INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-25 18:38 UTC

Apple Patches iOS/iPadOS Flaw Enabling Recovery of Deleted Signal Messages (CVE-2026-28950)

CVE VULNERABILITY | **MEDIUM** | CVSS 5.5

SCC Item ID	SCC-CVE-2026-0078
Type	CVE Vulnerability
CVE ID	CVE-2026-28950
Severity	MEDIUM
CVSS Base Score	5.5
EPSS Score	0.0001 (2th percentile)
Affected Products	Apple iOS and iPadOS (specific versions not confirmed from available data)
Published	2026-04-23
Discovery Source	Gemini

Executive Summary

Apple released an emergency out-of-band patch for CVE-2026-28950, a flaw in iOS and iPadOS that allowed deleted Signal messages to be recovered from notification or cache data that persisted after deletion. According to security reporting, law enforcement has used forensic access to retrieve Signal messages from devices, demonstrating an operational capability. Organizations and individuals relying on Signal for confidential communications, legal, M&A, executive, or regulated discussions should treat unpatched iOS and iPadOS devices as at-risk for those conversations until updated. Specific affected version ranges should be confirmed at https://support.apple.com/en-us/100100.

Technical Analysis

CVE-2026-28950 is classified under CWE-212 (Improper Removal of Sensitive Information Before Storage or Transfer). The flaw exists in iOS and iPadOS's handling of notification payloads and ephemeral storage: when Signal messages are deleted by the user, residual data associated with those messages - likely notification content, preview text, or cached payloads - persisted in accessible system storage. This residual data was recoverable via forensic methods without requiring the Signal application itself to be unlocked. MITRE ATT&CK techniques T1432 (Access Stored Application Data) and T1005 (Data from Local System) map to the exploitation pattern. Apple issued an out-of-band emergency patch, indicating elevated internal severity

assessment. CVSS base score 5.5 and qualitative rating (medium) are from NVD/vendor sources; full scoring details should be confirmed directly at https://nvd.nist.gov/vuln/detail/CVE-2026-28950 and https://www.tenable.com/cve/CVE-2026-28950. EPSS score of 0.00013 (0.013%) places this in the 1.95th percentile, indicating low likelihood of mass exploitation, consistent with targeted forensic use rather than opportunistic attack. Not listed on the CISA KEV catalog as of analysis date. **CRITICAL GAP: Specific affected iOS and iPadOS version ranges are not confirmed from available sources.** Cross-reference https://nvd.nist.gov/vuln/detail/CVE-2026-28950 and https://support.apple.com/en-us/100100 to identify your device version and confirm whether an update is required.

Action Checklist

1. Step 1: Containment. Identify all iOS and iPadOS devices in your environment, particularly those used by executives, legal counsel, or personnel conducting sensitive communications over Signal. Treat unpatched devices as having potential residual message exposure. Restrict use of Signal on unpatched devices for sensitive discussions until the patch is confirmed applied.
2. Step 2: Detection. There are no network-based indicators of compromise (IOCs) for this vulnerability; exploitation requires physical or forensic device access, not remote attack. Focus detection on fleet patch compliance rather than intrusion signals. Assess whether any organizational devices have been seized, accessed, or were out of possession. Review MDM enrollment logs for device compliance status. Check Apple MDM or endpoint management consoles for OS version reporting to identify unpatched devices fleet-wide.
3. Step 3: Eradication. Apply Apple's out-of-band security update for CVE-2026-28950 to all iOS and iPadOS devices. Confirm the update closes this specific CVE by cross-referencing Apple's security advisory at https://support.apple.com/en-us/100100. Push updates via MDM where possible; for unmanaged devices, require user self-update and verify compliance. Organizations typically target completion within 48-72 hours for critical OS patches, adjusted for MDM rollout capacity.
4. Step 4: Recovery. After patching, verify iOS and iPadOS version numbers confirm the fix is applied across all enrolled devices via MDM reporting. For devices that were unmanaged or potentially exposed, consider whether sensitive Signal conversations conducted prior to patching should be treated as potentially accessible. Monitor Apple's security advisory page for any supplemental guidance or version corrections.
5. Step 5: Post-Incident. Evaluate your policy for ephemeral and end-to-end encrypted communication tools on managed devices. Consider whether MDM policies enforce minimum OS versions as a baseline control. Review whether sensitive communications on personal or BYOD devices create organizational risk - this vulnerability demonstrates that OS-level data retention can undermine application-level deletion guarantees. Update acceptable use and device management policies accordingly.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to legal counsel and executive leadership if any iOS/iPadOS device used for legally privileged communications (attorney-client, M&A negotiations, regulated discussions under HIPAA, SOX, or financial regulations) was out of organizational custody during the CVE-2026-28950 exposure window, as confirmed law enforcement exploitation of this vulnerability creates potential breach notification obligations and evidentiary risk.
Recovery Notes	Patching remediates the vulnerability in the OS but does NOT purge Signal notification or cache data that persisted on devices during the exposure window — treat any unpatched device with a custody gap as having potentially accessible message content until a forensic review confirms otherwise. Monitor MDM compliance for OS version drift for a minimum of 60 days post-patch, as factory resets, device replacements, and new enrollments can reintroduce vulnerable OS versions. If your organization operates under regulatory frameworks requiring data confidentiality (HIPAA, SOX, attorney-client privilege), consult legal counsel before closing the incident to assess whether the exposure window triggers notification or disclosure obligations.
Forensic Artifacts	Signal SQLite notification database on iOS at /var/mobile/Containers/Shared/AppGroup/[Signal-UUID]/grdb/signal.sqlite — this is the specific artifact CVE-2026-28950 exposed; contains message content that persisted after user deletion due to the OS-level cache retention flaw | iOS notification cache store at /var/mobile/Library/UserNotifications/ — Signal push notification payloads containing message previews may persist here beyond application-level deletion, which is the core mechanism of CVE-2026-28950 | Apple MDM device check-in logs showing UDID, last enrollment timestamp, OS version reported, and any unenrollment or re-enrollment events — the primary detection artifact given that exploitation requires physical access and leaves no network IOCs | iOS crash logs and system diagnostic archives (retrievable via Settings > Privacy & Security > Analytics & Improvements > Analytics Data) — forensic extraction tools used on the device may generate process anomalies or crash logs if extraction encountered errors during Signal database access | Apple Business Manager device assignment and activation history — records device transfers, re-activations, and MDM re-enrollments that could indicate a device was wiped and re-configured after an extraction attempt, which would otherwise erase the Signal SQLite artifact

