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

CVE-2026-44049: An out-of-bounds write due to improper null termination in convert_charset() in Netatalk 2.0.4 throu...

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0216
Type	CVE Vulnerability
CVE ID	CVE-2026-44049
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0006 (20th percentile)
Affected Products	Netatalk 2.0.4 through 4.4.2
Published	2026-05-21T08:16:20.473
Discovery Source	Nvd

Executive Summary

CVE-2026-44049 is a high-severity out-of-bounds write vulnerability in Netatalk, an open-source Apple Filing Protocol server used to share files between Linux/Unix systems and Apple devices. A remote authenticated attacker can send crafted character input to trigger arbitrary code execution or crash the service. Organizations running Netatalk versions 2.0.4 through 4.4.2 for file sharing in mixed Apple-Linux environments should treat this as a priority patching item.

Technical Analysis

CVE-2026-44049 affects Netatalk versions 2.0.4 through 4.4.2. The vulnerability resides in the convert_charset() function, which fails to properly null-terminate character data during charset conversion operations. This improper null termination enables a remote authenticated attacker to write beyond the bounds of an allocated buffer (CWE-787: Out-of-Bounds Write). Successful exploitation can result in arbitrary code execution or denial of service. The attack vector is network-based and requires authentication, reducing but not eliminating risk. CVSS v3.1 base score is 7.5 (High). EPSS score is 0.00065 (20th percentile), indicating low current exploitation activity. MITRE ATT&CK mappings include T1190 (Exploit Public-Facing Application) and T1499 (Endpoint Denial of Service). No CISA KEV listing as of this report. Vector string pending NVD publication.

Action Checklist

1. Step 1: Containment, Identify all systems running Netatalk 2.0.4 through 4.4.2 using your asset inventory (CIS 1.1). Immediately restrict network access to AFP ports (TCP 548, TCP/UDP 427) at the perimeter firewall and host-based firewall (CIS 4.4, CIS 4.5) to authenticated internal users only. Remove internet-facing exposure of Netatalk services if present. Disable the service on any system where AFP file sharing is not operationally required.
2. Step 2: Detection, Query your SIEM for connection attempts to TCP port 548 from external or unexpected source IPs. Review Netatalk daemon logs (typically /var/log/netatalk/ or syslog, depending on distribution) for anomalous charset conversion errors, segfaults, or unexpected process terminations. Cross-reference authentication logs for unusual authenticated sessions preceding service crashes. Use your vulnerability scanner (e.g., Tenable Nessus) to confirm affected version presence across the environment (NIST SI-4, CIS 8.2).
3. Step 3: Eradication, Apply the vendor-released patch or upgrade Netatalk to a version beyond 4.4.2 once available from the official Netatalk project (https://netatalk.io). For Linux distributions, apply the distribution-provided update via your automated patch management process (CIS 7.3, CIS 7.4). If no patch is available at time of remediation, disable the convert_charset() code path if the vendor provides a configuration workaround, or disable Netatalk entirely until a fix is released. Document any exception with a risk acceptance sign-off.
4. Step 4: Recovery, After patching, verify the installed Netatalk version is outside the affected range (2.0.4-4.4.2). Restart the Netatalk service and validate AFP connectivity for authorized users. Monitor Netatalk daemon logs and system logs for 72 hours post-patch for residual anomalies. Confirm host-based firewall rules remain in place and that no unauthorized AFP exposure was re-introduced (NIST SI-4, AU-6).
5. Step 5: Post-Incident, Review your asset inventory process to confirm all Netatalk instances were identified promptly (CIS 1.1, CIS 2.1). Assess whether authenticated remote access controls for AFP services meet least-privilege standards (NIST AC-6, D3-UAP). Evaluate whether network segmentation would limit blast radius if a similar authenticated-RCE vulnerability emerges in file-sharing services. Add Netatalk to your recurring vulnerability scan scope if not already included (CIS 7.1).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and legal/compliance immediately if forensic review of /var/log/auth.log and packet captures reveals that an authenticated AFP session preceded an afpd crash or core dump during the exposure window, indicating a likely exploitation attempt against CVE-2026-44049 that may constitute a reportable incident under applicable data protection regulations if the Netatalk share hosted PII or regulated data.

