INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-19 13:51 UTC

SEPPMail Secure E-Mail Gateway: Seven Vulnerabilities Enable Full Appliance Compromise, Patch to 15.0.4 Required

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0193
Type	CVE Vulnerability
CVE ID	CVE-2026-2743, CVE-2026-7864, CVE-2026-44125, CVE-2026-44126, CVE-2026-44127, CVE-2026-44128, CVE-2026-44129, CVE-2026-27441
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.0057 (69th percentile)
Affected Products	SEPPMail Secure E-Mail Gateway, all versions prior to 15.0.4
Published	2026-05-19T05:23:15
Discovery Source	Rss

Executive Summary

InfoGuard Labs disclosed seven vulnerabilities in SEPPMail Secure E-Mail Gateway, including a critical path traversal flaw and multiple unauthenticated remote code execution vectors, affecting all versions prior to 15.0.4. The aggregate CVSS severity is 9.5. A publicly documented exploit chain allows an unauthenticated attacker to take full control of the appliance and intercept all mail traffic it processes. Organizations running SEPPMail must upgrade to version 15.0.4 immediately; prior partial patches (15.0.2.1 through 15.0.3) do not fully remediate the risk.

Technical Analysis

InfoGuard Labs disclosed seven vulnerabilities in SEPPMail Secure E-Mail Gateway (all versions prior to 15.0.4) affecting the LFT (Large File Transfer) feature and the GINA UI. The vulnerability set includes: a critical path traversal (CWE-22, CVE-2026-2743), insecure deserialization (CWE-502, CVE-2026-7864), eval injection (CWE-95, CVE-2026-44127), server-side template injection (CWE-1336, CVE-2026-44128), missing authorization (CWE-862, CVE-2026-44125 / CVE-2026-44126), and information disclosure (CWE-200, CVE-2026-44129 / CVE-2026-27441). Multiple vectors are unauthenticated and remotely exploitable. InfoGuard Labs has publicly documented a chained exploit path achieving complete appliance takeover and full mail traffic interception. Versions 15.0.2.1 through 15.0.3 received partial patches; full remediation requires upgrade to

15.0.4. Per-CVE CVSS scores and CWE mappings should be confirmed against individual NVD records (NVD CVE-2026-2743 page is the authoritative T1 source; verify URL resolves in your environment). The aggregate CVSS estimate of 9.5 is derived from the disclosed vulnerability set; individual scores may vary. MITRE ATT&CK techniques applicable to this chain include T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), T1059.003 (Windows Command Shell), T1548 (Abuse Elevation Control Mechanism), T1114 (Email Collection), T1557 (Adversary-in-the-Middle), T1565 (Data Manipulation), and T1083 (File and Directory Discovery). Source: InfoGuard Labs advisory and NVD.

Action Checklist

1. Step 1: Containment, Identify all SEPPMail Secure E-Mail Gateway instances in your environment running versions prior to 15.0.4. If immediate upgrade is not possible, restrict internet-facing access to the appliance at the network perimeter and disable the LFT (Large File Transfer) feature and GINA UI until patched. Consult the InfoGuard Labs advisory for component-specific exposure detail.
2. Step 2: Detection, Review appliance access logs for unauthenticated requests targeting LFT endpoints and GINA UI paths, particularly those containing path traversal sequences (e.g., '../' patterns), unexpected deserialization payloads, or template expression syntax (e.g., '{{', '${', '#{'}). Correlate with outbound mail relay anomalies or unexpected process spawns on the appliance host. Check for unexpected administrative sessions, configuration changes post-exploitation, or log clearing/tampering (T1070.002) which may indicate post-compromise activity.
3. Step 3: Eradication, Upgrade all SEPPMail Secure E-Mail Gateway instances to version 15.0.4. Do not treat versions 15.0.2.1 through 15.0.3 as fully remediated; InfoGuard Labs confirmed those releases addressed only a subset of the disclosed vulnerabilities. Obtain the upgrade package directly from SEPPMail's official vendor channel.
4. Step 4: Recovery, After upgrading to 15.0.4, verify appliance integrity: confirm version string, review configuration files for unauthorized changes, audit active mail routing rules, and validate that no unauthorized accounts or SSH keys were added. Monitor mail flow logs for evidence of interception or manipulation (T1114, T1557) for at least 30 days post-remediation. Reset credentials for any accounts that authenticated against the appliance prior to patching.
5. Step 5: Post-Incident, Review network segmentation controls for email gateway appliances; externally accessible management interfaces and LFT/GINA components should sit behind WAF or IP allowlist controls. Assess whether a vulnerability disclosure monitoring process would have surfaced this advisory earlier. Add SEPPMail to your asset inventory's patch-tracking scope and establish a repeatable cadence for vendor advisory review.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and legal/privacy counsel immediately if log analysis confirms unauthenticated access to LFT or GINA UI endpoints with HTTP 200 responses, any evidence of mail interception or configuration modification, or if the appliance processes email containing PII/PHI subject to GDPR, HIPAA, or equivalent breach notification requirements — the CVSS 10.0 path traversal with publicly documented unauthenticated RCE chain and full appliance compromise capability warrants treating any confirmed exploitation as a notifiable incident.
Recovery Notes	After upgrading to SEPPMail 15.0.4, perform a line-by-line review of all mail routing rules, transport maps, and BCC/forwarding configurations before returning the appliance to production, as an attacker with pre-patch RCE access could have persisted silent mail forwarding rules that survive the software upgrade. Monitor mail flow logs and SMTP relay records daily for the first 30 days post-remediation, specifically for unexpected relay hops, header modifications, or envelope recipients inconsistent with sender intent (MITRE T1114, T1557). All accounts — including service accounts and API keys — that authenticated to the appliance during the exposure window (from the earliest vulnerable version deployed to the confirmed patch date) must be treated as compromised and rotated before the appliance re-enters full production service.
Forensic Artifacts	SEPPMail web application access log ('/var/log/seppmail/access.log' or equivalent Apache/nginx log): will contain path traversal sequences ('../', '%2e%2e%2f'), SSTI payloads ('{{7*7}}', '${7*7}'), and deserialization probe patterns in POST bodies targeting '/lft/' and '/gina/' URI prefixes — the primary artifact for confirming exploitation attempts and establishing the attack timeline. | SEPPMail mail relay/transport log ('/var/log/seppmail/mail.log' or Postfix/Exim main.log equivalent): post-exploitation adversary access to the appliance would enable silent BCC forwarding or transport rule injection; look for envelope-from/to mismatches, unexpected relay destinations, or new transport rules with creation timestamps after the vulnerability's public disclosure date. | Appliance filesystem artifacts — '/etc/passwd', '/etc/shadow', '/root/.ssh/authorized_keys', '/etc/cron.d/', '/tmp/', '/var/tmp/', and the SEPPMail application working directory: unauthenticated RCE on this appliance class typically results in dropped webshells, added SSH keys, or cron-based persistence; file creation timestamps in these locations post-disclosure are high-confidence indicators of compromise. | SSH authentication log ('/var/log/auth.log' or '/var/log/secure'): successful SSH logins by unexpected accounts or from unexpected source IPs following exploitation of the RCE chain would appear here; correlate with the appliance's authorized administrator list and known management IP ranges. | Network capture (tcpdump/Wireshark PCAP from the appliance's external-facing interface): unauthenticated RCE exploitation via the LFT or GINA UI path traversal/SSTI chain will produce anomalous HTTP POST requests to specific URI paths with malformed or oversized payloads; a PCAP covering the pre-patch exposure window enables reconstruction of the full exploit chain and identification of attacker infrastructure for threat intelligence purposes (MITRE T1190).

