INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-24 06:20 UTC

CVE-2026-44051: An improper link resolution vulnerability in Netatalk 3.0.2 through 4.4.2 allows a remote authentica...

CVE VULNERABILITY | HIGH | CVSS 8.1

SCC Item ID	SCC-CVE-2026-0215
Type	CVE Vulnerability
CVE ID	CVE-2026-44051
Severity	HIGH
CVSS Base Score	8.1
EPSS Score	0.0002 (6th percentile)
Affected Products	Netatalk 3.0.2 through 4.4.2
Published	2026-05-21T08:16:20.690
Discovery Source	Nvd

Executive Summary

CVE-2026-44051 is a high-severity symlink vulnerability (CVSS 8.1) in Netatalk, the open-source Apple Filing Protocol server used on Linux and Unix systems to enable macOS file sharing. A remote authenticated attacker can plant attacker-controlled symbolic links, then read or overwrite arbitrary files on the host system. Organizations running Netatalk for macOS-to-Linux file sharing should treat this as a priority patching item, particularly where the AFP service is exposed to untrusted network segments.

Technical Analysis

CVE-2026-44051 affects Netatalk versions 3.0.2 through 4.4.2. The root cause is CWE-59 (Improper Link Resolution Before File Access, 'Link Following'). An authenticated remote attacker can create attacker-controlled symlinks through the AFP interface, then leverage them to perform arbitrary file reads or arbitrary file overwrites on the underlying host filesystem. No privilege escalation is required beyond valid AFP authentication. CVSS base score is 8.1 (High); impact is split across confidentiality (arbitrary read) and integrity (arbitrary overwrite) with no availability component scored. EPSS score is 0.00019 (5.5th percentile), indicating low current exploitation probability. The vulnerability is not listed in CISA KEV as of this report. MITRE ATT&CK mappings: T1083 (File and Directory Discovery) for the read vector; T1565.001 (Stored Data Manipulation) for the overwrite vector. No public exploit code or active threat actor campaigns are attributed at this time. Patch to Netatalk 4.4.3 or later; in the interim, restrict AFP service access to trusted network segments and require strong

authentication.

Action Checklist

1. Step 1: Containment. Identify all Linux and Unix hosts running Netatalk 3.0.2 through 4.4.2 (check `netatalk --version` or package manager). Restrict AFP port 548/TCP to trusted macOS client subnets via firewall rule immediately. If AFP is internet-facing, take the service offline until patched. Reference CIS Controls v8 4.4 (Implement and Manage a Firewall on Servers) and NIST AC-17 (Remote Access) for access restriction guidance.
2. Step 2: Detection. Query authentication logs for AFP service logins (typically /var/log/afpd.log, /var/log/netatalk.log, or syslog tagged 'afpd', path varies by distribution). Hunt for unexpected symlink creation events in directories served by Netatalk: use `find -type l` to enumerate existing symlinks. Review file access logs for reads or writes to paths outside expected share boundaries. Alert on AU-6 (Audit Record Review, Analysis, and Reporting) principles; look for file access patterns crossing share directory boundaries. No public IOCs are available for this CVE.
3. Step 3: Eradication. Upgrade Netatalk to version 4.4.3 or later. Check the official Netatalk GitHub release page and your Linux distribution's security advisory channel (e.g., SUSE, Debian, Ubuntu Security Notices) for confirmed patched package versions. If an official patch is not yet available, disable the AFP service (`systemctl stop netatalk && systemctl disable netatalk`) on non-essential hosts. Reference CIS Controls v8 7.3 (Perform Automated Operating System Patch Management) and CIS Controls v8 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery. After patching, audit all symlinks in AFP-served directories: `find -type l -ls`. Remove any symlinks pointing outside the intended share scope. Verify file integrity for sensitive files in or adjacent to shared directories using host-based integrity monitoring aligned with D3-SFA (System File Analysis). Re-enable AFP service only after confirming the patched version is installed. Monitor afpd logs for 7 days post-remediation for anomalous file access patterns. Reference NIST AU-6 for ongoing log review cadence.
5. Step 5: Post-Incident. This vulnerability exposes two control gaps: (1) insufficient network segmentation isolating AFP services from untrusted users (NIST AC-4, Information Flow Enforcement; CIS Controls v8 4.4), and (2) absence of symlink restriction controls in file-sharing service configurations. Document a configuration hardening baseline for Netatalk deployments that disables symlink following where AFP configuration supports it. Update the vulnerability management process to include AFP service inventory under CIS Controls v8 1.1 (Enterprise Asset Inventory) and CIS Controls v8 7.1 (Vulnerability Management Process). Review whether AFP is still required; replace with SMB/CIFS where feasible to reduce attack surface.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and legal/compliance immediately if forensic analysis of afpd.log or symlink artifacts reveals file reads or writes to paths containing PII, PHI, credentials (e.g., /etc/passwd, /etc/shadow, SSH private keys, or application secrets), or if any authenticated AFP session originated from an IP outside the known macOS client population, indicating potential attacker use of a compromised or rogue AFP client credential.