Recovery Notes	After patching to a Netatalk version beyond 4.4.2, verify the fixed binary's SHA-256 hash against the vendor-published checksum before restarting AFP services. Monitor /var/log/syslog and journalctl output for afpd segfault or charset conversion error recurrence for a minimum of 72 hours post-patch, as residual exploitation attempts may continue against the now-patched service from threat actors who identified the target during the exposure window. Confirm that AFP shares are re-enabled only for operationally required volumes and that the authenticated user list has been reviewed and trimmed to least privilege before returning Netatalk to production.
Forensic Artifacts	afpd core dump files (typically in /var/crash/, /tmp/, or the afpd working directory) — generated by the out-of-bounds write in convert_charset() causing SIGSEGV in the afpd process; these preserve the memory state at the moment of exploit and may contain attacker-controlled payload bytes | /var/log/syslog or /var/log/messages entries containing 'afpd' AND 'segfault' or 'killed' — the convert_charset() out-of-bounds write will produce kernel-logged segfault entries for the afpd PID correlated with the time of the malicious authenticated AFP request | Packet captures on TCP port 548 containing DSI (Data Stream Interface) or AFP FPLoginExt request frames with non-standard or multi-byte charset strings in the username or volume name fields — these are the network-layer artifact of the crafted character input used to trigger the vulnerability | /var/log/auth.log entries for PAM or AFP authentication events immediately preceding afpd crashes — CVE-2026-44049 requires an authenticated attacker, so the credential used to authenticate before triggering the overflow is a critical forensic artifact linking the exploit to a specific account | Pre-patch afpd binary preserved at /usr/sbin/afpd with SHA-256 hash documented — enables post-incident binary diffing against the patched version to confirm the convert_charset() function was indeed modified, and supports chain-of-custody documentation if exploitation is confirmed

Per-Action IR Details

Step 1: Containment — Identify all systems running Netatalk 2.0.4 through 4.4.2 using your asset inventory (CIS 1.1). Immediately restrict network access to AFP ports (TCP 548, TCP/UDP 427) at the perimeter firewall and host-based firewall (CIS 4.4, CIS 4.5) to authenticated internal users only. Remove internet-facing exposure of Netatalk services if present. Disable the service on any system where AFP file sharing is not operationally required.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run 'nmap -p 548,427 -sV ' across all internal subnets to identify live Netatalk instances without a CMDB. On each Linux host, run 'systemctl status netatalk' or 'ps aux | grep netatalk' to confirm the running version. Block AFP ports immediately with iptables: 'iptables -I INPUT -p tcp --dport 548 -j DROP && iptables -I INPUT -p udp --dport 427 -j DROP' and save with 'iptables-save > /etc/iptables/rules.v4'. For macOS clients that rely on AFP, assess whether SMB can serve as a temporary replacement before disabling Netatalk.

Evidence: Before restricting ports, capture current active AFP sessions and network state: run 'ss -tnp sport = :548' to document which source IPs have active connections to the Netatalk daemon. Capture 'netstat -anp | grep afpd' output. Record the exact Netatalk version per host via 'netatalk --version' or 'dpkg -l netatalk' / 'rpm -q netatalk'. Preserve /etc/netatalk/afp.conf and /etc/netatalk/AppleVolumes.default to document what shares were exposed and to which clients.

Step 2: Detection — Query your SIEM for connection attempts to TCP port 548 from external or unexpected source IPs. Review Netatalk daemon logs (typically /var/log/netatalk/ or syslog, depending on distribution) for

anomalous charset conversion errors, segfaults, or unexpected process terminations. Cross-reference authentication logs for unusual authenticated sessions preceding service crashes. Use your vulnerability scanner (e.g., Tenable Nessus plugin 314822) to confirm affected version presence across the environment (NIST SI-4, CIS 8.2).

