INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-14 18:52 UTC

Critical Kernel-Level Wi-Fi RCE Vulnerability Reported for Apple Devices (CVE-2026-28819)

CVE VULNERABILITY | CRITICAL

SCC Item ID	SCC-CVE-2026-0183
Type	CVE Vulnerability
CVE ID	CVE-2026-28819
Severity	CRITICAL
EPSS Score	0.0004 (14th percentile)
Affected Products	Apple devices (kernel-level Wi-Fi stack; specific products and versions unconfirmed, source data insufficient)
Discovery Source	Gemini

Executive Summary

A critical remote code execution vulnerability affecting the kernel-level Wi-Fi subsystem of Apple devices has been reported under CVE-2026-28819. If confirmed, an attacker within Wi-Fi range could execute arbitrary code at the highest system privilege level without any user interaction, potentially compromising any Apple device on an adjacent network. Confidence in this CVE is currently LOW, it has not been confirmed in NVD, CISA KEV, or Apple's official security advisories as of this analysis, and organizations should monitor authoritative sources before escalating response posture.

Technical Analysis

CVE-2026-28819 is reported as a critical remote code execution vulnerability in the kernel-level Wi-Fi subsystem of Apple devices. The attack vector is described as adjacent network (Wi-Fi range), requiring no user interaction, with code execution reportedly occurring at kernel privilege level. If accurate, this would represent a zero-click, proximity-based kernel compromise, a severity profile comparable to historical Apple Wi-Fi vulnerabilities such as CVE-2022-22641 (AirPlay) and Ian Beer's Project Zero Wi-Fi research (2021, for historical context on severity profile; not definitive for this unconfirmed CVE). Specific affected product lines (iPhone, iPad, Mac, etc.), OS version ranges, CWE classification, CVSS score, and patch status are all unconfirmed. No EPSS scoring is meaningful at this stage (current EPSS: 0.00045, 13.8th percentile) given the absence of NVD confirmation. The priority score assigned by the discovery system is 0.1/1.0, reflecting the low confidence tier. Source discovery was via Gemini (Google Search-grounded), a secondary source. NVD, CISA KEV, and Apple Security Advisories have not corroborated this CVE at time of analysis. All source URLs provided must be treated as unverified, do not use them as confirmation of CVE validity.

Action Checklist

1. Step 1: Containment, Do not escalate to emergency patching posture. This CVE is LOW confidence and unconfirmed in NVD or Apple advisories. Identify and inventory Apple devices (iPhone, iPad, Mac, Apple TV) on corporate and guest Wi-Fi segments. Document current OS versions for rapid assessment if the CVE is confirmed.
2. Step 2: Detection, Monitor NVD (https://nvd.nist.gov), CISA KEV (https://www.cisa.gov/known-exploited-vulnerabilities-catalog), and Apple Security Updates (https://support.apple.com/en-us/HT201222) for official CVE-2026-28819 publication. Set a watch alert on these sources. No confirmed IOCs, behavioral indicators, or log signatures are available at this time, do not deploy detection rules based on unverified data.
3. Step 3: Eradication, No patch is confirmed available. If Apple releases a security update referencing CVE-2026-28819, prioritize deployment to all managed Apple devices through MDM (e.g., Jamf, Intune). For unmanaged personal devices on corporate Wi-Fi, issue a user advisory to apply any available Apple software updates immediately upon release.
4. Step 4: Recovery, Upon official CVE confirmation and patch release, validate patch deployment across the Apple device inventory. Confirm MDM compliance reports show updated OS versions. Monitor Wi-Fi infrastructure logs for anomalous adjacent-network traffic patterns for 30 days post-patch.
5. Step 5: Post-Incident, This item exposes a gap in CVE triage workflows for low-confidence, pre-confirmation advisories. Review your process for handling CVEs that surface via secondary sources before NVD publication. Ensure MDM coverage of all Apple devices is current so patch deployment timelines are known in advance of future advisories.

IR / Forensic Enrichment

Triage Priority	DEFERRED
Escalation Criteria	Escalate immediately to urgent/immediate posture if any of the following occur: CVE-2026-28819 is published to NVD with a CVSS score of 9.0+, added to CISA KEV indicating active exploitation, or Apple releases an out-of-band Rapid Security Response — or if internal Wi-Fi infrastructure logs show repeated Apple device kernel crashes or unexpected reassociations consistent with Wi-Fi stack exploitation attempts against corporate-segment devices.
Recovery Notes	Upon patch release, validate remediation by cross-referencing MDM compliance reports against the Apple device inventory compiled at Step 1, confirming every device reflects the OS build identified in Apple's CVE-2026-28819 advisory as the fixed version. Maintain 30-day post-patch monitoring of Wi-Fi infrastructure logs for deauth floods, repeated reassociation events from Apple MACs, or kernel panic reports referencing AirPort/Wi-Fi kext — behaviors consistent with continued exploitation attempts against unpatched or patch-failed devices. Document any devices that could not be patched within the remediation window as residual risk items with compensating controls (e.g., VLAN isolation from corporate segments) per NIST IR-4 (Incident Handling).