Per-Action IR Details

Step 1: Containment — Identify all iOS and iPadOS devices in your environment, particularly those used by executives, legal counsel, or personnel conducting sensitive communications over Signal. Treat unpatched devices as having potential residual message exposure. Restrict use of Signal on unpatched devices for sensitive discussions until the patch is confirmed applied.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected assets and limit further exposure before eradication is possible

Controls: NIST IR-4 (Incident Handling) — implement containment actions consistent with the incident response plan, NIST AC-2 (Account Management) — identify accounts and roles with access to sensitive communications on unpatched devices, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — enumerate all iOS/iPadOS devices, tagging high-risk users (executives, legal, M&A) as priority scope, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — ensure privileged and sensitive-role users are flagged in the asset inventory for prioritized patching

Compensating: If MDM is unavailable, distribute a self-attestation form to all executive, legal, and M&A personnel requiring them to report iOS version within 4 hours. Cross-reference Apple's published vulnerable version range for CVE-2026-28950 against self-reported versions. For the duration of containment, redirect sensitive communications to an alternative channel confirmed not to use iOS notification or cache persistence (e.g., a managed desktop Signal

client or encrypted email with S/MIME). A 2-person team can run this via a shared spreadsheet and a brief all-hands Slack/Teams message to affected user groups.

Evidence: Before restricting device use, document the current iOS/iPadOS version on each device (Settings > General > About > Software Version) and photograph or screenshot the Signal app version (Signal Settings > Privacy > Advanced). Capture MDM device compliance reports as a timestamped export showing OS version per device UDID. This establishes a pre-containment baseline proving which devices were unpatched at time of discovery — critical if regulatory notification or litigation follows.

Step 2: Detection — There are no network-based IOCs for this vulnerability; exploitation is forensic and requires physical device access. Assess whether any organizational devices have been seized, accessed, or were out of possession. Review MDM enrollment logs for device compliance status. Check Apple MDM or endpoint management consoles for OS version reporting to identify unpatched devices fleet-wide.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: analyze available evidence to understand scope; note that CVE-2026-28950 exploitation leaves no network telemetry — analysis must pivot to physical custody and MDM compliance records

Controls: NIST IR-5 (Incident Monitoring) — track and document device custody status and MDM compliance findings as incident records, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review MDM enrollment and check-in logs to identify devices that have not reported compliance or have been offline, NIST SI-4 (System Monitoring) — assess monitoring gaps: CVE-2026-28950 is not detectable via network monitoring; detection depends entirely on device management telemetry, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — use inventory to identify unmanaged or BYOD iOS devices outside MDM visibility that carried sensitive Signal communications

Compensating: Without MDM, run a manual custody audit: email or message all personnel in sensitive roles asking three questions — (1) Has your device left your physical possession in the past 90 days? (2) Was it returned without explanation of where it had been? (3) Has it been connected to an unknown computer or charger? For managed Apple devices enrolled in Apple Business Manager, export device list via the ABM portal (appleid.apple.com/business) and filter on OS version. For unmanaged devices, use a free iOS profile (Apple Configurator 2, available free on macOS App Store) to query device OS version over USB without enrolling the device in MDM.

