INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-11 14:25 UTC

Slate Digital Connect macOS Privilege Escalation Vulnerabilities (CVE-2026-24067, CVE-2026-24066)

CVE VULNERABILITY | HIGH | CVSS 8.4

SCC Item ID	SCC-CVE-2026-0294
Type	CVE Vulnerability
CVE ID	CVE-2026-24067, CVE-2026-24066
Severity	HIGH
CVSS Base Score	8.4
EPSS Score	0.0001 (3th percentile)
Affected Products	Slate Digital Connect 1.37.0 for macOS
Published	2026-06-10
Discovery Source	Gemini

Executive Summary

Two local privilege escalation vulnerabilities in Slate Digital Connect 1.37.0 for macOS allow an attacker with existing local access to gain elevated system privileges. The first flaw exploits a race condition in process validation; the second bypasses certificate checks using a self-signed certificate with a matching organizational unit field. Organizations running this audio software on managed macOS endpoints should patch immediately when vendor remediation is available, or disable the privileged helper tool to prevent privilege escalation by a local threat actor.

Technical Analysis

Two local privilege escalation vulnerabilities affect Slate Digital Connect 1.37.0 for macOS. CVE-2026-24067 (CVSS 8.4) is a TOCTOU race condition (CWE-367) in the application's PID-based client validation mechanism. An attacker exploits the window between PID check and PID use to substitute a malicious process and inherit elevated privileges. CVE-2026-24066 (high severity, CWE-295) targets the privileged helper tool's certificate validation logic, which checks only the subject.OU field of a signing certificate. An attacker crafts a self-signed certificate with a matching subject.OU value to impersonate a trusted client and invoke privileged helper operations. Both vulnerabilities map to MITRE ATT&CK T1548.004 (Abuse Elevation Control Mechanism: Elevated Execution with Prompt) and T1574 (Hijack Execution Flow). Both require local access. No CISA KEV

listing. EPSS score is 0.00014 (2.7th percentile), indicating low observed exploitation activity at time of publication. Patch status: Verify vendor advisory from Slate Digital for patch availability and version number. If no patch is available, the recommended mitigation is to disable the privileged helper tool until remediation is released.

Action Checklist

1. Step 1: Containment, Identify all macOS endpoints running Slate Digital Connect 1.37.0 using your asset inventory (CIS 1.1). Restrict local interactive access to those systems until patched, prioritizing shared or multi-user studio workstations where untrusted local users may be present.
2. Step 2: Detection, Query endpoint logs for unexpected privileged helper tool invocations or XPC service connections originating from non-Slate Digital processes. On macOS, review Unified Log entries (log show --predicate) filtering on the Slate Digital Connect bundle identifier and privileged helper tool name. Look for process substitution patterns near PID reuse events (T1548.004, per MITRE ATT&CK). Enable AU-2 event logging for privilege escalation events if not already active (NIST SP 800-53).
3. Step 3: Eradication, Apply the vendor-supplied update for Slate Digital Connect when available. If no patch is yet released, remove or disable the privileged helper tool (typically registered under /Library/LaunchDaemons/) until a fix is confirmed. Verify removal using CIS 2.3 unauthorized software processes. Rotate any credentials accessible to processes running under the escalated context (NIST SP 800-53, IAC-7 Credential Rotation).
4. Step 4: Recovery, After patching or helper tool removal, verify no unauthorized LaunchDaemon or LaunchAgent entries were introduced (NIST SP 800-53, SI-7 System Monitoring). Confirm the updated application's code signature validates correctly against Apple's notarization service. Monitor local privilege events via endpoint detection tooling for 30 days post-remediation, aligned with AU-6 audit record review.
5. Step 5: Post-Incident, Review privileged helper tool deployment policies across all macOS software in the environment. Establish a review process requiring vendor-supplied privileged helpers to implement PID-independent validation and full certificate chain verification before deployment approval. Map identified control gaps to NIST AC-6 (Least Privilege) and AC-3 (Access Enforcement) and schedule a formal review of macOS endpoint privilege management practices.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to incident command and legal/compliance if forensic evidence confirms a non-Slate process successfully communicated with the privileged helper (indicating active exploitation), if any host shows net-new root-owned processes or files introduced during the exposure window, or if affected endpoints store or process regulated data (PII, PHI, financial) that may trigger breach notification obligations under HIPAA, CCPA, or applicable state law.