Forensic Artifacts	Apple device kernel panic files at /Library/Logs/DiagnosticReports/ (macOS) referencing com.apple.driver.AirPort.* kext — a zero-interaction kernel-level Wi-Fi RCE exploit targeting CVE-2026-28819 would likely produce kernel panics or unexpected Wi-Fi stack crashes as exploitation artifacts or failed attempt indicators | Wi-Fi access point association and disassociation event logs showing abnormal disconnect/reconnect cycles for Apple device MACs — adjacency-based Wi-Fi exploitation can cause the target device's Wi-Fi stack to crash and recover, producing a characteristic rapid reassociation pattern in AP logs | Packet capture (pcap) of 802.11 management frames on affected Wi-Fi segments, specifically malformed or oversized probe response, beacon, or action frames directed at Apple device MACs — a kernel Wi-Fi stack vulnerability is typically triggered by malformed frames processed before authentication, making management-frame pcap the primary network-layer forensic artifact | Apple device sysdiagnose bundle output ('sudo sysdiagnose -f /tmp/' on macOS, Settings > Privacy > Analytics on iOS) — these archives contain kernel logs, Wi-Fi diagnostic logs, and crash reporter data that would capture exploit trigger events and any post-exploitation kernel-level activity if collected promptly after a suspected attack | MDM enrollment and compliance logs from Jamf or Intune showing device OS version at time of advisory, patch deployment timestamps, and any devices that checked in post-advisory but failed to receive the update — this documents the organizational exposure window and identifies unpatched devices that remain at risk on Wi-Fi segments

Per-Action IR Details

Step 1: Containment — Do not escalate to emergency patching posture. This CVE is LOW confidence and unconfirmed in NVD or Apple advisories. Identify and inventory Apple devices (iPhone, iPad, Mac, Apple TV) on corporate and guest Wi-Fi segments. Document current OS versions for rapid assessment if the CVE is confirmed.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and asset readiness before an incident is confirmed

Controls: NIST IR-4 (Incident Handling) — preparation sub-phase requires maintaining readiness to respond before confirmation, NIST SI-5 (Security Alerts, Advisories, and Directives) — monitor external sources and stage response posture upon receipt of unconfirmed advisories, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — inventory must capture Apple device type, OS version, and Wi-Fi segment assignment to enable rapid scope assessment if CVE-2026-28819 is confirmed, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — process must include handling of pre-NVD, low-confidence CVE disclosures without triggering premature emergency response

Compensating: For a 2-person team without MDM: run 'arp -a' on Wi-Fi gateway or use 'nmap -O --osscan-guess ' to fingerprint Apple devices by MAC OUI prefix (Apple OUIs: 00:17:F2, 3C:15:C2, A4:C3:F0, etc.). Cross-reference against DHCP lease logs on your router/switch. Export results to a CSV with columns: IP, MAC, hostname, inferred OS. This becomes your CVE-2026-28819 blast-radius list the moment confirmation arrives.

Evidence: Before scoping, capture a timestamped snapshot of Wi-Fi association tables from your access points (e.g., 'show dot11 associations' on Cisco IOS, or AP admin UI export) and DHCP lease logs identifying Apple devices by MAC OUI. This baseline documents which Apple devices were on the network prior to any potential exploitation window, preserving pre-incident state per NIST 800-61r3 §2 asset documentation guidance.

Step 2: Detection — Monitor NVD (https://nvd.nist.gov), CISA KEV (https://www.cisa.gov/known-exploited-vulnerabilities-catalog), and Apple Security Updates (https://support.apple.com/en-us/111900) for official CVE-2026-28819 publication. Set a watch alert on these sources. No confirmed IOCs, behavioral indicators, or log signatures are available at this time — do not deploy detection rules based on unverified data.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Monitoring for indicators and analyzing adverse events; DE.AE-07 integration of CTI into event analysis

Controls: NIST SI-4 (System Monitoring) — monitor network-adjacent traffic on Wi-Fi segments for anomalous beacon/probe frames or unexpected kernel-level crash indicators on Apple devices, pending confirmed IOCs, NIST SI-5 (Security Alerts, Advisories, and Directives) — establish recurring watch process against NVD, CISA KEV, and Apple Security Updates page for CVE-2026-28819 publication, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review Wi-Fi infrastructure logs and Apple device management logs at defined frequency during monitoring window, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — process must include a triage queue for unconfirmed CVEs with defined re-evaluation triggers (NVD publication, KEV addition, Apple advisory)

Compensating: Set up a free RSS/change-detection monitor (e.g., Visualping free tier, or 'curl' cron job diffing https://support.apple.com/en-us/111900 page hash daily) to alert on Apple Security Updates page changes. For Wi-Fi anomaly detection without SIEM: enable WIDS (Wireless Intrusion Detection) on your access points if supported — Ubiquiti UniFi and Cisco Meraki both include free WIDS that alert on deauth floods and adjacent scanning, which are pre-exploitation behaviors consistent with Wi-Fi RCE proximity attacks. Log alerts to syslog.

