INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-24 06:19 UTC

CVE-2026-44050: A heap-based buffer overflow in the CNID daemon comm_rcv() function in Netatalk 2.0.0 through 4.4.2 ...

CVE VULNERABILITY | CRITICAL | CVSS 9.9

SCC Item ID	SCC-CVE-2026-0213
Type	CVE Vulnerability
CVE ID	CVE-2026-44050
Severity	CRITICAL
CVSS Base Score	9.9
EPSS Score	0.0014 (33th percentile)
Affected Products	Netatalk 2.0.0 through 4.4.2
Published	2026-05-21T08:16:20.580
Discovery Source	Nvd

Executive Summary

A critical heap-based buffer overflow (CVE-2026-44050, CVSS 9.9) has been disclosed in Netatalk versions 2.0.0 through 4.4.2, an open-source AFP file-sharing service widely deployed in mixed macOS/Linux environments. A remote authenticated attacker can send a malformed message to the CNID daemon to execute arbitrary code at elevated privileges or crash the service entirely. Organizations running Netatalk for macOS-to-Linux file sharing should treat this as an immediate patching priority.

Technical Analysis

CVE-2026-44050 is a heap-based buffer overflow (CWE-122) in the comm_rcv() function of the Netatalk CNID (Catalogue Node ID) daemon, affecting all releases from 2.0.0 through 4.4.2. The CNID daemon manages AFP file identifier mappings and runs with elevated privileges. An authenticated remote attacker can submit a malformed or oversized AFP message that overflows the heap buffer in comm_rcv(), corrupting adjacent memory regions. Successful exploitation enables arbitrary code execution in the daemon's privilege context (T1068, Exploitation for Privilege Escalation) or a denial-of-service condition (T1499, Endpoint Denial of Service). The attack vector requires network access to the AFP/CNID service and a valid authenticated session (T1210, Exploitation of Remote Services). CVSS base score is 9.9. EPSS score is 0.00137 (33rd percentile), indicating limited observed exploitation activity at time of disclosure. The vulnerability is not currently listed in the CISA KEV catalog. As of the time of this report, no patch has been released. Operators should monitor the

official Netatalk project repository (https://netatalk.io) and the NVD entry for patch availability announcements. Until a patch is available, mitigation relies on network segmentation and service restriction.

Action Checklist

1. Step 1: Containment, Immediately restrict network access to the Netatalk AFP service (default TCP port 548) and the CNID daemon port using host-based and perimeter firewall rules (NIST SC-7, CIS 4.4). Confirm no Netatalk instances (versions 2.0.0-4.4.2) are internet-facing. If the service cannot be firewalled, consider stopping the Netatalk daemon on non-essential hosts until a patch is available.
2. Step 2: Detection, Audit all hosts running Netatalk using asset inventory records (CIS 1.1). Query package managers (dpkg -l netatalk, rpm -q netatalk, brew list netatalk) to identify installed versions 2.0.0-4.4.2. Review CNID daemon logs (typically /var/log/netatalk/ or syslog) for unexpected crashes, large inbound message anomalies, or segfault entries in dmesg/kern.log that may indicate exploitation attempts. Monitor for abnormal child process spawns from the Netatalk daemon (D3-SFA, System File Analysis).
3. Step 3: Eradication, Apply the vendor-released patch for Netatalk once available from the official project repository (https://netatalk.io). If no patch is yet released, disable the CNID daemon service. On Linux/Unix hosts with systemd: systemctl stop cnid-metad && systemctl disable cnid-metad. On macOS, use launchctl unload to disable the Netatalk service. Confirm service is stopped across all deployment targets. Restrict AFP service to trusted subnets only via access control lists (NIST AC-3, AC-4). Remove or isolate any Netatalk instances that cannot be immediately patched.
4. Step 4: Recovery, After patching, restart Netatalk services and validate daemon integrity by comparing installed binaries against known-good checksums from the vendor release. Confirm firewall rules are still in place post-restart. Enable enhanced logging on the CNID daemon and AFP service (NIST AU-2, AU-12) and monitor for at least 72 hours for signs of prior compromise, including unexpected file modifications, new accounts, or privilege escalation events (D3-LAM, Local Account Monitoring).
5. Step 5: Post-Incident, Review asset inventory completeness for all AFP/Netatalk deployments (CIS 1.1). Evaluate whether least-privilege principles are enforced on the Netatalk daemon process (NIST AC-6, CIS 5.4). Assess whether authenticated remote access to AFP services requires MFA (CIS 6.3, D3-MFA). Document this vulnerability in the risk register and schedule a broader audit of open-source file-sharing services in the environment.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/privacy counsel immediately if forensic review of cnid-metad crash logs, auth.log, or AFP volume access records indicates exploitation occurred prior to containment — particularly if AFP shares hosted PII, PHI, or regulated data, as unauthorized RCE at daemon privilege level constitutes a reportable breach under HIPAA, GDPR, and most US state notification statutes.