Recovery Notes	After applying the Slate Digital Connect patch (or removing the helper tool), validate every affected macOS endpoint individually using `spctl` notarization checks and LaunchDaemon inventory diffs against pre-incident baselines — do not rely on MDM compliance status alone, as the race condition (CVE-2026-24067) or certificate bypass (CVE-2026-24066) could have been used to introduce a persistent LaunchDaemon before remediation. Monitor macOS Unified Log entries for `authd`, `securityd`, and XPC connection events referencing any `com.slatedigital.*` identifier for a minimum of 30 days post-patch to detect any re-exploitation attempts or residual backdoor activity. Retain all forensic artifacts from this incident for a minimum of 90 days to support any retrospective analysis if related exploitation activity is later identified.
Forensic Artifacts	macOS Unified Log archive (/var/log/ and collected via `log collect`): Contains XPC connection records, Authorization Services (`authd`) grant/deny decisions, and `securityd` code-signing validation events — the primary log source for detecting both the race condition PID reuse (CVE-2026-24067) and the certificate OU bypass (CVE-2026-24066) exploitation attempts. | /Library/PrivilegedHelperTools/: The privileged helper binary itself — SHA-256 hash and `codesign -dvvv` output should be preserved; a modified or attacker-substituted binary would show a self-signed certificate with a spoofed organizational unit field in the signing chain, the exact bypass mechanism of CVE-2026-24066. | /Library/LaunchDaemons/.plist and launchctl list output: Records the registered helper tool's run-at-boot configuration; attacker persistence via a backdoored LaunchDaemon would appear here as a net-new or modified plist entry introduced during the exploitation window. | /var/db/auth.db (Authorization Services database): Contains the policy rules that governed the Slate Digital helper's privilege grants; abnormal rule additions or modifications during the exposure window indicate the helper's authorization policy was tampered with following successful escalation. | macOS process accounting / `ps aux` snapshots and osquery process history: PID reuse race condition exploitation (CVE-2026-24067) would manifest as anomalous short-lived processes spawned by the Slate Digital helper or its parent, with PIDs rapidly cycling; timestamped process snapshots taken at detection time are the primary artifact for reconstructing this attack sequence.

Per-Action IR Details

Step 1: Containment — Identify all macOS endpoints running Slate Digital Connect 1.37.0 using your asset inventory (CIS 1.1). Restrict local interactive access to those systems until patched, prioritizing shared or multi-user studio workstations where untrusted local users may be present.

NIST Phase: Containment

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), NIST AC-6 (Least Privilege)

Compensating: Run `system_profiler SPApplicationsDataType` via SSH or MDM remote command (Jamf, Mosyle) on all managed macOS endpoints and grep for 'Slate Digital Connect' with version '1.37.0'. For endpoints without MDM, deploy a one-liner via shared admin: `find /Applications -name 'Slate Digital Connect.app' -exec defaults read {}/Contents/Info.plist CFBundleShortVersionString \;`. Restrict local console login by disabling the affected accounts temporarily via `sudo dseditgroup -o edit -d -t user com.apple.access_loginwindow` on shared studio machines.

Evidence: Before restricting access, capture a snapshot of currently running processes via `sudo ps aux > /tmp/ps_snapshot_$(hostname)_$(date +%Y%m%d%H%M%S).txt` and the current LaunchDaemons inventory via `launchctl list > /tmp/launchctl_snapshot.txt`. Capture `/Library/LaunchDaemons/` directory listing and plist contents for any Slate Digital helper tool (look for bundle identifiers matching `com.slatedigital.*` or `com.waves.*`). These baselines establish pre-containment state for later comparison.

Step 2: Detection — Query endpoint logs for unexpected privileged helper tool invocations or XPC service connections originating from non-Slate Digital processes. On macOS, review Unified Log entries (log show

--predicate) filtering on the Slate Digital Connect bundle identifier and privileged helper tool name. Look for process substitution patterns near PID reuse events (T1548.004). Enable AU-2 event logging for privilege escalation events if not already active.