Recovery Notes	Re-enable the afpd service only after 'netatalk --version' confirms the patched binary (4.4.3 or distribution-confirmed equivalent) is running and the post-remediation symlink audit shows zero symlinks resolving outside the intended share boundary. Monitor /var/log/afpd.log or journalctl -u netatalk daily for 7 days post-recovery, specifically hunting for file access events referencing paths outside configured AFP share volumes, which would indicate a missed attacker-planted symlink or a second exploitation attempt. If AIDE or Tripwire file integrity baselines flag unexpected changes to sensitive files adjacent to AFP share directories during the monitoring window, treat as a confirmed compromise and re-initiate containment.
Forensic Artifacts	/var/log/afpd.log or 'journalctl -u netatalk' output: Primary artifact for authenticated AFP session history, user-to-IP mapping, and file operation requests — exploitation of CVE-2026-44051 would show file access events resolving to paths outside the configured share volume boundaries. | Symlink enumeration snapshot ('find -type l -ls'): Attacker-planted symlinks targeting sensitive host paths (e.g., -> /etc/shadow, -> /root/.ssh/id_rsa, -> /var/lib/application/secrets) are the direct forensic signature of this vulnerability's exploitation mechanism. | Kernel auditd records for symlink/symlinkat syscalls by afpd PID ('ausearch -sc symlink,symlinkat -p $(pgrep afpd)'): Captures the moment of symlink creation within the AFP-served directory, attributable to an authenticated AFP session, which is the core exploitation action for CVE-2026-44051. | File mtime/ctime changes on sensitive files outside AFP share boundaries during the exposure window ('find / -newer -not -path "/*" -ls'): Post-exploitation indicator showing which host files were read or overwritten via the attacker-controlled symlink after it was planted. | Network connection logs (firewall logs, /proc/net/tcp, or 'ss -tnp' output) for port 548/TCP: Establishes the full population of source IPs that authenticated to AFP during the vulnerability window, enabling scope assessment of how many clients — legitimate or attacker-controlled — had access to the vulnerable afpd service.

Per-Action IR Details

Step 1: Containment — Identify all Linux and Unix hosts running Netatalk 3.0.2 through 4.4.2 (check 'netatalk --version' or package manager). Restrict AFP port 548/TCP to trusted macOS client subnets via firewall rule immediately. If AFP is internet-facing, take the service offline until patched. Reference CIS 4.4 (Implement and Manage a Firewall on Servers) and NIST AC-17 (Remote Access) for access restriction guidance.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Enumerate all affected hosts without a CMDB using: 'for host in $(cat hosts.txt); do ssh $host "netatalk --version 2>/dev/null || dpkg -l netatalk 2>/dev/null || rpm -q netatalk 2>/dev/null"'; done'. Block port 548/TCP immediately using iptables: 'iptables -I INPUT -p tcp --dport 548 ! -s -j DROP && iptables-save > /etc/iptables/rules.v4'. On hosts where iptables is unavailable, use 'ufw deny from any to any port 548' and allow only the specific macOS client subnet. Verify with 'ss -tlnp | grep 548' that afpd is no longer externally reachable.

Evidence: Before restricting port 548/TCP, capture a full netstat/ss snapshot of current AFP connections to identify any active authenticated sessions that may indicate ongoing exploitation: 'ss -tnp | grep :548 > /tmp/afp_active_connections_$(date +%Y%m%d%H%M%S).txt'. Preserve afpd.log (/var/log/afpd.log or via 'journalctl -u netatalk --since "7 days ago"') to establish a baseline of authenticated users and their source IPs prior to containment. Also snapshot all existing symlinks in AFP share directories before any cleanup: 'find -type l -ls > /tmp/afp_symlinks_pre_containment_$(date +%Y%m%d%H%M%S).txt'.

Step 2: Detection — Query authentication logs for AFP service logins (typically /var/log/afpd.log or syslog tagged 'afpd'). Hunt for unexpected symlink creation events in directories served by Netatalk: use 'find -type l'

to enumerate existing symlinks. Review file access logs for reads or writes to paths outside expected share boundaries. Alert on AU-6 (Audit Record Review, Analysis, and Reporting) principles — look for file access patterns crossing share directory boundaries. No public IOCs are available for this CVE.

