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

CVE-2026-44052: Netatalk 2.1.0 through 4.4.2 inserts LDAP simple-bind passwords into log output in cleartext, which ...

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0217
Type	CVE Vulnerability
CVE ID	CVE-2026-44052
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0003 (9th percentile)
Affected Products	Netatalk 2.1.0 through 4.4.2
Published	2026-05-21T08:16:20.800
Discovery Source	Nvd

Executive Summary

Netatalk versions 2.1.0 through 4.4.2 write LDAP authentication passwords to log files in cleartext, exposing valid directory credentials to anyone with log read access. Organizations running Netatalk for Apple Filing Protocol (AFP) file sharing on Linux or Unix systems are at risk of credential theft that could enable attackers to move laterally through Active Directory or LDAP environments. The exposure is credential theft via log file access, not remote code execution; the downstream impact on identity infrastructure can be significant.

Technical Analysis

CVE-2026-44052 affects Netatalk versions 2.1.0 through 4.4.2. The flaw is classified as CWE-532 (Insertion of Sensitive Information into Log File). When Netatalk performs LDAP simple-bind authentication, it logs the bind password in cleartext within application log output. An attacker with read access to the affected log files, whether through a compromised service account, misconfigured log permissions, or log aggregation pipeline access, can recover valid LDAP credentials. Exploitation maps to MITRE ATT&CK T1552.001 (Credentials in Files) and T1078 (Valid Accounts). No network-level exploit is required; the attack surface is the log file itself. CVSS base score is 7.5 (High). EPSS score is 0.00031 (9.19th percentile), indicating low current exploitation activity. No CISA KEV listing as of the configuration date. Patch status should be confirmed against the Netatalk project's

official advisory; upgrade to a version beyond 4.4.2 once available.

Action Checklist

1. Step 1: Containment, Identify all systems running Netatalk 2.1.0 through 4.4.2 using your asset inventory (CIS 1.1). Immediately restrict read access to Netatalk log files to root and dedicated service accounts only. Review log file permissions with 'ls -la' on default log paths (typically /var/log/netatalk/ or configured log destination). If logs are shipped to a SIEM or log aggregation platform, restrict access to the Netatalk log source to authorized SOC personnel only (NIST AC-3).
2. Step 2: Detection, Search aggregated logs for Netatalk LDAP bind events. Query for log entries containing 'LDAP' and 'bind' or 'password' in the Netatalk log stream. Audit who has read access to Netatalk log files and directories (NIST AU-9). Review LDAP/Active Directory authentication logs for anomalous bind activity from service accounts associated with Netatalk, look for off-hours logins, access from unexpected source IPs, or privilege escalation events following Netatalk log access (NIST AU-6). Monitor local account activity on Netatalk hosts to flag unusual privilege changes or enumeration (NIST SI-4).
3. Step 3: Eradication, Upgrade Netatalk to a version that resolves CVE-2026-44052, per the official Netatalk project advisory (check https://netatalk.io for the patched release). If no patch is available yet, disable LDAP simple-bind in the Netatalk configuration and switch to a more secure bind method, or disable LDAP authentication entirely if operationally feasible. Apply the principle of least privilege to Netatalk's service account (NIST AC-6; CIS 5.4).
4. Step 4: Recovery, After patching, rotate all LDAP credentials that were used by Netatalk for simple-bind authentication (NIST IA-4). Treat any exposed LDAP bind account as compromised. Audit LDAP directory access logs for the full window the vulnerable version was in production. Verify the patched version no longer writes credentials to logs by reviewing log output after a test bind. Re-confirm log file permissions are correctly restricted (NIST AU-9). Monitor LDAP authentication for 30 days post-remediation for residual anomalies (NIST SI-4).
5. Step 5: Post-Incident, Review log sanitization practices across all services that authenticate to LDAP or Active Directory (NIST AU-2, AU-3). Assess whether other services use LDAP simple-bind and whether those credentials also appear in logs. Implement a log content inspection control to detect credential patterns in log output as part of your detection engineering program. Document this gap against CWE-532 in your risk register and reference CIS 8.2 and NIST AU-9 for control improvement priorities.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to incident commander and directory services owner immediately if LDAP/AD authentication logs show any successful bind or privileged account activity from the Netatalk service account outside of its normal operational pattern during the exposure window, or if the Netatalk bind account holds elevated directory permissions (e.g., Domain Admins, Account Operators, or read access to password attributes) that would amplify the blast radius beyond AFP file service authentication.