NIST Phase: Detection Analysis

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

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

Compensating: Execute the following Unified Log query on each affected macOS host to surface anomalous XPC connections and privileged helper invocations: `log show --predicate '(subsystem == "com.apple.xpc") AND (category == "connection")' --info --last 72h > /tmp/xpc_log.txt`. Separately query for Authorization Services events tied to the Slate Digital helper: `log show --predicate 'process == "authd" OR process == "Security"' --info --last 72h | grep -i slate > /tmp/authd_slate.txt`. For PID reuse race condition artifacts (CVE-2026-24067), look for rapid sequential PID assignments near the Slate helper PID using `log show --predicate 'subsystem == "com.apple.launchd"' --info --last 72h | grep -i 'pid'`. Use osquery with the query `SELECT pid, parent, name, cmdline, start_time FROM processes WHERE name LIKE '%slate%' OR cmdline LIKE '%com.slatedigital%';` to enumerate any residual suspicious processes.

Evidence: Collect the macOS Unified Log archive covering the window of potential exploitation: `log collect --last 72h --output /tmp/unified_log_$(hostname).logarchive`. Extract Security framework authorization logs from `/var/log/` and the ASL (Apple System Log) database. Capture the XPC service endpoint list for the Slate Digital helper via `sudo launchctl print system/`. For the certificate bypass vector (CVE-2026-24066), collect code signing audit entries: `log show --predicate 'subsystem == "com.apple.securityd" AND category == "codesigning"' --info --last 72h > /tmp/codesign_log.txt`. These artifacts would reveal whether a self-signed cert with a matching organizational unit field was accepted by the helper's validation routine.

Step 3: Eradication — Apply the vendor-supplied update for Slate Digital Connect when available. If no patch is yet released, remove or disable the privileged helper tool (typically registered under /Library/LaunchDaemons/) until a fix is confirmed. Verify removal using CIS 2.3 unauthorized software processes. Rotate any credentials accessible to processes running under the escalated context (D3-CRO).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 2.3 (Address Unauthorized Software), CIS 7.4 (Perform Automated Application Patch Management), NIST SI-2 (Flaw Remediation)

Compensating: If no vendor patch is yet available, unload and disable the Slate Digital privileged helper via: `sudo launchctl bootout system/` and `sudo rm /Library/LaunchDaemons/com.slatedigital..plist`, then verify removal with `sudo launchctl list | grep -i slate` (should return no results). Validate the helper binary is removed from `/Library/PrivilegedHelperTools/`. For credential rotation on systems where escalation may have occurred, enumerate local accounts that were active during the exposure window: `dscl . list /Users UniqueID | awk '$2 >= 500'` and force password resets via `sudo passwd `. Document each removed component with SHA-256 hashes (`shasum -a 256 `) before deletion for forensic continuity.

Evidence: Before eradication, preserve forensic copies of the privileged helper binary from `/Library/PrivilegedHelperTools/` and its associated plist from `/Library/LaunchDaemons/`. Compute and record SHA-256 hashes. Capture the code signing details of any suspicious binary that exploited the certificate bypass: `codesign -dvvv /Library/PrivilegedHelperTools/ 2>&1 > /tmp/codesign_detail.txt` — this will expose whether an attacker-controlled self-signed cert with a matching OU field was used (CVE-2026-24066). Preserve the full `/var/db/auth.db` Authorization Services database, which records policy rules that the helper relied upon for privilege grants.

Step 4: Recovery — After patching or helper tool removal, verify no unauthorized LaunchDaemon or LaunchAgent entries were introduced (D3-SICA). Confirm the updated application's code signature validates correctly against Apple's notarization service. Monitor local privilege events via endpoint detection tooling for 30 days post-remediation, aligned with AU-6 audit record review.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Verify the patched Slate Digital Connect installation's notarization status using: `spctl -a -vvv /Applications/'Slate Digital Connect.app' 2>&1` — output must show `source=Notarized Developer ID` and `origin=Developer ID Application: Slate Digital` with Apple's certificate chain, not a self-signed cert. Audit all LaunchDaemons and LaunchAgents for unauthorized entries introduced during the exposure window by diffing against your pre-containment snapshot: `ls -la /Library/LaunchDaemons/ /Library/LaunchAgents/ ~/Library/LaunchAgents/ > /tmp/post_patch_launch_inventory.txt && diff /tmp/pre_patch_launch_inventory.txt /tmp/post_patch_launch_inventory.txt`. For 30-day monitoring without EDR, configure a daily cron job running `launchctl list | grep -v com.apple > /var/log/launchctl_daily_$(date +%Y%m%d).txt` and alert on any net-new entries.