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST RA-5 (Vulnerability Monitoring and Scanning), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, parse Netatalk logs directly: 'grep -iE "charset|convert_charset|segfault|SIGSEGV|core dumped" /var/log/syslog /var/log/netatalk/*.log' to identify crash artifacts consistent with the out-of-bounds write in convert_charset(). Check for core dumps left by afpd crashes: 'find / -name "core" -o -name "core.afpd*" 2>/dev/null'. Use 'last' and 'lastlog' to identify authenticated sessions that correlate temporally with service crashes. Deploy a Sigma rule targeting process crash events for afpd: match on syslog entries containing 'afpd' AND 'segfault' within a 5-minute window of an authenticated AFP login. Capture full packet traces on port 548 with 'tcpdump -i eth0 -w /tmp/afp_capture.pcap port 548' to preserve exploit attempt payloads for later analysis.

Evidence: The convert_charset() out-of-bounds write will manifest as afpd process crashes (SIGSEGV) immediately after an authenticated DSI/AFP request containing multi-byte or non-standard charset strings. Collect: (1) /var/log/syslog or /var/log/messages entries with 'afpd' and 'segfault' or 'killed' within the timeframe of suspicious sessions; (2) any core dump files generated by afpd, typically in the afpd working directory or /var/crash/; (3) packet captures showing malformed AFP FPLoginExt or DSI Write commands with unexpected character encoding payloads; (4) authentication logs (/var/log/auth.log) for the authenticated user accounts active immediately before each crash, to identify which credential was used as the pre-authentication stepping stone for the exploit.

Step 3: Eradication — Apply the vendor-released patch or upgrade Netatalk to a version beyond 4.4.2 once available from the official Netatalk project (https://netatalk.io). For Linux distributions, apply the distribution-provided update via your automated patch management process (CIS 7.3, CIS 7.4). If no patch is available at time of remediation, disable the convert_charset() code path if the vendor provides a configuration workaround, or disable Netatalk entirely until a fix is released. Document any exception with a risk acceptance sign-off.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: If no patch is yet available, immediately disable the Netatalk service on all affected hosts: 'systemctl stop netatalk && systemctl disable netatalk'. If AFP file sharing is operationally required and cannot be disabled, assess whether the distribution's netatalk package supports a charset restriction in afp.conf — set 'afpcharset = UTF8' and 'maccharset = MAC_ROMAN' to reduce the charset conversion attack surface, documenting this as an unvalidated workaround pending vendor guidance. Track patch availability by monitoring the official Netatalk GitHub repository (https://github.com/Netatalk/netatalk) releases page and the distribution's security advisory feed (e.g., Debian DSA, Ubuntu USN, RHEL RHSA). Record version pre- and post-patch in a change log tied to each affected host.

Evidence: Before applying the patch, preserve the vulnerable binary for forensic comparison: 'cp /usr/sbin/afpd /forensics/afpd.pre-patch.$(hostname).$(date +%Y%m%d)'. Record the SHA-256 hash of the pre-patch binary: 'sha256sum /usr/sbin/afpd'. If a prior exploitation attempt is suspected, collect any web or network logs showing authenticated AFP sessions and preserve the afpd core dumps before the service is restarted, as patching and restarting will overwrite runtime state. Capture 'dpkg -l netatalk' or 'rpm -qi netatalk' output pre- and post-patch to document the version transition.

Step 4: Recovery — After patching, verify the installed Netatalk version is outside the affected range (2.0.4–4.4.2). Restart the Netatalk service and validate AFP connectivity for authorized users. Monitor Netatalk daemon logs and system logs for 72 hours post-patch for residual anomalies. Confirm host-based firewall rules remain in place and that no unauthorized AFP exposure was re-introduced (NIST SI-4, AU-6).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CP-10 (System Recovery and Reconstitution), NIST CM-6 (Configuration Settings), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Verify the patched version with 'netatalk --version' and compare against the fixed release identifier from the Netatalk changelog. Confirm the service is running cleanly: 'systemctl status netatalk' and 'journalctl -u netatalk -n 100 --no-pager' to review the first 100 post-restart log entries for segfault or charset error recurrence. Set a cron job to alert on afpd crashes during the 72-hour window: 'grep -c "afpd.*segfault" /var/log/syslog' run every 15 minutes via cron, outputting to a monitoring file. Re-run 'nmap -p 548,427 ' from an external vantage point to confirm AFP is no longer reachable from outside the authorized network segment.

