS Boot	Defense-Evasion
T1011	Exfiltration Over Other Network Medium	Exfiltration
T1542.001	System Firmware	Persistence
T1200	Hardware Additions	Initial-Access

Technique ID	Technique Name	Tactic
T1557	Adversary-in-the-Middle	Credential-Access
T1552.004	Private Keys	Credential-Access
T1091	Replication Through Removable Media	Lateral-Movement
T1195	Supply Chain Compromise	Initial-Access
T1040	Network Sniffing	Credential-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/apple-patches-beats-studio-buds-f...	T3
CVE-2025-20702 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2025-20702	T1
Product Security Bulletin 2025 | Airoha Technology	https://www.airoha.com/product-security-bulletin/2025	T3
Keep your stuff up to date (CVE-2025-20700, 20701, 20702) - Reddit	https://www.reddit.com/r/programmingHungary/comments/1n38968/tarts%...	T3
CVE-2025-20701 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2025-20701	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-20701, CVE-2025-20700, CV...	T1
Apple Security Advisory	https://support.apple.com/en-us/100100	T1

Generated 2026-06-19 13:53 UTC by TJS Security Command Center