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), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Enable afpd verbose logging if not already active by adding 'log level:default = debug' to /etc/netatalk/afp.conf, then restart netatalk. Parse afpd.log for symlink-related activity using: 'grep -E "(symlink|EPERM|path traversal|\.\./)" /var/log/afpd.log'. Deploy inotifywait (from inotify-tools package) on AFP share directories to alert on symlink creation in real time: 'inotifywait -m -r -e create --format "%T %w%f %e" --timefmt "%Y%m%d-%H%M%S" | grep -i "symlink\|lnk"'. For host-level file integrity, run: 'find -type l | while read L; do T=$(readlink -f "$L"); echo "$L -> $T"; done | grep -v "^"' to identify symlinks resolving to paths outside the intended share boundary — these are your primary exploitation indicators for CVE-2026-44051.

Evidence: Collect the full afpd authentication log showing user logins, session tokens, and file operation requests (/var/log/afpd.log or 'journalctl -u netatalk -o json > /tmp/afpd_journal.json'). Extract kernel audit records (if auditd is running) for symlink system calls from the afpd process: 'ausearch -sc symlink,symlinkat -p $(pgrep afpd) > /tmp/afpd_symlink_syscalls.txt'. Capture a recursive directory listing with inode details of all AFP-served share paths: 'find -ls > /tmp/afp_share_snapshot_$(date +%Y%m%d%H%M%S).txt'. Preserve syslog entries tagged 'afpd' from the 30 days preceding discovery to establish attacker dwell time. If auditd is not running, check /proc//fd for any open file descriptors pointing outside share boundaries as a live triage indicator.

Step 3: Eradication — Upgrade Netatalk to version 4.4.3 or the vendor-released patched version once available. Check the official Netatalk GitHub release page and your Linux distribution's security advisory channel (e.g., SUSE, Debian, Ubuntu Security Notices) for confirmed patched package versions. If an official patch is not yet available, disable the AFP service (systemctl stop netatalk && systemctl disable netatalk) on non-essential hosts. Reference CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Before upgrading, record the installed Netatalk version and package hash as evidence: 'dpkg -l netatalk | tee /tmp/netatalk_pre_patch_version.txt' (Debian/Ubuntu) or 'rpm -qi netatalk | tee /tmp/netatalk_pre_patch_version.txt' (RHEL/SUSE). After upgrade, verify the binary matches the expected version: 'netatalk --version' and compare the package checksum against the distribution's signed repository metadata. Where package manager upgrade is unavailable (e.g., compiled from source), download the 4.4.3 tarball from https://github.com/Netatalk/netatalk/releases, verify the GPG signature or SHA256 checksum published in the release notes before building, and replace the running binary. Confirm afpd is running the new version post-restart: 'systemctl status netatalk && netatalk --version'.

Evidence: Before patching, preserve a memory snapshot of the running afpd process if exploitation is suspected: 'gcore $(pgrep afpd) -o /tmp/afpd_memdump' (requires gdb). Capture the pre-patch binary hash for chain-of-custody: 'sha256sum $(which afpd) > /tmp/afpd_binary_hash_pre_patch.txt'. Record all open files held by afpd at time of eradication: 'lsof -p $(pgrep afpd) > /tmp/afpd_open_files_$(date +%Y%m%d%H%M%S).txt'. These artifacts establish whether the vulnerable binary was actively exploited and provide forensic baseline for post-eradication comparison.

Step 4: Recovery — After patching, audit all symlinks in AFP-served directories: 'find -type l -ls'. Remove any symlinks pointing outside the intended share scope. Verify file integrity for sensitive files in or adjacent to shared directories using host-based integrity monitoring aligned with D3-SFA (System File Analysis).

Re-enable AFP service only after confirming the patched version is installed. Monitor afpd logs for 7 days post-remediation for anomalous file access patterns. Reference NIST AU-6 for ongoing log review cadence.

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), NIST CM-6 (Configuration Settings), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Run AIDE (Advanced Intrusion Detection Environment) or Tripwire Open Source to baseline file integrity of the AFP share directories and adjacent sensitive paths post-patch: 'aide --init && mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db'. Schedule daily checks: 'aide --check > /tmp/aide_check_$(date +%Y%m%d).txt'. For symlink-specific cleanup, run: 'find -type l | while read L; do T=$(readlink -f "$L"); if [["$T" != *]]; then echo "MALICIOUS SYMLINK: $L -> $T"; rm -v "$L"; fi; done'. Configure afpd to log at 'info' level minimum post-recovery and pipe logs to a central syslog server or local log file monitored by logwatch for the 7-day post-remediation window.