Evidence: CVE-2026-28950 exploitation requires physical device access — the primary detection artifact is chain-of-custody records, not log files. Collect: (1) MDM last-check-in timestamps per device UDID to identify devices that went offline or unenrolled unexpectedly; (2) Apple Business Manager device assignment history showing any re-enrollment or device transfer events; (3) iCloud account activity logs (if accessible via organizational Apple ID management) for unexpected device sign-ins; (4) Signal's local notification database on iOS, located at /var/mobile/Containers/Shared/AppGroup/[Signal-UUID]/grdb/signal.sqlite, which is the specific artifact CVE-2026-28950 allowed recovery from — document its existence on unpatched devices before patching to understand exposure scope.

Step 3: Eradication — Apply Apple's out-of-band security update for CVE-2026-28950 to all iOS and iPadOS devices. Confirm the update closes this specific CVE by cross-referencing Apple's security advisory at https://support.apple.com/en-us/100100. Push updates via MDM where possible; for unmanaged devices, require user self-update and verify compliance.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the vulnerability from all affected systems; for CVE-2026-28950 this means eliminating the iOS/iPadOS flaw that permitted Signal notification and cache data to persist post-deletion

Controls: NIST SI-2 (Flaw Remediation) — apply Apple's out-of-band patch for CVE-2026-28950; test update deployment in a non-production device subset before fleet-wide push if MDM allows staged rollout, NIST CM-6 (Configuration Settings) — enforce minimum iOS/iPadOS version as a configuration baseline in MDM compliance policy post-patch, CIS 7.3 (Perform Automated Operating System Patch Management) — use MDM (Jamf, Intune, Apple MDM protocol) to push the CVE-2026-28950 patch to all enrolled iOS/iPadOS devices; set non-compliance action to restrict network access for devices still running vulnerable versions, CIS 7.4 (Perform Automated Application

Patch Management) — verify Signal app is also updated to the latest version post-OS patch, as Signal may release a companion update addressing cache handling behavior on its side

Compensating: For teams without enterprise MDM, use Apple Configurator 2 (free, macOS) to sideload the iOS update to devices via USB in supervised mode, or instruct users to update via Settings > General > Software Update and confirm the resulting build number matches Apple's advisory for CVE-2026-28950. Create a shared tracking spreadsheet where users paste their Settings > General > About > iOS Version screenshot. For BYOD devices, issue a written directive under your acceptable use policy requiring update within 24 hours and collect signed acknowledgment — this creates a compliance record if the device is later identified in an investigation.

Evidence: Before pushing the patch, capture a fleet-wide MDM compliance report as a timestamped CSV export showing per-device UDID, OS version, and last check-in time — this is your pre-eradication baseline. After patching, capture a second export and diff the two to confirm all previously vulnerable devices have been remediated. Retain both exports as incident documentation per NIST IR-5 (Incident Monitoring). Note: the patch itself does not retroactively purge Signal cache data that persisted under the vulnerability — devices that were unpatched during a custody gap may still contain recoverable messages in the SQLite notification store prior to the update.

Step 4: Recovery — After patching, verify iOS and iPadOS version numbers confirm the fix is applied across all enrolled devices via MDM reporting. For devices that were unmanaged or potentially exposed, consider whether sensitive Signal conversations conducted prior to patching should be treated as potentially accessible. Monitor Apple's security advisory page for any supplemental guidance or version corrections.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operation with verified integrity; for CVE-2026-28950, recovery includes confirming patch application and assessing the confidentiality impact of messages that persisted in Signal's notification or cache store during the exposure window

Controls: NIST IR-4 (Incident Handling) — document recovery actions and verify that patched devices are confirmed remediated before resuming sensitive Signal communications, NIST SI-7 (Software, Firmware, and Information Integrity) — verify iOS build numbers post-patch against Apple's published fixed versions for CVE-2026-28950 to confirm integrity of the update deployment, NIST CA-7 (Continuous Monitoring) — establish ongoing MDM compliance monitoring for iOS version drift post-recovery; alert on any device falling below the patched version threshold, CIS 7.2 (Establish and Maintain a Remediation Process) — document closure of CVE-2026-28950 remediation with verified compliance percentages and record any devices that required manual intervention

Compensating: Without a SIEM, set a recurring weekly MDM compliance report (or manual ABM export) for 60 days post-patch to catch any newly enrolled or factory-reset devices that rejoin the fleet at a vulnerable OS version. For devices where custody was uncertain, conduct a structured conversation with the device owner using a 5-question custody checklist (last known location, connection to unknown systems, unexpected reboots, unfamiliar profiles under Settings > General > VPN & Device Management, and any unusual battery drain consistent with forensic extraction activity). Document responses and retain for 90 days.