Recovery Notes	After applying the official Netatalk patch from netatalk.io (versions beyond 4.4.2), validate binary integrity against vendor SHA-256 checksums before restarting services and confirm cnid-metad is running as a non-root service account with filesystem permissions scoped to AFP volume paths only. Monitor afpd.log, cnid_metad.log, and auth.log continuously for a minimum of 72 hours post-recovery, specifically watching for heap corruption indicators (segfaults, abnormal child spawns from afpd), new SUID binaries, and account creation events that could indicate a pre-patch compromise was not fully eradicated. If any indicators of prior compromise are found during the recovery monitoring window, treat the affected host as potentially fully compromised and escalate to full forensic acquisition before returning it to production.
Forensic Artifacts	/var/log/netatalk/cnid_metad.log and /var/log/netatalk/afpd.log — heap overflow exploitation of comm_rcv() produces malformed inbound CNID message entries immediately followed by daemon crash or abnormal restart; these logs establish the exploitation timeline and source IP of the attacker's AFP session | dmesg and /var/log/kern.log segfault entries for cnid_metad PID — a heap-based buffer overflow in comm_rcv() that leads to RCE or crash produces kernel-level segfault records of the form 'cnid_metad[]: segfault at ip sp error in cnid_metad[]', which can be correlated with the specific overflow offset | gcore memory dump of cnid_metad process (capture before patching or stopping) — preserves heap layout at time of exploitation for offline analysis; a successful heap overflow RCE against comm_rcv() will show corrupted heap metadata and injected shellcode or ROP chain fragments in the heap region used for inbound message buffering | AFP volume paths (defined in afp.conf) — inspect for AppleDouble resource fork files (._filename pattern) and .DS_Store modifications timestamped during the exploitation window, as post-RCE attacker activity on AFP shares leaves macOS-format metadata artifacts that are distinct from normal Linux file operations | /etc/passwd, /etc/sudoers, and ~/.ssh/authorized_keys on the Netatalk host — if cnid-metad ran as root (the common default), successful RCE would most likely result in persistence implanted via new root-equivalent account creation, sudoers modification, or SSH key injection, all of which leave plaintext artifacts with filesystem timestamps correlating to the exploitation window

Per-Action IR Details

Step 1: Containment — Immediately restrict network access to the Netatalk AFP service (default TCP port 548) and the CNID daemon port using host-based and perimeter firewall rules (NIST SC-7, CIS 4.4). Confirm no Netatalk instances (versions 2.0.0–4.4.2) are internet-facing. If the service cannot be firewalled, consider stopping the Netatalk daemon on non-essential hosts until a patch is available.

NIST Phase: Containment

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

Controls: NIST SC-7 (Boundary Protection), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On Linux hosts, immediately execute: `iptables -A INPUT -p tcp --dport 548 -j DROP && iptables -A INPUT -p tcp --dport 4700 -j DROP` (port 4700 is the default cnid-metad port). Persist rules with `iptables-save > /etc/iptables/rules.v4`. For macOS clients, use `pfctl` to block outbound AFP: add `block out proto tcp to any port 548` to /etc/pf.conf and run `pfctl -f /etc/pf.conf -e`. Verify no active AFP sessions survive: `ss -tnp | grep ':548'` and `lsof -i :4700`.

Evidence: BEFORE blocking the port, capture active connection state: `ss -tnp | grep ':548'` and `ss -tnp | grep ':4700'` to document any currently connected remote IPs to the cnid-metad and afpd processes. Record process tree with `ps auxf | grep -E 'cnid|afpd'` to baseline parent-child relationships. Export current iptables state with `iptables -L -n -v` to document pre-containment exposure. Capture `/proc//net/tcp` for socket-level connection detail before the daemon is touched.

Step 2: Detection — Audit all hosts running Netatalk using asset inventory records (CIS 1.1). Query package managers (dpkg -l netatalk, rpm -q netatalk, brew list netatalk) to identify installed versions 2.0.0–4.4.2. Review CNID daemon logs (typically /var/log/netatalk/ or syslog) for unexpected crashes, large inbound message anomalies, or segfault entries in dmesg/kern.log that may indicate exploitation attempts. Monitor for abnormal child process spawns from the Netatalk daemon (D3-SFA — System File Analysis).

