INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-03 06:52 UTC

Android Framework Integer Overflow Enables Local Privilege Escalation (CVE-2025-48595)

CVE VULNERABILITY | HIGH | CVSS 8.4 | CISA KEV

SCC Item ID	SCC-CVE-2026-0257
Type	CVE Vulnerability
CVE ID	CVE-2025-48595
Severity	HIGH
CVSS Base Score	8.4
EPSS Score	0.0001 (0th percentile)
KEV Status	Yes — CISA Known Exploited Vulnerability (due: 2026-06-05)
Affected Products	Android Framework (patched in June 2026 Android Security Bulletin; originally disclosed September 2025 Android Security Bulletin)
Published	2026-06-02
Discovery Source	Cisa Kev

Executive Summary

A high-severity integer overflow vulnerability in the Android Framework (CVE-2025-48595, CVSS 8.4) allows an attacker with local device access to escalate privileges and execute arbitrary code. CISA confirmed active exploitation by adding this CVE to its Known Exploited Vulnerabilities catalog with a remediation deadline of June 5, 2026. Organizations issuing or managing Android devices, including corporate-owned fleets, BYOD programs, and kiosk deployments, face elevated risk from targeted attacks involving physical access or malicious applications.

Technical Analysis

CVE-2025-48595 is an integer overflow (CWE-190) in the Android Framework component, initially disclosed in the September 2025 Android Security Bulletin and patched in the June 2026 Android Security Bulletin. The vulnerability maps to MITRE ATT&CK T1203 (Exploitation for Client Execution) and T1068 (Exploitation for Privilege Escalation). Attack vector is local; exploitation requires the attacker to either have physical access to the device or deliver a malicious application that executes in an unprivileged context. A successful exploit achieves arbitrary code execution at an elevated privilege level within the Android Framework. CVSS base score is 8.4 (high severity); note that this score is sourced from secondary reporting and has not been verified against an official vendor CVSS vector. EPSS score is 0.006% (6e-05), reflecting low automated exploitation

probability at time of scoring; however, CISA KEV status supersedes EPSS as the operative risk signal. The KEV remediation due date is June 5, 2026. Patch is available via the June 2026 Android Security Bulletin. No public IOCs (file hashes, domains, or IP addresses) have been reported at this time.

