INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-13 18:55 UTC

CVE-2026-45185: Unauthenticated RCE in Exim Targets GnuTLS Builds Across Debian and Ubuntu Deployments

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0172
Type	CVE Vulnerability
CVE ID	CVE-2026-45185
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.0006 (18th percentile)
Affected Products	Exim 4.97 through 4.99.2 (GnuTLS builds with STARTTLS and CHUNKING enabled) on Debian, Ubuntu, and other Linux/Unix distributions; patched in Exim 4.99.3
Published	2026-05-13T16:23:50
Discovery Source	Rss

Executive Summary

A critical unauthenticated remote code execution vulnerability in Exim mail server (CVE-2026-45185) allows attackers to fully compromise any internet-facing mail server running affected GnuTLS builds without credentials or prior access. Exim is the default mail transfer agent on Debian and Ubuntu, meaning a significant share of enterprise, hosting, and government mail infrastructure is exposed. A public proof-of-concept exploit is circulating, and the window between disclosure and active weaponization is narrow.

Technical Analysis

CVE-2026-45185 is a use-after-free vulnerability (CWE-416) with a secondary code injection dimension (CWE-94) affecting Exim versions 4.97 through 4.99.2 compiled with GnuTLS (as opposed to OpenSSL builds). Exploitation requires the target to advertise both STARTTLS and CHUNKING in its SMTP capability response, the default configuration on Debian and Ubuntu deployments. The flaw arises from improper memory management at the intersection of TLS handshake processing and SMTP CHUNKING command handling; a remote, unauthenticated attacker can trigger the use-after-free condition to gain arbitrary code execution as the Exim process owner (typically the 'Debian-exim' user, which often has elevated mail-handling privileges). A public proof-of-concept exploit is available, materially compressing the exploitation timeline. CVSS base score:

9.5. EPSS: 0.0059% (low current exploitation probability, though PoC availability typically accelerates this). Exim 4.99.3, released 2026-05-13, contains the patch. Relevant MITRE ATT&CK techniques: T1190 (Exploit Public-Facing Application), T1210 (Exploitation of Remote Services), T1203 (Exploitation for Client Execution), T1059 (Command and Scripting Interpreter), T1071.003 (Application Layer Protocol: Mail Protocols), T1133 (External Remote Services). No CISA KEV entry as of configuration date.