NIST Phase: Detection Analysis

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring)

Compensating: Deploy a Sigma rule targeting cnid-metad segfaults: search syslog/kern.log with `grep -rE 'cnid_metad.*segfault|afpd.*segfault|heap.*netatalk' /var/log/`. For version enumeration across multiple Linux hosts, use a one-liner via SSH: `for h in $(cat hosts.txt); do ssh $h 'dpkg -l netatalk 2>/dev/null || rpm -q netatalk 2>/dev/null'; done`. On hosts with osquery deployed, run: `SELECT name, version, source FROM deb_packages WHERE name='netatalk';` For process spawn anomalies without EDR, configure Sysmon (Linux) with a rule targeting ProcessCreate events where ParentImage matches `/usr/sbin/cnid_metad` and ChildImage is not `/usr/sbin/afpd`.

Evidence: Collect `/var/log/netatalk/afpd.log` and `/var/log/netatalk/cnid_metad.log` for the 30 days prior to detection — heap overflow exploitation of comm_rcv() in cnid-metad produces malformed message receipt entries followed by abnormal termination. Run `dmesg | grep -E 'cnid|afpd|segfault|heap'` and export full output. Check `/var/log/syslog` or `/var/log/messages` for `cnid_metad[]: segfault at` entries, which indicate a crash caused by a malformed inbound CNID message. Capture `journalctl -u netatalk --since '30 days ago'` and `journalctl -u cnid-metad --since '30 days ago'` before any service restarts overwrite volatile journal data.

Step 3: Eradication — Apply the vendor-released patch for Netatalk once available from the official project repository (https://netatalk.io). If no patch is yet released, disable the CNID daemon service (systemctl stop cnid-metad / systemctl disable cnid-metad) and restrict AFP service to trusted subnets only via access control lists (NIST AC-3, AC-4). Remove or isolate any Netatalk instances that cannot be immediately patched.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If the official patch is not yet available from netatalk.io, apply a compiled-from-source temporary mitigation: build Netatalk with stack canaries and ASLR explicitly enabled (`./configure CFLAGS='-fstack-protector-strong -D_FORTIFY_SOURCE=2' LDFLAGS='-Wl,-z,relro,-z,now'`), which will not fix the underlying heap overflow in comm_rcv() but significantly raises exploitation difficulty. Alternatively, replace cnid-metad with the `cnid_last` backend (set `cnid scheme = last` in `afp.conf`) which eliminates the vulnerable CNID daemon entirely at the cost of CNID persistence across renames. Validate the patch version post-install: `dpkg -l netatalk | grep '^ii'` and confirm the version string is beyond 4.4.2.

Evidence: Before stopping or patching the cnid-metad service, collect a full process memory snapshot if exploitation is suspected: `gcore ` to capture heap state for post-incident forensic analysis. Hash all Netatalk binaries prior to patch: `sha256sum /usr/sbin/cnid_metad /usr/sbin/afpd /usr/lib/*/netatalk/*.so* > /evidence/netatalk_pre_patch_hashes.txt`. Export the running afp.conf and AppleVolumes configuration: `cp /etc/netatalk/afp.conf /evidence/ && cp /etc/netatalk/AppleVolumes.default /evidence/` — these document share exposure scope and may reveal attacker-modified configurations if the host was already compromised.

Step 4: Recovery — After patching, restart Netatalk services and validate daemon integrity by comparing installed binaries against known-good checksums from the vendor release. Confirm firewall rules are still in place post-restart. Enable enhanced logging on the CNID daemon and AFP service (NIST AU-2, AU-12) and monitor for at least 72 hours for signs of prior compromise, including unexpected file modifications, new accounts, or privilege escalation events (D3-LAM — Local Account Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 8.2 (Collect Audit Logs)

Compensating: Verify patched binary integrity against vendor-published SHA-256 checksums from the netatalk.io release page: `sha256sum -c netatalk-.sha256`. Monitor for post-exploitation persistence artifacts specific to a heap overflow RCE against cnid-metad running as root or a privileged daemon account: `find / -newer /etc/netatalk/afp.conf -type f -ls 2>/dev/null` to surface files created after the service was first exposed. Monitor new SUID/SGID binaries: `find / -perm /6000 -type f 2>/dev/null > /tmp/suid_post_patch.txt && diff /tmp/suid_baseline.txt /tmp/suid_post_patch.txt`. Watch for new entries in `/etc/passwd`, `/etc/sudoers`, and `~/.ssh/authorized_keys` on hosts where cnid-metad ran as root, as these are primary persistence targets after heap overflow RCE.