Action Checklist

1. Step 1: Containment. Immediately audit all corporate-managed and BYOD Android devices enrolled in MDM. Identify devices running Android versions not yet patched to the June 2026 Security Patch Level (SPL: 2026-06-01 or later). Restrict network access for unpatched devices where MDM policy supports quarantine (NIST IR-4, CIS 4.4). Disable sideloading of unsigned applications on managed devices as an interim control (NIST CM-7, AC-3).
2. Step 2: Detection. Review MDM and UEM console telemetry for anomalous privilege escalation events on Android endpoints. Examine Android device logs (via ADB or MDM log collection) for unexpected process spawning from Framework-level services. Look for newly installed applications from unknown sources (CIS 2.3). Check EDR or mobile threat defense (MTD) platforms for T1068 and T1203 technique detections. No public IOCs (file hashes, domains, or IP addresses) have been reported. Detection relies on behavioral indicators: look for unexpected system app crashes followed by new process creation at elevated UID. Review logs per NIST AU-6 (Audit Record Review) and AU-12 (Audit Record Generation).
3. Step 3: Eradication. Apply the June 2026 Android Security Bulletin patch to all affected devices. For OEM-managed devices, push the update via MDM OTA policy targeting a patch level of 2026-06-01 or later. For devices whose OEMs have not yet released the June 2026 patch, enforce compensating controls: disable unknown-source app installation (NIST CM-6), enforce application allowlisting where MDM supports it (CIS 2.3, AC-3), and flag the device as non-compliant in your MDM posture policy (CIS 7.3).
4. Step 4: Recovery. Validate patched devices report SPL 2026-06-01 or later in MDM inventory. Conduct a post-patch audit of all device privilege states and application inventories on previously unpatched endpoints (CIS 1.1, 2.1). Monitor MDM and MTD dashboards for 30 days post-remediation for residual anomalous activity. Re-enable any network access restrictions lifted for remediated devices only after SPL verification is confirmed (NIST AU-6).
5. Step 5: Post-Incident. Review mobile device policy for enforcement of automatic OS updates (CIS 7.3, NIST SI-2). Evaluate whether current MDM policies enforce minimum SPL compliance as a continuous control, not a reactive one. Assess BYOD policy to determine whether personal devices with access to corporate resources require mandatory patch compliance windows. Document this incident in the vulnerability management remediation log (CIS 7.2). If your environment lacks mobile threat defense (MTD) coverage, document this as a capability gap and prioritize MTD acquisition to improve detection coverage for future local privilege escalation attempts.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and legal counsel immediately if MDM telemetry or ADB forensics on any device show evidence of post-exploitation persistence (unexpected packages, anomalous UID processes, or Framework crash events correlated with new application installs), as CVE-2025-48595's CISA KEV confirmed active exploitation status combined with any indicator of successful privilege escalation on a device with access to PII, PHI, or PCI data triggers breach notification assessment obligations under applicable state and federal regulations.
Recovery Notes	After SPL 2026-06-01 is confirmed across the device fleet via MDM inventory export, conduct a package diff audit on all previously unpatched devices — the Android Framework integer overflow could have been leveraged to install a persistent payload prior to patching, and that payload will not be removed by the OS update alone if it achieved system-level persistence. Monitor MDM and MTD dashboards for Framework crash events and anomalous UID escalation activity for a minimum of 30 days post-remediation, with particular focus on devices that were unpatched for the longest duration or that had physical access exposure. Re-evaluate MTD tooling coverage for the BYOD and kiosk segments given that CVE-2025-48595's local-access attack vector means any individual with brief physical access to an unpatched device was a viable threat actor.
Forensic Artifacts	Android logcat crash buffer (`adb logcat -b crash -d -v threadtime`): filter for fatal exceptions in `system_server`, `zygote`, or `android.hardware.*` processes — integer overflow exploitation in Android Framework will typically manifest as a Framework-layer crash immediately preceding unexpected privilege elevation, making this the primary exploitation signal in the absence of public IOCs. | ADB process UID snapshot (`adb shell ps -A` and `adb shell cat /proc/*/status | grep -E 'Name|Uid'`): a successful exploit of CVE-2025-48595 results in a non-system process executing at UID 0 (root) or system UID 1000 — this snapshot captures the anomalous UID assignment that constitutes direct forensic evidence of privilege escalation. | MDM application installation event log with installer field: packages installed via the privilege escalation path will have a null, empty, or non-Play-Store installer record in `adb shell pm list packages -i` output — correlate installation timestamps against Framework crash events in logcat to establish exploitation-to-payload-delivery timeline. | `adb shell dumpsys permission` runtime permission grant history: post-exploitation, an attacker leveraging CVE-2025-48595 may persist by granting a malicious or compromised application dangerous or signature-level permissions that it could not obtain through legitimate Play Store installation — anomalous runtime permission grants to non-system packages are a high-fidelity persistence indicator. | MDM Security Patch Level compliance timeline report: documents the exact window between June 2026 Android Security Bulletin publication and each device's confirmed patching — this artifact establishes the organizational exposure duration per device, required for regulatory breach notification assessment and for identifying which specific devices were at risk during the CISA KEV-confirmed active exploitation period.

Per-Action IR Details

Step 1: Containment — Immediately audit all corporate-managed and BYOD Android devices enrolled in MDM. Identify devices running Android versions not yet patched to the June 2026 Security Patch Level (SPL: 2026-06-01 or later). Restrict network access for unpatched devices where MDM policy supports quarantine (NIST IR-4, CIS 4.4). Disable sideloading of unsigned applications on managed devices as an interim control (NIST CM-7, AC-3).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST AC-3 (Access Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: For teams without enterprise MDM: use ADB in a scripted batch query — `adb shell getprop ro.build.version.security_patch` — across USB-connected devices to extract SPL strings and pipe output to a CSV for triage. Disable Unknown Sources via ADB: `adb shell settings put global install_non_market_apps 0`. For network quarantine without MDM, implement VLAN-based isolation at the Wi-Fi controller or use a RADIUS policy to deny network certificates to devices below minimum SPL.

Evidence: Before quarantining a device, capture the following via ADB or MDM log export: (1) `adb bugreport` full diagnostic archive to preserve the current process table and running UID assignments; (2) `adb shell ps -A` output to document all running processes and their effective UIDs at the moment of containment; (3) MDM device posture snapshot showing current SPL, installed application list with package names and install sources, and last check-in timestamp; (4) `adb shell dumpsys package` to record all installed packages, their declared permissions, and installer origin (com.android.vending vs. sideloaded) before any remediation alters the device state.