Action Checklist

1. Containment: Identify all Exim instances running versions 4.97-4.99.2 in your environment using package managers (dpkg -l exim4 on Debian/Ubuntu; rpm -qa | grep exim on RHEL-family). For GnuTLS builds specifically, run: exim --version | grep GnuTLS. If patching is not immediately possible, temporarily disable CHUNKING by adding 'chunking_advertise_hosts =' (empty) in the Exim main configuration to remove the exploitable condition. Restrict SMTP access to known sender IPs where operationally feasible.
2. Detection: Query mail logs (/var/log/exim4/mainlog or /var/log/exim/mainlog) for anomalous SMTP sessions combining STARTTLS negotiation with BDAT (CHUNKING) commands from external IPs, especially sessions that terminate abnormally or produce unexpected process spawns. Monitor for unexpected child processes spawned by the Exim parent PID using auditd or EDR process-tree telemetry. Watch for outbound connections initiated by the Exim process to external IPs; legitimate Exim processes do not initiate outbound non-mail connections. SIEM query concept: alert on process creation events where parent process name = 'exim' and child process is a shell (sh, bash, dash) or network utility (curl, wget, nc).
3. Eradication: Upgrade Exim to version 4.99.3 on all affected systems. On Debian/Ubuntu: apt-get update && apt-get install --only-upgrade exim4. Confirm the installed version with exim --version. If the distribution package has not yet been updated to 4.99.3, apply the patch from the Exim project release repository (https://www.exim.org/exim-html-current/doc/html/spec_html/ch-building_and_installing_exim.html) or disable GnuTLS CHUNKING interaction as a temporary mitigation. Do not rely solely on network-layer controls; the code path must be patched or disabled.
4. Recovery: After patching, verify Exim is running the patched version (exim --version) and restart the service to confirm clean startup. Send test mail flows through the system and validate delivery logs show normal behavior. Re-enable any temporarily restricted SMTP access rules only after patch confirmation. Monitor mail logs and process telemetry for 72 hours post-patch for any signs of prior compromise; a successful exploitation may have left persistence mechanisms (cron jobs, SSH keys, modified Exim configuration files).
5. Post-Incident: This vulnerability exposes two recurring control gaps: (1) patch lag on default-installed infrastructure components - Exim ships as default on Debian/Ubuntu and may not be actively managed if the organization does not operate a deliberate mail server. Audit for 'default-on' services across your Linux fleet. (2) Absence of egress filtering on mail server hosts - a compromised Exim process initiating outbound connections should be detectable and blockable. Implement host-level egress controls and process-based network monitoring on mail infrastructure. Map findings to NIST SP 800-53 controls SI-2 (Flaw Remediation), CM-7 (Least Functionality), and SC-7 (Boundary Protection).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and legal/privacy counsel immediately if auditd or mainlog evidence shows a successful Exim child-shell spawn (BDAT-triggered RCE) on any host processing PII, PHI, or regulated data, or if unauthorized SSH keys or cron persistence are discovered on mail infrastructure, as these conditions indicate confirmed breach and may trigger breach notification obligations under GDPR, HIPAA, or applicable state law.
Recovery Notes	After confirming Exim 4.99.3 is installed and 'debsums -c exim4' returns clean, run a full 72-hour monitoring window on both /var/log/exim4/mainlog and auditd process-creation events before declaring recovery complete, as a successful pre-patch exploitation may have staged persistence (SSH keys, cron jobs, or modified Exim router/transport configs) that survives the package upgrade. Re-enable any temporarily blocked SMTP sender IPs only after verifying no anomalous Exim child processes were recorded during the monitoring window. If any persistence artifacts are found, treat the host as fully compromised, reimage from a known-good baseline, and restore mail configuration from a pre-incident backup predating the earliest suspicious mainlog entry.
Forensic Artifacts	/var/log/exim4/mainlog — Search for SMTP session records containing both 'TLS' and 'BDAT' in the same session ID, sessions from external IPs that show GnuTLS negotiation followed by abnormal termination (no corresponding delivery '=>' record), and any session where the remote host issues BDAT without a prior successful EHLO/MAIL FROM sequence, as this pattern is specific to CVE-2026-45185 exploitation attempts. | auditd SYSCALL execve records in /var/log/audit/audit.log — Filter for execve events where ppid matches the Exim master or delivery process PID; a successful CVE-2026-45185 exploit would manifest here as sh, bash, dash, curl, wget, python, or nc spawned as a direct child of the Exim process under the Debian-exim service account UID. | Exim spool directory /var/spool/exim4/ — Examine for unexpected files, setuid binaries, or scripts dropped by the exploit payload; the Exim process writes to this directory under its service account and an attacker achieving RCE would likely use it as a writable staging area for persistence payloads. | /etc/cron.d/, /var/spool/cron/crontabs/Debian-exim, and /var/spool/exim4/.ssh/authorized_keys — These are the highest-priority persistence locations for an attacker who obtained the Debian-exim service account via CVE-2026-45185 RCE; presence of any entries added after the earliest suspicious mainlog timestamp is a confirmed compromise indicator. | Memory capture of the running Exim process (via 'gcore $(pgrep -o exim)' or LiME kernel module for full RAM) if exploitation is suspected but not confirmed — the CVE-2026-45185 exploit operates through a GnuTLS buffer condition during STARTTLS/BDAT interaction, and shellcode or injected payload artifacts may be recoverable from heap memory of the Exim process before a restart flushes them.