Evidence: Run `last` and `lastb` to identify any login events correlated with the window of cnid-metad exposure, particularly from IPs that previously connected to port 4700. Check `/var/log/auth.log` or `/var/log/secure` for `sudo` or `su` invocations originating from the Netatalk daemon's UID. Inspect the Netatalk AFP volumes (defined in afp.conf) for unexpected files with CREATOR/TYPE metadata inconsistencies using `find -name '._*' -newer /var/log/netatalk/afpd.log` — AppleDouble resource fork files (._filename) written during the exploitation window may indicate attacker file staging. Capture `crontab -l` for all users and `/etc/cron.*` directories before declaring recovery complete.

Step 5: Post-Incident — Review asset inventory completeness for all AFP/Netatalk deployments (CIS 1.1). Evaluate whether least-privilege principles are enforced on the Netatalk daemon process (NIST AC-6, CIS 5.4). Assess whether authenticated remote access to AFP services requires MFA (CIS 6.3, D3-MFA). Document this vulnerability in the risk register and schedule a broader audit of open-source file-sharing services in the environment.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST RA-3 (Risk Assessment), NIST IR-4 (Incident Handling), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Audit whether cnid-metad and afpd run as root or a dedicated low-privilege service account: `ps aux | grep -E 'cnid|afpd' | awk '{print $1}'` — if the UID is root (0), document this as a critical finding because heap overflow RCE in comm_rcv() directly yields root shell. Create a dedicated `netatalk` system user and configure `afp.conf` with `uamlist = uams_dhx2.so` (strongest available UAM) and `login message` to enforce authenticated sessions. For broader open-source AFP/SMB service audit, enumerate all listening file-sharing services: `ss -tnlp | grep -E ':548|:445|:139|:2049'` across all Linux hosts and cross-reference against the asset inventory to identify undocumented Netatalk, Samba, or NFS instances.

Evidence: Produce a lessons-learned artifact documenting: (1) time from CVE-2026-44050 disclosure to identification of all vulnerable Netatalk instances in the environment (measures CIS 1.1 effectiveness), (2) whether any cnid-metad crash logs predating the advisory were present but unreviewed (measures AU-6 monitoring gap), and (3) the privilege level at which cnid-metad ran on each identified host (measures AC-6 compliance). Archive all collected forensic artifacts — cnid-metad core dumps, pre-patch binary hashes, afpd.log exports, and connection logs — per NIST AU-11 (Audit Record Retention) retention requirements for potential regulatory disclosure obligations if AFP shares contained PII or regulated data.

Detection Guidance

Query package managers across all Linux/Unix hosts for Netatalk versions 2.0.0-4.4.2: run 'dpkg -l netatalk' (Debian/Ubuntu), 'rpm -q netatalk' (RHEL/CentOS), or check Homebrew on macOS. Review /var/log/netatalk/, syslog, and kernel logs (dmesg) for CNID daemon crashes, segmentation faults, or unusually large AFP

message processing entries. These may indicate exploitation attempts or successful overflow triggering. Use EDR tooling to flag unexpected child processes spawned by cnid-metad or afpd parent processes. Monitor network traffic on TCP port 548 (AFP) for sessions sending oversized or malformed message payloads. Cross-reference authenticated AFP session logs with user account activity to identify anomalous access patterns (NIST AU-6). No public IOCs (IPs, hashes, domains) are associated with this CVE at time of disclosure.

Framework Mappings

MITRE-ATTACK

- **T1499** — Endpoint Denial of Service
- **T1068** — Exploitation for Privilege Escalation
- **T1210** — Exploitation of Remote Services

NIST-800-53R5

- **SC-5** — Denial-of-Service Protection
- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1499	Endpoint Denial of Service	Impact
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1210	Exploitation of Remote Services	Lateral-Movement

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-44050	T1
CVE-2026-44050: A heap-based buffer overflow in the CNID ...	https://research.averlon.ai/vulnerability-intelligence/cve/CVE-2026...	T3
CVE-2026-44050 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-44050	T3

Source	URL	Tier
CVE-2026-44050 - Debian Security Tracker	https://security-tracker.debian.org/tracker/CVE-2026-44050	**T3**
CVE-2026-44050 CPEs | Tenable®	https://www.tenable.com/cve/CVE-2026-44050/cpes	**T3**

Generated 2026-05-24 06:19 UTC by TJS Security Command Center