Recovery Notes	After credential rotation and patching, monitor the Netatalk LDAP bind account in Active Directory or OpenLDAP for 30 days for authentication attempts from any source other than the Netatalk service host IP — any such attempt indicates the exposed cleartext credential has been captured and is being replayed by a threat actor. Verify AFP service functionality by confirming client mount operations succeed post-patch and post-credential rotation, and spot-check '/var/log/netatalk/afpd.log' daily for the first week to confirm no regression to credential-logging behavior. If your organization is subject to GDPR, HIPAA, or SOC 2 obligations, assess whether the LDAP bind account had read access to personal data attributes in the directory and document that assessment in the incident record before closing.
Forensic Artifacts	Netatalk AFP daemon log (/var/log/netatalk/afpd.log or syslog-routed equivalent): primary artifact containing the cleartext LDAP simple-bind password strings written by CVE-2026-44052; preserve with 'sha256sum' hash before any log rotation occurs. | Netatalk configuration file (/etc/netatalk/afp.conf or /etc/atalk/afpd.conf): documents the LDAP bind DN, configured log destination, and authentication method in use — establishes the scope of credential exposure and whether simple-bind was explicitly configured. | Linux auth log (/var/log/auth.log or /var/log/secure): records local user access to the Netatalk host that may indicate unauthorized log file reads by a local user who obtained the cleartext password from afpd.log. | Active Directory or OpenLDAP authentication logs (Windows Security Event IDs 4624, 4625, 4648, 4768, 4769 for AD; /var/log/slapd.log for OpenLDAP): reveals whether the exposed Netatalk LDAP bind credential was used for lateral movement or unauthorized directory queries during the exposure window. | Linux audit log (/var/log/audit/audit.log via auditd, filtered for OPEN and READ syscalls against Netatalk log file paths): identifies which users or processes accessed the credential-bearing log files, establishing whether exfiltration of the cleartext password occurred and by whom.

Per-Action IR Details

Step 1: Containment — Identify all systems running Netatalk 2.1.0 through 4.4.2 using your asset inventory (CIS 1.1). Immediately restrict read access to Netatalk log files to root and dedicated service accounts only. Review log file permissions with 'ls -la' on default log paths (typically /var/log/netatalk/ or configured log destination). If logs are shipped to a SIEM or log aggregation platform, restrict access to the Netatalk log source to authorized SOC personnel only (NIST AC-3).

NIST Phase: Containment

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AU-9 (Protection of Audit Information), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 3.3 (Configure Data Access Control Lists)

Compensating: Run 'find /var/log/netatalk/ -type f -ls' and 'stat /var/log/netatalk/*.log' to enumerate current permissions. Immediately execute 'chmod 640 /var/log/netatalk/*.log && chown root:adm /var/log/netatalk/*.log' to restrict read access. Use 'grep -r "netatalk" /etc/rsyslog.conf /etc/rsyslog.d/ /etc/syslog-ng/syslog-ng.conf' to identify if logs are forwarded to any remote destination and manually restrict access on the receiving host. On systems using systemd-journald, run 'journalctl _COMM=netatalk | grep -i "ldap\|bind\|password"' to assess immediate exposure before log rotation occurs.

Evidence: Capture BEFORE restricting permissions: run 'ls -laR /var/log/netatalk/' and redirect output to a timestamped file to preserve the pre-remediation permission state as evidence. Collect 'last -a' and 'lastb -a' output to document recent logins to the Netatalk host. If auditd is running, preserve '/var/log/audit/audit.log' entries for file opens against Netatalk log paths using 'ausearch -f /var/log/netatalk/ --start recent'. Capture the running Netatalk configuration with 'cat /etc/netatalk/afp.conf' or 'cat /etc/atalk/afpd.conf' to document the configured log destination and LDAP bind settings before any changes are made.

Step 2: Detection — Search aggregated logs for Netatalk LDAP bind events. Query for log entries containing 'LDAP' and 'bind' or 'password' in the Netatalk log stream. Audit who has read access to Netatalk log files and directories (NIST AU-9). Review LDAP/Active Directory authentication logs for anomalous bind activity from service accounts associated with Netatalk — look for off-hours logins, access from unexpected source IPs, or privilege escalation events following Netatalk log access (NIST AU-6). Use D3-LAM (Local Account Monitoring) to flag unusual local account activity on Netatalk hosts.

