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

CVE-2026-44048: A stack-based buffer overflow via UCS-2 type confusion in convert_charset() in Netatalk 2.0.4 throug...

CVE VULNERABILITY | HIGH | CVSS 8.8

SCC Item ID	SCC-CVE-2026-0214
Type	CVE Vulnerability
CVE ID	CVE-2026-44048
Severity	HIGH
CVSS Base Score	8.8
EPSS Score	0.0014 (33th percentile)
Affected Products	Netatalk 2.0.4 through 4.4.2
Published	2026-05-21T08:16:20.360
Discovery Source	Nvd

Executive Summary

A stack-based buffer overflow vulnerability in Netatalk (CVE-2026-44048) allows a remote authenticated attacker to execute arbitrary code on systems running Netatalk versions 2.0.4 through 4.4.2. Netatalk is widely deployed on Linux and Unix servers to provide Apple Filing Protocol (AFP) file sharing with macOS clients. Organizations using Netatalk for mixed-OS file sharing environments face direct risk of system compromise and service disruption.

Technical Analysis

CVE-2026-44048 is a CWE-121 (Stack-based Buffer Overflow) in the convert_charset() function within Netatalk versions 2.0.4 through 4.4.2. The flaw originates from UCS-2 type confusion: when the function processes character set conversions, improper handling of UCS-2 encoded data allows an attacker to write beyond the bounds of a stack-allocated buffer. Authentication is required, placing the attack surface at any session-authenticated AFP client. Successful exploitation can yield arbitrary code execution with the privileges of the Netatalk process, or trigger a denial of service via process crash. CVSS base score is 8.8 (High). EPSS score is 0.00137 (33rd percentile), indicating low current exploitation probability. No CISA KEV listing as of this writing. MITRE ATT&CK techniques T1190 (Exploit Public-Facing Application) and T1059 (Command and Scripting Interpreter) are relevant to post-exploitation paths. CVSS vector is pending NVD publication. Patch status should be confirmed against the Netatalk project's official release channel.

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). Restrict AFP port 548 (TCP) at the perimeter firewall and on host-based firewalls (CIS 4.4, CIS 4.5, NIST SC-7) to block remote access until patching is complete. If AFP is not required by any business function, disable the service immediately.
2. Step 2: Detection. Query asset inventory and CMDB for Netatalk installations across Linux and Unix hosts. On Linux, run 'dpkg -l | grep netatalk' or 'rpm -qa | grep netatalk' across your fleet. Review authentication logs for AFP session activity (event source: netatalk/afpd log, typically at /var/log/syslog or /var/log/afpd.log) for anomalous authenticated sessions, unexpected process spawning from the afpd process, or crash/core dump events consistent with a buffer overflow (NIST AU-6, CIS 8.2). No public IOCs or exploit signatures are available at this time.
3. Step 3: Eradication. Upgrade Netatalk to a version above 4.4.2 once the project releases a patched build. Check the official Netatalk project (https://netatalk.io, verify URL resolves to current project) and your Linux distribution's security advisories (SUSE, Debian, Ubuntu channels) for the patched package. If no patch is yet available, disable or uninstall Netatalk on non-essential systems (NIST CM-7, CIS 2.2, CIS 2.3). Document any exceptions with a risk acceptance record.
4. Step 4: Recovery. After applying the patch, verify the installed Netatalk version matches the patched release. Re-enable AFP service only on systems with a documented business need. Confirm AFP port 548 is firewalled to authorized subnets only (NIST AC-17, NIST SC-7). Resume monitoring afpd logs for anomalous behavior. Validate that no unauthorized accounts were created or persistence mechanisms installed during any potential exploitation window (NIST AC-2, NIST IR-4).
5. Step 5: Post-Incident. Review whether authenticated AFP access is appropriately scoped; limit AFP credentials to the minimum required user set (NIST AC-6, CIS 5.4). Evaluate whether privileged network services like AFP require additional access controls or network segmentation (NIST AC-4). Add Netatalk version detection to your recurring vulnerability scan profile (CIS 7.1, CIS 7.3). Document the control gap: asset inventory processes should have flagged this legacy AFP service proactively.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and legal/privacy counsel immediately if afpd process tree analysis, core dump review, or account audits reveal evidence of successful RCE or unauthorized access — particularly if AFP-shared volumes contain PII, PHI, or regulated data triggering breach notification obligations under HIPAA, GDPR, or applicable state law.
Recovery Notes	After patching to the Netatalk release that addresses CVE-2026-44048, restrict AFP access to authorized macOS client subnets via firewall ACL rather than relying solely on afpd authentication, since the vulnerability is exploitable by remote authenticated users. Monitor afpd logs and host process trees continuously for a minimum of 30 days post-recovery for signs of delayed persistence (scheduled tasks, modified startup scripts, or implanted SUID binaries) that may have been installed during the exposure window. Validate that the patched afpd binary's SHA-256 checksum matches the distribution's published value before declaring recovery complete.