Step 2: Detection — Review MDM and UEM console telemetry for anomalous privilege escalation events on Android endpoints. Examine Android device logs (via ADB or MDM log collection) for unexpected process spawning from Framework-level services. Look for newly installed applications from unknown sources (CIS 2.3). Check EDR or mobile threat defense (MTD) platforms for T1068 and T1203 technique detections. No public IOCs are available; behavioral indicators — unexpected system app crashes followed by new process creation at elevated UID — are the primary signal (NIST AU-6, AU-12).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 2.3 (Address Unauthorized Software), CIS 8.2 (Collect Audit Logs)

Compensating: Without MTD or EDR: run `adb logcat -b crash -d` and filter for fatal exceptions originating from `android.os.Binder`, `android.app.ActivityManagerService`, or Framework-layer process names — these crash events immediately preceding unexpected UID changes are the primary behavioral signal for CVE-2025-48595 exploitation. Use `adb shell getprop | grep -i uid` combined with `adb shell dumpsys activity processes` to identify any non-system process executing at UID 0 or system UID 1000. For free-tool MITRE T1068 detection on the network side, capture Wi-Fi traffic with Wireshark and filter for unexpected outbound connections from Android device IPs immediately following Framework crash events in logcat — a successful privilege escalation is likely to be followed by a C2 beacon or data staging attempt.

Evidence: Collect before analysis modifies device state: (1) `adb logcat -b main -b system -b crash -d -v threadtime` full log buffer export — filter specifically for crash entries in `system_server`, `zygote`, or `android.hardware.*` processes, which host the integer overflow-vulnerable Framework code paths; (2) `adb shell dumpsys activity` to capture process ancestry and UID assignments — look for child processes spawned by Framework services with unexpected elevated UIDs inconsistent with their declared manifest permissions; (3) MDM application installation event log filtered for installs occurring within 60 minutes of any Framework crash event, with particular attention to packages installed without a Play Store installer record (installer field = null or unknown); (4) `adb shell dumpsys permission` to capture current runtime permission grants — post-exploitation, a successful privilege escalation may persist through illegitimately granted permissions that survive the crash.

Step 3: Eradication — Apply the June 2026 Android Security Bulletin patch to all affected devices. For OEM-managed devices, push the update via MDM OTA policy targeting a patch level of 2026-06-01 or later. For devices whose OEMs have not yet released the June 2026 patch, enforce compensating controls: disable unknown-source app installation (NIST CM-6), enforce application allowlisting where MDM supports it (CIS 2.3, AC-3), and flag the device as non-compliant in your MDM posture policy (CIS 7.3).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST CM-6 (Configuration Settings), NIST CM-7 (Least Functionality), NIST AC-3 (Access Enforcement), NIST SI-2 (Flaw Remediation), CIS 2.3 (Address Unauthorized Software), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For OEM-delayed patch scenarios: use ADB to enforce unknown-source restriction (`adb shell settings put secure install_non_market_apps 0`) and verify with `adb shell settings get secure install_non_market_apps`. For application allowlisting without MDM, use Android Enterprise Work Profile restrictions via open-source EMM tools (e.g., Headwind MDM, available free for self-hosted deployment) to whitelist only verified package names. Document each device flagged as non-compliant with its OEM model, current Android version, and last vendor security bulletin date — this list becomes your residual risk register for the vulnerability management remediation log required under CIS 7.2.

Evidence: Before applying the OTA patch, capture: (1) full `adb bugreport` as a forensic baseline to preserve pre-patch system state for any post-eradication investigation; (2) `adb shell pm list packages -f -i` to record all installed packages with their APK file paths and installer sources — if exploitation occurred, a malicious payload installed via the privilege escalation will appear here with a null or anomalous installer field; (3) `adb shell cat /proc/*/status | grep -E 'Name|Uid'` snapshot to document all running process UIDs immediately before patching, preserving evidence of any processes operating at unexpected privilege levels that patching would otherwise obscure; (4) MDM OTA policy push logs timestamped to confirm patch deployment initiation, required for audit trail under NIST AU-12 (Audit Record Generation).

Step 4: Recovery — Validate patched devices report SPL 2026-06-01 or later in MDM inventory. Conduct a post-patch audit of all device privilege states and application inventories on previously unpatched endpoints (CIS 1.1, 2.1). Monitor MDM and MTD dashboards for 30 days post-remediation for residual anomalous activity. Re-enable any network access restrictions lifted for remediated devices only after SPL verification is confirmed (NIST AU-6).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without MDM inventory reporting: build a SPL verification spreadsheet using batch ADB queries — script `adb shell getprop ro.build.version.security_patch` across all enrolled devices and compare output against the 2026-06-01 threshold. For post-patch application integrity verification without MTD, run `adb shell pm list packages -f` on each previously unpatched device and diff the output against the pre-eradication baseline captured in Step 3 — any new package present post-patch that was not in the pre-incident authorized software inventory (CIS 2.1) requires immediate investigation as a potential persistence mechanism left by exploitation of CVE-2025-48595 before patching.