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-9 (Protection of Audit Information), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: On the Netatalk host, run 'grep -Ei "ldap|bind|password|passwd" /var/log/netatalk/*.log /var/log/syslog /var/log/messages 2>/dev/null | tee /tmp/netatalk_ldap_exposure_$(date +%F).txt' to extract all credential-bearing log lines and preserve them for triage. Use 'getent passwd | awk -F: "\$3 >= 1000"' and 'getfacl /var/log/netatalk/' to enumerate all users with potential log read access. For AD/LDAP exposure assessment without a SIEM, pull OpenLDAP access logs from '/var/log/slapd.log' or query Active Directory using PowerShell: 'Get-EventLog -LogName Security -InstanceId 4768,4769,4776 | Where-Object {$_.Message -match "netatalk service account name"}' filtering for the Netatalk bind account over the full vulnerable version deployment window.

Evidence: Capture the raw Netatalk log files in their current state — specifically grep for lines matching the pattern 'ldap_simple_bind\|ldap_bind\|bindpw\|password' in '/var/log/netatalk/afpd.log', '/var/log/syslog', and any configured log destination in afp.conf. On the LDAP/AD side, extract Windows Security Event Log entries for Event ID 4624 (successful logon) and 4625 (failed logon) for the Netatalk service account, and Event ID 4768/4769 (Kerberos TGT/service ticket requests) if the account is domain-joined. Document the deployment timeline — run 'rpm -qi netatalk' or 'dpkg -l netatalk' to establish the exact installed version and installation date, which determines the credential exposure window.

Step 3: Eradication — Upgrade Netatalk to a version that resolves CVE-2026-44052, per the official Netatalk project advisory (check https://netatalk.io for the patched release). If no patch is available yet, disable LDAP simple-bind in the Netatalk configuration and switch to a more secure bind method, or disable LDAP authentication entirely if operationally feasible. Apply the principle of least privilege to Netatalk's service account (NIST AC-6; CIS 5.4).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST AC-6 (Least Privilege), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: If the patched Netatalk release is not yet available for your distribution, edit '/etc/netatalk/afp.conf' or '/etc/atalk/afpd.conf' and change the LDAP bind method from 'ldapauth = simple' to a SASL/GSSAPI bind if your directory supports it, or set 'ldapauth = none' as a temporary measure. After any configuration change, run 'systemctl restart netatalk && journalctl -u netatalk -n 50' and verify no LDAP bind passwords appear in the output. For package-managed installations, pin the patched version using 'apt-mark hold netatalk' or 'yum versionlock netatalk' post-upgrade to prevent inadvertent downgrade. Verify the installed version with 'netatalk --version' or 'afpd -V' after upgrade.

Evidence: Before patching, capture a full copy of the current Netatalk configuration files: 'cp -p /etc/netatalk/afp.conf /tmp/afp.conf.pre-patch.$(date +%F)' and preserve the output of 'netatalk --version'. After patching, run 'diff /tmp/afp.conf.pre-patch.$(date +%F) /etc/netatalk/afp.conf' to document configuration changes as part of the eradication record. Preserve the vulnerable package metadata with 'dpkg -l netatalk > /tmp/netatalk_pkg_pre_patch.txt' or 'rpm -qi netatalk > /tmp/netatalk_pkg_pre_patch.txt' for chain-of-custody documentation. Verify package integrity post-upgrade using distribution package signing verification ('dpkg -V netatalk' or 'rpm -V netatalk').

Step 4: Recovery — After patching, rotate all LDAP credentials that were used by Netatalk for simple-bind authentication (D3-CRO). Treat any exposed LDAP bind account as compromised. Audit LDAP directory access logs for the full window the vulnerable version was in production. Verify the patched version no longer writes credentials to logs by reviewing log output after a test bind. Re-confirm log file permissions are correctly restricted (NIST AU-9). Monitor LDAP authentication for 30 days post-remediation for residual anomalies (NIST SI-4).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IA-5 (Authenticator Management), NIST AU-9 (Protection of Audit Information), NIST SI-4 (System Monitoring), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Rotate the Netatalk LDAP bind account password immediately via your directory service console (ADUC, 'ldappasswd', or 'samba-tool user setpassword'). After rotation, update the credential reference in '/etc/netatalk/afp.conf' under the 'ldappasswd' directive and restart the service. Perform a functional test bind by mounting an AFP share from a test client and running 'tail -f /var/log/netatalk/afpd.log' in parallel — confirm no password string appears in the output. For 30-day post-remediation LDAP monitoring without a SIEM, schedule a daily cron job: '0 6 * * * grep -c "4625\|failed" /var/log/auth.log >> /tmp/ldap_failure_monitor.log' and review weekly for anomalous spikes tied to the Netatalk service account.