Forensic Artifacts	/var/log/afpd.log or /var/log/syslog (afpd entries) — the convert_charset() stack overflow exploit will appear as malformed AFP protocol requests (FPLoginExt or charset-handling commands) immediately preceding an afpd crash or anomalous child process spawn; correlate source IP and authenticated user against known macOS client inventory | Core dump files in /var/crash, /tmp, or afpd working directory — a failed or partially successful exploit of the CVE-2026-44048 buffer overflow will produce a core dump referencing the vulnerable convert_charset() stack frame; analyze with 'gdb /usr/sbin/afpd ' to confirm overflow in convert_charset() | Process accounting records ('lastcomm' or /var/log/pacct if psacct enabled) — successful RCE via afpd will manifest as shell processes (/bin/sh, /bin/bash) with afpd as parent PID, which is never legitimate normal behavior for the afpd daemon | Network packet capture on TCP/548 — the UCS-2 type confusion trigger in convert_charset() will appear as AFP protocol messages with oversized or malformed character set conversion data; capture with 'tcpdump -i -w /evidence/afp-traffic.pcap tcp port 548' and analyze in Wireshark using the AFP dissector to identify crafted charset payloads | /etc/passwd, /etc/shadow, /etc/cron.d/*, and SUID binary listing timestamped against afpd.conf modification time — post-exploitation persistence on a compromised Netatalk host would most likely involve local account creation or a cron-based backdoor installed by the shell spawned from the overflowed afpd process

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). Restrict AFP port 548 (TCP) at the perimeter firewall and on host-based firewalls (CIS 4.4, CIS 4.5, NIST SC-7) to block remote access until patching is complete. If AFP is not required by any business function, disable the service immediately.

NIST Phase: Containment

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

Controls: NIST SC-7 (Boundary Protection), NIST IR-4 (Incident Handling), 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: Use nmap to enumerate AFP listeners across your RFC 1918 ranges: 'nmap -p 548 --open -sV 192.168.0.0/16' — any host returning 'afp' or 'netatalk' on TCP/548 is a candidate. Block port 548 at the host with 'iptables -I INPUT -p tcp --dport 548 -j DROP && iptables -I OUTPUT -p tcp --sport 548 -j DROP', then make persistent via iptables-save. Stop the afpd daemon immediately: 'systemctl stop netatalk && systemctl disable netatalk'. For macOS clients that will lose AFP connectivity, coordinate with end users before disabling — Finder will lose mapped shares.

Evidence: Before blocking, capture a netstat snapshot of active AFP sessions to identify any attacker-controlled sessions already established: 'ss -tnp sport = :548' or 'netstat -tnp | grep :548'. Record all remote IP addresses currently connected to afpd — these are containment-critical indicators if exploitation has already occurred. Also run 'ps aux | grep afpd' to capture current afpd process tree and any anomalous child processes spawned by the afpd parent, which would indicate a successful RCE via the convert_charset() overflow.

Step 2: Detection — Query asset inventory and CMDB for Netatalk installations across Linux and Unix hosts. On Linux, run 'dpkg -l | grep netatalk' or 'rpm -qa | grep netatalk' across your fleet. Review authentication logs for AFP session activity (event source: netatalk/afpd log, typically at /var/log/syslog or /var/log/afpd.log) for anomalous authenticated sessions, unexpected process spawning from the afpd process, or crash/core dump events consistent with a buffer overflow (NIST AU-6, CIS 8.2). No public IOCs or exploit signatures are available at this time.