Evidence: Post-recovery evidence to retain: (1) Final MDM compliance report showing 100% of enrolled devices at or above the patched iOS/iPadOS version, with UDID-level detail; (2) A list of devices that were identified as unmanaged or BYOD during the incident, with the owner, device model, and whether patch compliance was self-attested or verified; (3) Apple security advisory page content for CVE-2026-28950 archived at time of closure (screenshot or PDF) — advisory pages can be updated or retracted, and your closure record should capture the exact fixed version cited at time of remediation.

Step 5: Post-Incident — Evaluate your policy for ephemeral and end-to-end encrypted communication tools on managed devices. Consider whether MDM policies enforce minimum OS versions as a baseline control. Review whether sensitive communications on personal or BYOD devices create organizational risk — this vulnerability demonstrates that OS-level data retention can undermine application-level deletion guarantees. Update acceptable use and device management policies accordingly.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons learned and update policies, procedures, and detection capabilities to prevent recurrence; CVE-2026-28950 reveals a structural gap between application-layer

deletion and OS-layer data persistence that policy must address

Controls: NIST IR-8 (Incident Response Plan) — update the IR plan to include ephemeral messaging platforms (Signal, WhatsApp, iMessage) as in-scope assets for future incident response, with specific containment and evidence-handling procedures, NIST SI-12 (Information Management and Retention) — update data retention policy to explicitly address OS-level notification cache and app data persistence, which CVE-2026-28950 demonstrated can survive application-level deletion, NIST CM-6 (Configuration Settings) — codify minimum iOS/iPadOS version enforcement as a mandatory MDM compliance policy baseline, with automated non-compliance remediation (quarantine or access restriction), CIS 4.6 (Securely Manage Enterprise Assets and Software) — update MDM configuration baselines to include OS version minimums and Signal app version requirements as enforced compliance rules, not advisory guidelines, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — update the vulnerability management process to include Apple security advisories as a monitored feed, with a defined SLA for out-of-band patches affecting communication confidentiality

Compensating: For teams without formal GRC tooling, produce a one-page policy addendum to the existing acceptable use policy that: (1) prohibits use of Signal for legally privileged, M&A, or regulated discussions on any iOS/iPadOS device not enrolled in MDM and confirmed at current OS version; (2) requires immediate self-report if a device used for sensitive Signal communications leaves organizational custody; (3) establishes a 48-hour patch deadline for out-of-band Apple security updates rated MEDIUM or above that affect communication confidentiality. Store signed acknowledgments in a shared drive folder as your compliance record. This is achievable by a 2-person team in under a day.

Evidence: Post-incident artifacts to retain for lessons learned: (1) The full device inventory with patch compliance timeline showing days-to-remediation per device — this benchmarks your response against NIST SI-2 (Flaw Remediation) requirements; (2) Custody audit responses from sensitive-role personnel, retained for 1 year in case of future legal discovery; (3) A written lessons-learned memo documenting the gap CVE-2026-28950 exposed — specifically that Signal's disappearing message feature and manual deletion do not guarantee data removal at the iOS notification/cache layer — this memo should drive the policy updates above and be reviewed at the next IR tabletop.

Detection Guidance

This vulnerability does not produce network-based indicators of compromise (IOCs); exploitation requires physical or forensic access to the device. Detection focus should be on fleet patch compliance rather than intrusion signals. Query your MDM platform (Jamf, Intune, or equivalent) for all iOS and iPadOS devices reporting OS versions below the patched release. Flag any devices that are unmanaged, unenrolled, or overdue on OS updates. If a device seizure or unauthorized physical access event is known or suspected, treat any Signal communications from that device prior to patching as potentially accessible. Consult https://nvd.nist.gov/vuln/detail/CVE-2026-28950 and https://support.apple.com/en-us/100100 for the specific patched versions and affected version ranges.

Framework Mappings

MITRE-ATTACK

- **T1432**
- **T1005** — Data from Local System

NIST-800-53R5

- **SI-2** — Flaw Remediation

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1432		
T1005	Data from Local System	Collection

Sources

Source	URL	Tier
CVE-2026-28950 Details - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-28950	T1
CVE-2026-28950: Apple Fixes iOS Data Retention Flaw	https://socprime.com/blog/cve-2026-28950-detection/	T3
CVE-2026-28950	https://www.tenable.com/cve/CVE-2026-28950	T3
Apple fixes iPhone bug that let FBI retrieve deleted Signal ...	https://www.helpnetsecurity.com/2026/04/23/cve-2026-28950-iphone-vu...	T3
Apple's security notice for the update, titled CVE	https://www.facebook.com/PCMag/posts/apples-security-notice-for-the...	T3
Apple Security Advisory	https://support.apple.com/en-us/100100	T1

Generated 2026-04-25 18:38 UTC by TJS Security Command Center