Evidence: Document the credential rotation event with timestamp and authorizing personnel as part of the incident record. Pull LDAP access logs for the full vulnerable-version deployment window — on OpenLDAP, extract from '/var/log/slapd.log' filtering on the Netatalk bind DN; on Active Directory, use 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4648 -and $_.Message -match "netatalk bind account CN"}' to identify explicit credential use events. Preserve the post-patch log sample that confirms no credential leakage as positive eradication evidence. Retain all collected evidence per your organization's IR retention policy (minimum 90 days recommended for a credential compromise event).

Step 5: Post-Incident — Review log sanitization practices across all services that authenticate to LDAP or Active Directory (NIST AU-2, AU-3). Assess whether other services use LDAP simple-bind and whether those credentials also appear in logs. Implement a log content inspection control to detect credential patterns in log output as part of your detection engineering program. Document this gap against CWE-532 in your risk register and reference CIS 8.2 and NIST AU-9 for control improvement priorities.

NIST Phase: Post Incident

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

Controls: NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), NIST AU-9 (Protection of Audit Information), NIST SI-2 (Flaw Remediation), NIST RA-3 (Risk Assessment), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run a grep sweep across all service log directories to detect CWE-532-class leakage from other LDAP-authenticating services: 'grep -rEi "ldappasswd|bindpw|bind_password|ldap_password|simple.bind" /var/log/ /etc/ 2>/dev/null | grep -v ".conf.bak"'. Write a YARA rule targeting credential strings in log files: define a rule matching patterns like 'ldap_simple_bind_s.*password' or 'bindpw\s*=\s*[^\"]+' and run it against archived log directories using 'yara -r cwe532_ldap.yar /var/log/'. Submit a Sigma rule to your detection backlog targeting Netatalk log output patterns for future prevention. Document the CWE-532 gap in your risk register with the Netatalk CVE as the triggering event, the affected asset list, and the credential rotation date as the remediation timestamp.

Evidence: Compile the full incident timeline: Netatalk version install date (from package manager history), date of CVE-2026-44052 public disclosure, date of detection, date of containment, date of patch and credential rotation. Preserve the grep output from the initial detection sweep showing credential-bearing log lines as the primary evidence of exposure scope. Retain the pre- and post-patch configuration diffs and the post-patch log verification sample. Archive the LDAP access log extracts covering the full exposure window. This evidence package supports both lessons-learned review and any regulatory notification assessment triggered by exposure of directory credentials.

Detection Guidance

Query Netatalk application logs (default path: /var/log/netatalk/ or as configured in afpd.conf) for any log entries containing the strings 'LDAP', 'ldap_simple_bind', 'bind', or 'password'. Presence of password strings in these entries confirms exposure. In your SIEM, create a search across the Netatalk log source for these patterns and flag results for immediate review. Cross-reference with LDAP/Active Directory authentication logs: look for bind events from the Netatalk service account at unusual times, from unexpected hosts, or followed by privilege escalation or lateral movement events. Map suspicious LDAP authentications to ATT&CK T1552.001 (Credentials in Files) and T1078 (Valid Accounts). Monitor local account activity on Netatalk hosts to detect privilege changes post-credential-exposure (NIST SI-4). Note: no network-based IOC signatures are expected for this vulnerability, the attack surface is file system access, not network traffic.

Framework Mappings

MITRE-ATTACK

- **T1552.001** — Credentials In Files
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC6.3** — Authorizes, modifies, or removes access

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1552.001	Credentials In Files	Credential-Access

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-44052	T1
CVE-2026-44052 Detail - NVD	http://nvd.nist.gov/vuln/detail/CVE-2026-44052	T1
CVE-2026-44052 Common Vulnerabilities and Exposures - SUSE	https://www.suse.com/security/cve/CVE-2026-44052.html	T3
CVE-2026-44052 | Mondoo Vulnerability Intelligence	https://mondoo.com/vulnerability-intelligence/vulnerability/CVE-202...	T3
CVE-2026-44052 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-44052	T3

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