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), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy osquery on Netatalk hosts and run: 'SELECT pid, name, parent, cmdline FROM processes WHERE parent IN (SELECT pid FROM processes WHERE name = "afpd")' — any non-afpd child process spawned by afpd (e.g., /bin/sh, /bin/bash, python) indicates successful RCE via the stack overflow. For crash detection without a SIEM, configure a cron job to watch for core dumps: 'find /var/crash /tmp /var/tmp -name "core*" -newer /etc/netatalk/afpd.conf -ls' run every 15 minutes. Enable afpd debug logging temporarily by adding '-d' to the afpd startup flags and redirecting stderr to /var/log/afpd-debug.log to capture malformed UCS-2 charset conversion attempts that precede exploitation.

Evidence: Collect the following before any remediation: (1) /var/log/afpd.log or /var/log/syslog filtered for 'afpd' entries — look for authentication events from unexpected source IPs or service accounts not associated with macOS clients; (2) Core dump files in /var/crash, /tmp, or the working directory of the afpd process — a successful stack overflow in convert_charset() will produce a crash dump before a stable shell is achieved; (3) Process accounting logs ('lastcomm' output if psacct/acct is enabled) for shell processes with afpd as parent or ancestor; (4) /var/log/auth.log for new local account creation or sudo usage in the same timeframe as AFP session anomalies; (5) Network capture on TCP/548 — the UCS-2 type confusion exploit will manifest as oversized or malformed FPLoginExt or FPSetFileDirParms AFP commands containing crafted charset strings.

Step 3: Eradication — Upgrade Netatalk to a version above 4.4.2 once the project releases a patched build. Monitor the official Netatalk project repository (https://netatalk.io — note: verify this URL resolves to the current project; this is provided from training-data knowledge, not active verification) and your Linux distribution's security advisories (e.g., SUSE, Debian, Ubuntu security channels) for the patched package. If no patch is yet available, disable or uninstall Netatalk on non-essential systems (NIST CM-7, CIS 2.2, CIS 2.3). Document any exceptions with a risk acceptance record.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST CM-7 (Least Functionality), NIST SI-2 (Flaw Remediation), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If the upstream Netatalk patch has not yet shipped, compile Netatalk from source with stack protection flags as a temporary hardening measure: add '-fstack-protector-strong -D_FORTIFY_SOURCE=2' to CFLAGS before building — this will not eliminate the CVE-2026-44048 vulnerability but raises the exploitation bar by triggering stack canary faults on overflow attempts, producing a crash rather than code execution. For Debian/Ubuntu, watch the security tracker at https://security-tracker.debian.org/tracker/CVE-2026-44048 (verify URL; provided from training-data pattern, not active verification) and configure 'unattended-upgrades' to auto-apply security updates in the 'netatalk' package namespace once a patched package appears. For RPM-based systems, use 'dnf updateinfo list security | grep netatalk' to poll for an advisory.

Evidence: Before uninstalling or upgrading, preserve a forensic image of the vulnerable afpd binary ('sha256sum /usr/sbin/afpd > /evidence/afpd-pre-patch.sha256; cp /usr/sbin/afpd /evidence/afpd-$(date +%Y%m%d).bin') to support later analysis confirming the vulnerable code path in convert_charset() was present. Also capture the full afpd configuration ('cp /etc/netatalk/afpd.conf /evidence/' and 'cp -r /etc/netatalk/ /evidence/netatalk-config-$(date +%Y%m%d)/') to document the attack surface that was exposed. If any core dumps exist, preserve them before the upgrade overwrites the binary they reference.

Step 4: Recovery — After applying the patch, verify the installed Netatalk version matches the patched release. Re-enable AFP service only on systems with a documented business need. Confirm AFP port 548 is firewalled to authorized subnets only (NIST AC-17, NIST SC-7). Resume monitoring afpd logs for anomalous behavior. Validate that no unauthorized accounts were created or persistence mechanisms installed during any potential exploitation window (NIST AC-2, NIST IR-4).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AC-17 (Remote Access), NIST SC-7 (Boundary Protection), NIST IR-4 (Incident Handling), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Run a diff of /etc/passwd and /etc/shadow against a known-good baseline to detect accounts created during any exploitation window: 'diff /evidence/passwd-baseline /etc/passwd'. Check for SUID binaries modified or created recently: 'find / -perm -4000 -newer /etc/netatalk/afpd.conf -ls 2>/dev/null'. Audit cron jobs for persistence: 'for u in $(cut -f1 -d: /etc/passwd); do crontab -l -u $u 2>/dev/null | grep -v "^#" && echo "user: $u"; done'. Inspect afpd volumes for web shells or unusual executables: 'find $(grep "path" /etc/netatalk/AppleVolumes.default | awk "{print $1}") -name "*.sh" -o -name "*.py" -newer /etc/netatalk/afpd.conf 2>/dev/null'.