Per-Action IR Details

Containment — Identify all Exim instances running versions 4.97–4.99.2 in your environment using package managers (dpkg -l exim4 on Debian/Ubuntu; rpm -qa | grep exim on RHEL-family). For GnuTLS builds specifically, run: exim --version | grep GnuTLS. If patching is not immediately possible, temporarily disable CHUNKING by adding 'chunking_advertise_hosts =' (empty) in the Exim main configuration to remove the exploitable condition. Restrict SMTP access to known sender IPs where operationally feasible.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run 'dpkg -l exim4 | grep exim4' and 'exim --version | grep -i gnutls' across the fleet via parallel SSH: 'for h in $(cat mail_hosts.txt); do ssh $h "exim --version 2>&1 | grep -i gnutls && dpkg -l exim4 | grep exim4"; done'. Apply CHUNKING disable immediately by appending 'chunking_advertise_hosts =' to /etc/exim4/exim4.conf.template

and restarting Exim: 'systemctl restart exim4'. Use iptables or ufw to whitelist known sending MX IPs on port 25: 'ufw default deny incoming && ufw allow from to any port 25'.

Evidence: Before disabling CHUNKING or restricting SMTP, capture: (1) a full snapshot of the running Exim process tree via 'ps auxf > /tmp/exim_proctree_$(date +%s).txt'; (2) active network connections from Exim PID via 'ss -tnp | grep exim > /tmp/exim_netstate_$(date +%s).txt'; (3) a copy of the current Exim configuration at /etc/exim4/exim4.conf.template and /etc/exim4/conf.d/ to establish pre-change baseline; (4) current /var/log/exim4/mainlog entries covering the past 72 hours, focusing on BDAT command sequences and any sessions that show GnuTLS handshake followed by abnormal session termination.

Detection — Query mail logs (/var/log/exim4/mainlog or /var/log/exim/mainlog) for anomalous SMTP sessions combining STARTTLS negotiation with BDAT (CHUNKING) commands from external IPs, especially sessions that terminate abnormally or produce unexpected process spawns. Monitor for unexpected child processes spawned by the Exim parent PID using auditd or EDR process-tree telemetry. Watch for outbound connections initiated by the Exim process to external IPs — legitimate Exim processes do not initiate outbound non-mail connections. SIEM query concept: alert on process creation events where parent process name = 'exim' and child process is a shell (sh, bash, dash) or network utility (curl, wget, nc).

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-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Enable auditd rules targeting Exim process spawns: 'auditctl -a always,exit -F arch=b64 -S execve -F ppid=$(pgrep -o exim) -k exim_child_exec'. Parse mainlog for BDAT sessions from external IPs using: 'grep -E "BDAT|chunking" /var/log/exim4/mainlog | grep -v "<= " | awk \'{ print $1, $2, $3, $NF }\'". Detect unexpected Exim child processes without auditd using a cron-based snapshot: 'watch -n 5 "ps --ppid $(pgrep -o exim) -o pid,ppid,cmd"'. For network egress detection, run 'ss -tnp | grep exim' every 60 seconds via cron and alert on any destination port other than 25/465/587. Deploy the public Sigma rule for Exim shell spawn (search community.sigma.hq.io for 'exim' process creation rules) converted to grep-compatible format.

Evidence: Preserve before any log rotation or system change: (1) /var/log/exim4/mainlog and /var/log/exim4/mainlog.1 — search for log lines containing 'BDAT' or 'chunking' co-occurring with 'TLS' in the same session ID, and session records showing 'H=' (remote host) entries followed by no corresponding delivery record; (2) auditd log /var/log/audit/audit.log filtered for SYSCALL execve events where ppid resolves to an Exim PID — exploit success would show sh, bash, dash, curl, wget, or nc spawned as direct Exim children; (3) /var/log/syslog entries timestamped within the SMTP session window for unexpected setuid, setgid, or privilege escalation events; (4) 'ss -tnp' or 'netstat -tnp' output captured at time of anomaly showing Exim-owned sockets with non-SMTP destination ports.