Evidence: Post-recovery, preserve the before/after diff of LaunchDaemons and LaunchAgents directories as evidence of clean state. Retain the `spctl` notarization validation output for the patched binary. Capture the updated code signing certificate chain (`codesign -dvvv`) for the new Slate Digital helper as the verified-good baseline. These artifacts establish the authenticated recovery state and support any post-incident review or audit inquiry.

Step 5: Post-Incident — Review privileged helper tool deployment policies across all macOS software in the environment. Establish a review process requiring vendor-supplied privileged helpers to implement PID-independent validation and full certificate chain verification before deployment approval. Map identified control gaps to NIST AC-6 (Least Privilege) and AC-3 (Access Enforcement) and schedule a formal review of macOS endpoint privilege management practices.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AC-3 (Access Enforcement), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Enumerate all currently deployed privileged helper tools across the macOS fleet: `find /Library/PrivilegedHelperTools/ -type f -exec codesign -dvvv {} 2>&1 \; | grep -E '(Identifier|TeamIdentifier|Authority)' > /tmp/all_helpers_codesign_audit.txt`. Review each helper's plist for `SMAuthorizedClients` key values — these define which applications are permitted to communicate with the helper and are the trust boundary that the certificate bypass (CVE-2026-24066) circumvented. Flag any helper whose `SMAuthorizedClients` string relies solely on organizational unit matching rather than full Team ID verification. Document findings in a macOS privileged helper risk register and assign remediation owners per CIS 7.2.

Evidence: Retain the full incident timeline, including the Unified Log archive, pre/post eradication file hashes, and LaunchDaemon diff artifacts collected in prior steps. These serve as lessons-learned inputs and support the helper deployment policy review. If escalated privileges were confirmed on any host, preserve a copy of the affected host's `/var/db/auth.db` and process snapshots as evidence of the attack surface that existed.

Detection Guidance

On macOS, use the Unified Log to query for XPC connections to the Slate Digital Connect privileged helper tool from unexpected client processes. Example query (adjust bundle ID to match your environment): 'log show --predicate "subsystem == \"com.slatedigital.connect\"" --info'. Look for client PIDs that do not correspond to the Slate Digital Connect application binary. Monitor for rapid PID reuse events near helper tool invocations, which may indicate a TOCTOU exploitation attempt (CWE-367). For CVE-2026-24066, look for self-signed certificate presentations to the helper tool's XPC interface where the subject.OU matches Slate Digital's expected value but the issuer chain does not resolve to a trusted CA. Endpoint detection tools with macOS XPC monitoring (e.g., EDR with kernel extension or system extension coverage) should alert on privilege escalation attempts matching T1548.004 (MITRE ATT&CK). NIST SP 800-53 controls: AC-6 (Least Privilege), SI-7 (System

Monitoring) are applicable countermeasures. No public IOCs or exploitation signatures are available in the provided source material at this time. Check Slate Digital's security advisory for any vendor-supplied indicators or detection signatures.

Framework Mappings

MITRE-ATTACK

- **T1548.004** — Elevated Execution with Prompt
- **T1574** — Hijack Execution Flow

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures

NIST-800-53R5

- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates
- **AT-2** — Literacy Training and Awareness
- **SC-13** — Cryptographic Protection
- **AC-6** — Least Privilege

CIS-V8

- **3.10** — Encrypt Sensitive Data in Transit
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

ISO-27001-2022

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

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1548.004	Elevated Execution with Prompt	Privilege-Escalation
T1574	Hijack Execution Flow	Persistence

Sources

Source	URL	Tier
CVE-2026-24066 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-24066	T1
Newest CVEs | Tenable®	https://www.tenable.com/cve/newest	T3
CVE-2026-24040: jsPDF Information Disclosure Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2026-24040/	T3
CVEs and Security Vulnerabilities - OpenCVE	https://app.opencve.io/cve/?cwe=CWE-338	T3
CVE-2026-21262: SQL Server Zero-Day Fixed in Microsoft's March ...	https://socprime.com/blog/cve-2026-21262-vulnerability/	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-24067, CVE-2026-24066	T1

Generated 2026-06-11 14:25 UTC by TJS Security Command Center