Evidence: Prior to re-enabling afpd, collect: (1) Current /etc/passwd, /etc/shadow, /etc/sudoers, and /etc/crontab as post-incident baselines; (2) 'last' and 'lastlog' output to identify any local logins that occurred on Netatalk hosts during the exposure window — an attacker who achieved RCE via the buffer overflow would likely escalate to an interactive shell session; (3) Output of 'ss -tnlp' after patching to confirm no unexpected listeners were introduced during the exploitation window; (4) Verify afpd binary integrity post-patch: 'sha256sum /usr/sbin/afpd' and compare against the distribution's published checksum for the patched package.

Step 5: Post-Incident — Review whether authenticated AFP access is appropriately scoped; limit AFP credentials to the minimum required user set (NIST AC-6, CIS 5.4). Evaluate whether privileged network services like AFP require additional access controls or network segmentation (NIST AC-4). Add Netatalk version detection to your recurring vulnerability scan profile (CIS 7.1, CIS 7.3). Document the control gap: asset inventory processes should have flagged this legacy AFP service proactively.

NIST Phase: Post Incident

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Write a Sigma rule targeting the specific afpd crash pattern for future detection: match on syslog messages containing 'afpd' AND ('segfault' OR 'stack smashing' OR 'core dumped') and forward to any log aggregator. Add a Nessus or OpenVAS check using the plugin pattern 'netatalk' with version comparison logic against the patched version threshold — OpenVAS has community NVTs for AFP service detection. For network segmentation without enterprise tooling, implement a dedicated VLAN for AFP file servers and enforce inter-VLAN ACLs allowing only TCP/548 from authorized macOS client subnet ranges. Document AFP as a monitored legacy protocol in your risk register with a quarterly review trigger.

Evidence: For the lessons-learned record: compile the full timeline from the first authenticated AFP session in the exposure window to containment, using afpd log timestamps; document which asset inventory or CMDB process failed to flag Netatalk as a monitored software package subject to vulnerability scanning; record whether any CVSS 8.8 HIGH advisory for a network-accessible service would have triggered an emergency patching SLA under existing policy — if not, this is a policy gap requiring remediation. Retain all collected forensic artifacts (core dumps, afpd binaries, log exports) for a minimum of 90 days or per your retention policy under NIST AU-11 (Audit Record Retention).

Detection Guidance

No public exploit code or IOCs are associated with CVE-2026-44048 at this time. Detection should focus on identifying vulnerable installations and monitoring for exploitation indicators at the process level. Query package managers across Linux/Unix hosts for Netatalk versions 2.0.4 through 4.4.2 ('dpkg -l netatalk', 'rpm -qa netatalk'). Monitor /var/log/afpd.log and syslog for: (1) afpd process crashes or core dumps, which may indicate failed exploitation attempts; (2) unexpected child processes spawned from afpd, which may indicate successful code execution; (3) authenticated AFP sessions from unusual source IPs or outside business hours (NIST AU-6,

NIST SI-4, CIS 8.2). If your SIEM ingests AFP session logs, alert on afpd spawning shells (e.g., /bin/sh, /bin/bash) or network utilities (curl, wget, nc). Behavioral detection aligned to MITRE T1190 and T1059 is recommended on hosts running the affected service. No confirmed exploit signatures, hashes, or network IOCs are available from the referenced sources.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter

NIST-800-53R5

- **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
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-44048	T1
CVE-2026-44048 Common Vulnerabilities and Exposures - SUSE	https://www.suse.com/security/cve/CVE-2026-44048.html	T3

Source	URL	Tier
CVE-2026-44048 | Mondoo Vulnerability Intelligence	https://mondoo.com/vulnerability-intelligence/vulnerability/CVE-202...	T3
CVE-2026-44048 - Stack buffer overflow via UCS-2 type confusion ...	https://cvefeed.io/vuln/detail/CVE-2026-44048	T3
CVE-2026-44048 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-44048	T3

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