Evidence: During the 72-hour monitoring window, collect: (1) continuous output of 'journalctl -u netatalk -f' piped to a timestamped log file to capture any post-patch anomalies; (2) periodic 'ss -tnp sport = :548' snapshots every 30 minutes to verify only expected client IPs are maintaining AFP sessions; (3) /var/log/auth.log entries for AFP authentication events to confirm no unexpected accounts are authenticating; (4) iptables rule listing ('iptables -L -n -v') snapshots before and after service restart to confirm firewall posture was not altered by the Netatalk service restart scripts.

Step 5: Post-Incident — Review your asset inventory process to confirm all Netatalk instances were identified promptly (CIS 1.1, CIS 2.1). Assess whether authenticated remote access controls for AFP services meet least-privilege standards (NIST AC-6, D3-UAP). Evaluate whether network segmentation would limit blast radius if a similar authenticated-RCE vulnerability emerges in file-sharing services. Add Netatalk to your recurring vulnerability scan scope if not already included (CIS 7.1).

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), 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)

Compensating: Conduct a lessons-learned session using the gap between when CVE-2026-44049 was published and when all Netatalk instances were identified as the primary metric. If that gap exceeded 72 hours, add Netatalk and other AFP-related packages to a weekly 'dpkg -l | grep netatalk' or 'rpm -qa | grep netatalk' scan script run against all Linux hosts via SSH in a cron job. Write a persistent YARA rule to detect netatalk binaries in the affected version range for future asset discovery scans. Formally document which user accounts have AFP authentication rights and revoke any that are not operationally required, reducing the authenticated-attacker pool that CVE-2026-44049 requires for exploitation.

Evidence: For the post-incident review record, assemble: (1) a timeline mapping the CVE publication date against the date each Netatalk instance was identified, contained, and patched — gaps highlight asset inventory and patch process deficiencies; (2) a complete list of AFP-authenticated accounts that were active during the exposure window, sourced from /var/log/auth.log, to assess whether any account may have been used as the exploit's required authenticated session; (3) network flow records (or tcpdump captures) from the exposure window showing all source IPs that connected to TCP 548, to determine whether any external or unexpected hosts reached the vulnerable service before containment.

Detection Guidance

Query SIEM or log aggregation for connections to TCP port 548 (AFP) from external IP ranges or any IP outside expected client subnets. Look for Netatalk process crashes, segmentation faults, or unexpected restarts in /var/log/syslog, /var/log/messages, or the Netatalk-specific log path configured in afpd.conf. Alert on authentication events to the AFP service from accounts not in your approved file-sharing user group (NIST AU-6, AU-2). Run vulnerability scanner queries to identify unpatched Netatalk versions across Linux endpoints. No public IOCs (hashes, IPs, domains) are associated with active exploitation of this CVE at the time of this report; EPSS score (0.00065) indicates no observed exploitation in the wild. Behavioral hunting focus: repeated connection attempts followed by service termination events on AFP-serving hosts.

Framework Mappings

MITRE-ATTACK

- **T1499** — Endpoint Denial of Service
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **SC-5** — Denial-of-Service Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-16** — Memory Protection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures

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
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-44049	T1

Source	URL	Tier
Linux Distros Unpatched Vulnerability : CVE-2026-44049 | Tenable®	https://www.tenable.com/plugins/nessus/314822	T3
CVE-2026-42249 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-42249	T1
CVE-2026-44049 - Out-of-bounds write in convert_charset() null ...	https://cvefeed.io/vuln/detail/CVE-2026-44049	T3
CVE-2026-31049: Hostbill RCE Vulnerability - SentinelOne	https://www.sentinelone.com/vulnerability-database/cve-2026-31049/	T3

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