Evidence: Before re-enabling afpd, generate a post-remediation symlink audit report: 'find -type l -ls > /tmp/afp_symlinks_post_remediation_$(date +%Y%m%d%H%M%S).txt' and diff against the pre-containment snapshot captured in Step 1 to identify any attacker-planted symlinks that persisted. Collect file modification timestamps (mtime/ctime) for sensitive files in or adjacent to share directories: 'find -newer /tmp/afp_symlinks_pre_containment*.txt -ls' to identify files accessed or modified during the exploitation window. Preserve post-patch afpd binary hash: 'sha256sum $(which afpd) > /tmp/afpd_binary_hash_post_patch.txt' to confirm eradication integrity.

Step 5: Post-Incident — This vulnerability exposes two control gaps: (1) insufficient network segmentation isolating AFP services from untrusted users (NIST AC-4, Information Flow Enforcement; CIS 4.4), and (2) absence of symlink restriction controls in file-sharing service configurations. Document a configuration hardening baseline for Netatalk deployments that disables symlink following where AFP configuration supports it. Update the vulnerability management process to include AFP service inventory under CIS 1.1 (Enterprise Asset Inventory) and CIS 7.1 (Vulnerability Management Process). Review whether AFP is still required; replace with SMB/CIFS where feasible to reduce attack surface.

NIST Phase: Post Incident

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), NIST CM-6 (Configuration Settings), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Document the Netatalk hardening baseline in a version-controlled configuration file (e.g., git-tracked /etc/netatalk/afp.conf). Add 'follow symlinks = no' to afp.conf if supported by the installed version to restrict symlink traversal at the application layer — verify the option is honored by testing with a symlink pointing outside the share after config reload. Build an osquery query to continuously inventory AFP service presence across the fleet: 'SELECT name, version, source FROM deb_packages WHERE name = "netatalk" UNION SELECT name, version, source FROM rpm_packages WHERE name = "netatalk";'. Schedule this as a weekly osquery scheduled query and alert on any result showing versions 3.0.2 through 4.4.2. Add Netatalk (port 548/TCP) to network scanning scope in Nmap-based asset discovery: 'nmap -p 548 --open -oN /tmp/afp_exposure_scan.txt'.

Evidence: Compile the lessons-learned dossier including: (1) timeline from Netatalk version install date to patch date derived from package manager history ('zcat /var/log/dpkg.log*.gz | grep netatalk'), (2) the pre/post symlink audit diff from Step 4, (3) the afpd authentication log excerpt identifying all authenticated users during the exposure window, and (4) network flow records or firewall logs confirming which source IPs accessed port 548/TCP during the vulnerability window. These artifacts collectively document exposure duration, blast radius, and affected user accounts for any regulatory breach notification assessment.

Detection Guidance

Primary log source: afpd service logs, typically at /var/log/afpd.log or /var/log/netatalk.log, or captured via syslog with the 'afpd' process tag (path varies by distribution). Detection approach: (1) Enumerate symlinks in all AFP share directories with `find -type l -ls`; flag any symlink resolving outside the share boundary. (2) Monitor for file read or write events on sensitive paths (/etc/passwd, /etc/shadow, SSH key directories, application config files) correlated with afpd process activity; use auditd rules: `-w /etc/passwd -p r -k afp_sensitive_read` and equivalent for other targets. (3) Alert on authentication events to AFP port 548/TCP from unexpected source IPs or at unusual hours (aligns with NIST AU-6, AU-2). (4) If a SIEM is in use, create a rule correlating afpd process file-access events with paths outside the configured share root. Behavioral indicator: symlinks created inside an AFP share that resolve to absolute paths outside that share root are a direct exploitation indicator. No CVE-specific IOCs (hashes, IPs, domains) are publicly attributed at this time.

Framework Mappings

MITRE-ATTACK

- **T1083** — File and Directory Discovery
- **T1565.001** — Stored Data Manipulation

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1083	File and Directory Discovery	Discovery
T1565.001	Stored Data Manipulation	Impact

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-44051	T1
CVE-2026-44051 Common Vulnerabilities and Exposures | SUSE	https://www.suse.com/zh-cn/security/cve/CVE-2026-44051.html	T3
CVE-2026-44551 Detail - NVD	http://nvd.nist.gov/vuln/detail/CVE-2026-44551	T1
CVE-2026-44051 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-44051	T3

Source	URL	Tier
Linux Distros Unpatched Vulnerability : CVE-2026-44051 | Tenable®	https://www.tenable.com/plugins/nessus/314884	**T3**

Generated 2026-05-24 06:20 UTC by TJS Security Command Center