Eradication — Upgrade Exim to version 4.99.3 on all affected systems. On Debian/Ubuntu: apt-get update && apt-get install --only-upgrade exim4. Confirm the installed version with exim --version. If the distribution package has not yet been updated to 4.99.3, apply the upstream source patch from the official Exim project (https://www.exim.org) or disable GnuTLS CHUNKING interaction as a temporary mitigation. Do not rely solely on network-layer controls; the code path must be patched or disabled.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), NIST SI-7 (Software, Firmware, and Information Integrity), 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: If the distro package repo has not yet published Exim 4.99.3, pin the CHUNKING disable mitigation and build from upstream source: download the 4.99.3 tarball from https://www.exim.org/mirrors.html, verify the SHA-256 checksum published in the Exim release announcement, then compile with 'make install' targeting the existing Exim install prefix. Post-install, confirm the GnuTLS build identifier is present and version is 4.99.3 with 'exim --version'. Validate the patched code path by running 'openssl s_client -starttls smtp -connect localhost:25' and issuing

a manual BDAT command to confirm the server returns an error or does not advertise CHUNKING in EHLO response.

Evidence: Before applying the patch, capture: (1) SHA-256 hash of the existing Exim binary ('sha256sum $(which exim)') to establish a pre-patch integrity baseline for later comparison and forensic chain of custody; (2) full output of 'dpkg -l exim4' and 'apt-cache policy exim4' to document the vulnerable version installed and the repo state at time of remediation; (3) a diff of /etc/exim4/ configuration directory against your known-good configuration backup to detect any attacker-modified Exim config that could survive a package upgrade; (4) check for attacker-planted setuid binaries in Exim's working directories: 'find /var/spool/exim4 /var/log/exim4 /tmp -perm /4000 -o -perm /2000 2>/dev/null'.

Recovery — After patching, verify Exim is running the patched version (exim --version) and restart the service to confirm clean startup. Send test mail flows through the system and validate delivery logs show normal behavior. Re-enable any temporarily restricted SMTP access rules only after patch confirmation. Monitor mail logs and process telemetry for 72 hours post-patch for any signs of prior compromise — a successful exploitation may have left persistence mechanisms (cron jobs, SSH keys, modified Exim configuration files).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Verify service integrity post-patch with: 'debsums exim4' (Debian/Ubuntu) to compare installed Exim package file hashes against the dpkg database and detect any attacker-modified Exim binaries or configs. Hunt for persistence left by a pre-patch exploitation: 'crontab -l -u Debian-exim; cat /var/spool/cron/crontabs/Debian-exim 2>/dev/null' to check the Exim service account crontab; 'find /home /root /var/spool/exim4 -name authorized_keys -newer /var/log/exim4/mainlog.1' to detect SSH keys added during the exploit window; 'find /etc/exim4 -newer /var/cache/apt/pkgcache.bin -type f' to identify config files modified after the last apt run. Send a test message via 'exim -bt test@example.com && echo test | exim -v test@yourdomain.com' and verify mainlog shows a clean STARTTLS handshake without BDAT anomalies.

Evidence: Document the recovery state by capturing: (1) 'exim --version' output with timestamp to confirm 4.99.3 is active; (2) 'debsums -c exim4' output showing no modified package files; (3) full listing of /etc/exim4/ with mtimes ('ls -la /etc/exim4/') compared against pre-incident baseline; (4) /root/.ssh/authorized_keys and /home/*/.ssh/authorized_keys and /var/spool/exim4/.ssh/ checked for unauthorized keys added during the exploitation window; (5) 72-hour mainlog tail with grep for any BDAT or child-shell-spawn patterns matching the pre-patch detection signatures to confirm no residual attacker activity.

Post-Incident — This vulnerability exposes two recurring control gaps: (1) patch lag on default-installed infrastructure components — Exim ships as default on Debian/Ubuntu and may not be actively managed if the organization does not operate a deliberate mail server. Audit for 'default-on' services across your Linux fleet. (2) Absence of egress filtering on mail server hosts — a compromised Exim process initiating outbound connections should be detectable and blockable. Implement host-level egress controls and process-based network monitoring on mail infrastructure. Map findings to NIST SP 800-53 controls SI-2 (Flaw Remediation), CM-7 (Least Functionality), and SC-7 (Boundary Protection).