Evidence: Because CVE-2026-28819 targets the kernel-level Wi-Fi subsystem and requires no user interaction, pre-confirmation evidence to preserve includes: (1) Apple device crash reports — on macOS, collect '/Library/Logs/DiagnosticReports/' and '~/Library/Logs/DiagnosticReports/' for kernel panic (.panic) files referencing Wi-Fi kext (com.apple.driver.AirPort.*); (2) Wi-Fi access point association event logs showing unexpected disconnections or re-associations from Apple device MACs; (3) pcap of Wi-Fi management frames on affected segments captured via tcpdump or Wireshark on a monitor-mode adapter, preserving pre-exploitation network baseline.

Step 3: Eradication — No patch is confirmed available. If Apple releases a security update referencing CVE-2026-28819, prioritize deployment to all managed Apple devices through MDM (e.g., Jamf, Intune). For unmanaged personal devices on corporate Wi-Fi, issue a user advisory to apply any available Apple software updates immediately upon release.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Removing the vulnerability from the environment; RS.MA-01 execution of IR plan upon confirmation

Controls: NIST SI-2 (Flaw Remediation) — upon Apple advisory publication referencing CVE-2026-28819, apply vendor-supplied patch through MDM; track remediation per SI-2(a) identify, report, and correct system flaws, NIST CM-3 (Configuration Change Control) — patch deployment to Apple devices via Jamf or Intune constitutes a controlled configuration change requiring documented approval and verification, CIS 7.3 (Perform Automated Operating System Patch Management) — deploy Apple OS update via MDM automated update policy targeting all enrolled iOS, iPadOS, macOS, and tvOS devices, CIS 7.4 (Perform Automated Application Patch Management) — applies to managed Apple devices where the OS update also delivers Wi-Fi stack fixes bundled as system software

Compensating: For teams without Jamf/Intune: use Apple Configurator 2 (free, Mac App Store) to push supervised update commands to tethered iOS/iPadOS devices. For unmanaged Macs: deploy a signed shell script via SSH that runs 'softwareupdate --install --all --restart' and logs output to a central file share. For unmanaged personal devices on corporate Wi-Fi: push a network-level advisory via your captive portal or RADIUS-connected guest SSID notification. Until patch is available, consider isolating the guest SSID from corporate segments at the VLAN level as a compensating control for the zero-interaction adjacency attack surface.

Evidence: Before deploying the patch, capture forensic evidence that documents pre-patch device state: (1) On managed Macs, collect 'system_profiler SPSoftwareDataType SPNetworkDataType' output to document Wi-Fi driver version and OS build; (2) From Jamf or Intune, export device compliance report showing pre-patch OS versions for all Apple devices — this establishes the remediation baseline and documents exposure window duration; (3) Preserve any Apple device sysdiagnose bundles ('sudo sysdiagnose -f /tmp/') from devices suspected of prior anomalous Wi-Fi behavior, as these include kernel logs, crash reports, and Wi-Fi diagnostics that would contain post-exploitation artifacts if the vulnerability was triggered before patching.

Step 4: Recovery — Upon official CVE confirmation and patch release, validate patch deployment across the Apple device inventory. Confirm MDM compliance reports show updated OS versions. Monitor Wi-Fi infrastructure logs for anomalous adjacent-network traffic patterns for 30 days post-patch.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restoring systems to normal operation; verify integrity and monitor for recurrence post-patch

Controls: NIST SI-2 (Flaw Remediation) — verify patch deployment completeness per SI-2(b): test software updates for effectiveness; confirm all Apple devices in inventory reflect OS version containing CVE-2026-28819 fix, NIST CA-7 (Continuous Monitoring) — maintain 30-day post-patch monitoring of Wi-Fi segments for anomalous traffic patterns consistent with adjacency-based exploitation attempts against remaining unpatched devices, NIST IR-5 (Incident Monitoring) — track and document patch deployment status per device, noting any devices that remain unpatched and their exposure status on Wi-Fi segments, CIS 7.2 (Establish and Maintain a Remediation Process) — validate remediation completion against the Apple device inventory compiled in Step 1; document residual risk for any devices that cannot be patched

Compensating: Without SIEM: use osquery on managed Macs ('SELECT * FROM os_version;' via scheduled osquery pack) to confirm OS build number matches Apple's patched release. For Wi-Fi monitoring without network detection tooling: configure your access point syslog to forward to a free Graylog or ELK stack instance, then manually review for repeated deauth events, probe request floods, or unexpected kernel extension crash reports from Apple device MACs. Flag any Apple device MAC that appears in AP logs as 'reassociated' more than 3 times in a 5-minute window — consistent with a Wi-Fi stack crash/recovery cycle that could indicate exploit attempts against unpatched devices.