Evidence: Collect during and after recovery validation: (1) MDM SPL inventory report exported with device identifiers, model numbers, OEM, and confirmed SPL string `2026-06-01` as the authoritative remediation verification record; (2) `adb shell dumpsys package` post-patch diff against the Step 3 pre-patch baseline — the integer overflow in Android Framework could have been used to install a persistent payload before remediation, and this diff will surface any packages that survived the patch cycle; (3) MDM access control policy enforcement logs confirming that quarantine restrictions were lifted only after SPL verification, not before, preserving the integrity of the containment boundary; (4) 30-day MTD or MDM telemetry export at the end of the monitoring window to document absence of residual Framework crash events or anomalous UID escalation activity as the formal closure record.

Step 5: Post-Incident — Review mobile device policy for enforcement of automatic OS updates (CIS 7.3, NIST SI-2). Evaluate whether current MDM policies enforce minimum SPL compliance as a continuous control, not a reactive one. Assess BYOD policy to determine whether personal devices with access to corporate resources require mandatory patch compliance windows. Document this incident in the vulnerability management remediation log (CIS 7.2). Consider whether MTD tooling coverage is adequate given the local-access attack vector.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST SI-2 (Flaw Remediation), NIST IR-4 (Incident Handling), NIST CM-6 (Configuration Settings), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: For teams without commercial MTD: document a minimum SPL compliance window policy — recommend a 30-day maximum from Android Security Bulletin release to confirmed device patching, modeled on the CISA KEV remediation deadline framework. For BYOD policy enforcement without MDM conditional access, implement network-level controls: configure Wi-Fi RADIUS policy or VPN certificate issuance to require device attestation check-ins proving SPL compliance before granting corporate network access. Add CVE-2025-48595 as a permanent entry in the vulnerability management remediation log with CISA KEV catalog reference and document the OEM patch gap timeline for affected device models as a procurement risk input.

Evidence: Preserve for lessons-learned and regulatory documentation: (1) complete MDM SPL compliance timeline report showing the gap between June 2026 Android Security Bulletin release date and each device's confirmed patch date — this gap document quantifies organizational exposure duration and is required for any regulatory breach notification assessment; (2) BYOD policy document version history showing pre- and post-incident SPL enforcement requirements, demonstrating policy improvement as a direct outcome; (3) MTD coverage gap analysis identifying any Android device models or BYOD segments that had no behavioral monitoring during the exploitation window — given CVE-2025-48595's local-access attack vector, devices with physical access exposure (kiosk, shared-use, contractor) that lacked MTD represent an unmonitored attack surface that must be documented; (4) CISA KEV catalog entry for CVE-2025-48595 preserved as the authoritative record of confirmed active exploitation status, supporting the incident severity classification and any insurance or regulatory reporting obligations.

Detection Guidance

No public IOCs (IP addresses, domains, file hashes) have been reported for CVE-2025-48595 at this time. Detection relies on behavioral and telemetry signals. In MDM or UEM consoles: filter devices by Security Patch Level older than 2026-06-01; these are your confirmed-unpatched population. In mobile threat defense (MTD) platforms: enable detections for T1068 (Privilege Escalation) and T1203 (Exploitation for Client Execution) on Android endpoints. In Android device logs (accessible via ADB shell or MDM log forwarding): look for abnormal UID transitions in process tables, unexpected spawning of system-level processes from non-privileged parent processes, and crash reports originating from Android Framework services followed by process re-execution at elevated privilege. NIST AU-6 (Audit Record Review) and AU-12 (Audit Record Generation) provide the control framework for this log review activity. CIS 8.2 (Collect Audit Logs) should be validated to confirm mobile endpoint log collection is active. If your environment lacks MTD coverage, document this as a detection capability gap. However, patch deployment remains the primary control and should not be delayed pending MTD acquisition.

Framework Mappings

MITRE-ATTACK

- **T1203** — Exploitation for Client Execution
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection

- **SI-4** — System Monitoring
- **AC-6** — Least Privilege
- **SI-16** — Memory Protection
- **IR-5** — Incident Monitoring

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

ISO-27001-2022

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

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1203	Exploitation for Client Execution	Execution
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Sources

Source	URL	Tier
cisa_kev	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
Android Security Bulletin—September 2025	https://source.android.com/docs/security/bulletin/2025-09-01	T3
Google fixes actively exploited Android vulnerability (CVE-2025 ...	https://www.helpnetsecurity.com/2026/06/02/android-vulnerability-ex...	T3
Android just patched 124 security flaws. One of them — CVE-2025 ...	https://www.facebook.com/thehackernews/posts/-android-just-patched-...	T3
June 2026 Android Security Bulletin notes CVE-2025-48595 is ...	https://x.com/GrapheneOS/status/2061860506126684595	T3

Source	URL	Tier
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-48595	T1

Generated 2026-06-03 06:52 UTC by TJS Security Command Center