NIST Phase: Post Incident

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

Controls: NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), NIST SC-7 (Boundary Protection), NIST IR-4 (Incident Handling), NIST AU-2 (Event Logging), 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), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Audit for default-on Exim across the Linux fleet using: 'for h in $(cat linux_hosts.txt); do ssh $h "dpkg -l exim4 2>/dev/null | grep -q exim && echo $h: EXIM INSTALLED"; done'. Enumerate services not actively managed by tagging all running SMTP listeners: 'ss -tlnp | grep :25' across all hosts. Implement process-level egress control on mail servers using iptables owner module to restrict outbound connections to Exim's service account (typically Debian-exim

UID): 'iptables -A OUTPUT -m owner --uid-owner Debian-exim ! -p tcp --dport 25 -j LOG --log-prefix "EXIM_EGRESS_ANOMALY: "' followed by a DROP rule. Deploy the MITRE ATT&CK-aligned Sigma rule for T1059.004 (Unix Shell spawned by mail server process) using sigma-cli to convert to auditd or syslog format for ongoing detection.

Evidence: For lessons-learned documentation and control gap evidence, preserve: (1) the full asset inventory gap report showing Exim instances not tracked in the CMDB or vulnerability management platform — this directly evidences the CIS 1.1 and CIS 2.1 control failure; (2) firewall/iptables rule export from all mail server hosts at time of incident showing absence of process-level egress controls, evidencing the SC-7 gap; (3) patch timeline artifact — date of CVE-2026-45185 disclosure versus date Exim 4.99.3 appeared in apt repos versus date applied in your environment — to measure patch lag against your SI-2 SLA; (4) auditd or syslog records from the 72-hour post-patch monitoring window confirming absence or presence of residual Exim child-process anomalies.

Detection Guidance

Primary detection surface is Exim mail logs combined with host process telemetry. In Exim mainlog, look for SMTP sessions from external IPs that complete a STARTTLS handshake followed by BDAT commands and then produce log anomalies (connection resets, unexpected deferrals, or no subsequent delivery log entry). These alone are not conclusive but warrant investigation. On the host, use auditd EXECVE rules or EDR process-tree monitoring to alert on shell or interpreter processes (bash, sh, python, perl) spawned as children of the Exim daemon process; this is a high-fidelity indicator of post-exploitation command execution (MITRE T1059). Also monitor for file write events in /var/spool/exim, /etc/cron*, ~/.ssh/authorized_keys, and /tmp from the Exim process owner UID. For network-level detection, watch for outbound TCP connections on non-standard ports initiated by the Exim process; legitimate Exim only connects outbound on port 25/587 to other mail servers. Snort/Suricata rules targeting malformed BDAT command sequences in STARTTLS SMTP sessions may provide additional coverage once community signatures are published. Note: EPSS is currently 0.0059% (0.18th percentile), indicating low observed exploitation in the wild as of scoring date, but PoC availability makes rapid escalation likely.

Framework Mappings

MITRE-ATTACK

- **T1071.003** — Mail Protocols
- **T1210** — Exploitation of Remote Services
- **T1133** — External Remote Services
- **T1203** — Exploitation for Client Execution
- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems

- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality
- **SI-10** — Information Input Validation
- **SI-16** — Memory Protection
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

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

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071.003	Mail Protocols	Command-And-Control
T1210	Exploitation of Remote Services	Lateral-Movement
T1133	External Remote Services	Persistence
T1203	Exploitation for Client Execution	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-critical-exim-ma...	T3
CVE-2026-45185 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-45185	T1
Daily CyberSecurity • Zero-hour alerts. Unmatched analysis.	https://securityonline.info/	T3
March 2026 Threat Report: Critical CVEs - Greenbone	https://www.greenbone.net/en/blog/march-2026-threat-report-new-crit...	T3
CVE-2026-25185: Windows Shell Link Spoofing Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2026-25185/	T3

Generated 2026-05-13 18:55 UTC by TJS Security Command Center