Evidence: Post-patch evidence to collect and retain: (1) MDM compliance report export (Jamf 'Device Management' report or Intune 'Device Compliance' export) timestamped at patch deployment completion, showing all Apple devices at patched OS build — this is your remediation proof of record; (2) Wi-Fi access point association logs for the 30-day monitoring window, preserved to detect post-patch exploitation attempts against any devices that missed the update; (3) Any Apple device kernel panic logs generated during the 30-day window referencing AirPort or Wi-Fi kext crashes, which would indicate continued exploitation attempts or patch failure on specific hardware.

Step 5: Post-Incident — This item exposes a gap in CVE triage workflows for low-confidence, pre-confirmation advisories. Review your process for handling CVEs that surface via secondary sources before NVD publication. Ensure MDM coverage of all Apple devices is current so patch deployment timelines are known in advance of future advisories.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned, process improvement, and capability update following handling of the advisory

Controls: NIST IR-4 (Incident Handling) — update incident handling procedures to include a triage lane for pre-NVD, low-confidence CVEs with defined criteria for escalation (e.g., kernel-level + zero-interaction + adjacency = elevated watch regardless of NVD status), NIST IR-8 (Incident Response Plan) — update IR plan to include decision criteria for Wi-Fi-adjacent, zero-interaction RCE class vulnerabilities on Apple platforms, reflecting lessons from CVE-2026-28819 handling, NIST SI-2 (Flaw Remediation) — update flaw remediation process to document MDM enrollment coverage gaps identified during Step 1 inventory, and set a target enrollment percentage for Apple devices prior to next advisory, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — revise vulnerability management process documentation to include a pre-NVD advisory triage procedure, specifying source authority thresholds (e.g., Apple PSIRT, CISA pre-publication notice) that warrant action before NVD confirmation, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — close the inventory gap exposed by this advisory: ensure Apple device inventory is maintained with OS version, MDM enrollment status, and Wi-Fi segment assignment updated at least monthly

Compensating: For teams without a formal vulnerability management platform: create a lightweight CVE watch register in a shared spreadsheet with columns: CVE ID, source, confidence level, affected product, NVD status, CISA KEV status, Apple advisory status, and review date. Set a calendar reminder to review open low-confidence items weekly. For MDM coverage gaps: audit Apple device enrollment using 'profiles status -type enrollment' on macOS endpoints and document any unmanaged devices by segment — this becomes your compensating control gap register

for future adjacent-network RCE advisories.

Evidence: Post-incident documentation to retain as institutional record: (1) The full Apple device inventory compiled in Step 1 with OS versions as of advisory receipt date — this documents the exposure window and informs future preparedness metrics; (2) Timeline log of NVD, CISA KEV, and Apple advisory monitoring actions taken from advisory receipt through patch confirmation, demonstrating due diligence per NIST IR-5 (Incident Monitoring); (3) Written lessons-learned memo documenting the gap between secondary-source CVE disclosure and NVD confirmation for CVE-2026-28819, with recommended process changes — this feeds the IR-8 (Incident Response Plan) update cycle.

Detection Guidance

No confirmed IOCs, MITRE technique mappings, or behavioral indicators exist for CVE-2026-28819 at this time, fabricating detection rules from unconfirmed data would introduce noise and false confidence. For preparedness: review Wi-Fi infrastructure logs for unexpected adjacent-network probe or association anomalies. On managed Apple devices, enable and review system crash logs (via MDM or Console.app) for kernel panics in Wi-Fi driver components (e.g., IO80211Family, wlan). If this CVE is confirmed, CISA and Apple advisories will publish specific indicators. Subscribe to Apple Product Security notifications at productSecurity@apple.com and monitor CISA Known Exploited Vulnerabilities catalog for KEV addition.

Framework Mappings

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

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

Sources

Source	URL	Tier
CVE-2026-28819 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-28819	T1
CVE Record: CVE-2026-28819	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2026-28819	T3
CVE-2026-22819 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-22819	T1
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
CVE-2026-20819 - OSV - Open Source Vulnerabilities	https://osv.dev/vulnerability/CVE-2026-20819	T3

Source	URL	Tier
Apple Security Advisory	https://support.apple.com/en-us/100100	**T1**

Generated 2026-05-14 18:52 UTC by TJS Security Command Center