Per-Action IR Details

Step 1: Containment — Identify all SEPPMail Secure E-Mail Gateway instances in your environment running versions prior to 15.0.4. If immediate upgrade is not possible, restrict internet-facing access to the appliance at the network perimeter and disable the LFT (Large File Transfer) feature and GINA UI until patched. Consult the InfoGuard Labs advisory at labs.infoguard.ch for component-specific exposure detail.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 12.2 (Establish and Maintain a Secure Network Architecture)

Compensating: Run 'curl -s http://localhost/seppmail/version' or SSH to each appliance and check '/opt/seppmail/etc/version.txt' to enumerate installed versions without an asset management platform. Block TCP 443 and TCP 80 inbound to the appliance from any source outside your internal mail relay IPs using iptables: 'iptables -I INPUT -p tcp --dport 443 ! -s -j DROP'. Disable the LFT service via the appliance's admin CLI or by stopping the responsible process: 'systemctl stop seppmail-lft' (verify exact service name against your installed version). Document all changes with timestamps for the incident record.

Evidence: Before making any network changes, capture a full snapshot of active network connections on the appliance using 'ss -tulnp > /evidence/netstat_$(date +%s).txt' and 'netstat -anp >> /evidence/netstat_$(date +%s).txt'. Preserve the appliance's current web server access log at '/var/log/seppmail/access.log' (or equivalent path for your version) and the LFT/GINA UI access logs in their entirety — these will contain the path traversal sequences (e.g., '../../../etc/passwd') and any template injection payloads ('{{', '${') that confirm exploitation attempts. Image the appliance OS disk or snapshot the VM before any changes if compromise is suspected.

Step 2: Detection — Review appliance access logs for unauthenticated requests targeting LFT endpoints and GINA UI paths, particularly those containing path traversal sequences (e.g., '../' patterns), unexpected deserialization payloads, or template expression syntax (e.g., '{{', '${', '#{'}). Correlate with outbound mail relay anomalies or unexpected process spawns on the appliance host. Check for unexpected administrative sessions or configuration changes post-exploitation (T1070.002 — log clearing may indicate post-compromise activity).

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), MITRE ATT&CK T1190 (Exploit Public-Facing Application), MITRE ATT&CK T1059 (Command and Scripting Interpreter), MITRE ATT&CK T1070.002 (Indicator Removal: Clear Linux or Mac System Logs)

Compensating: Use 'grep -E "(\.\./|\.\.%2[Ff]|\{\{|\$\{|#\{|%7[Bb])" /var/log/seppmail/access.log' to extract path traversal and template injection candidates from the SEPPMail web access log. Pipe through 'awk' to isolate unauthenticated requests (HTTP 200/500 responses to LFT or GINA UI endpoints without a valid session cookie). For process spawn detection without EDR, deploy Sysmon on any Windows-based monitoring host forwarding logs from the appliance, or on the appliance itself if Linux-compatible; use Sigma rule 'proc_creation_lnx_webshell_spawn.yml' from the SigmaHQ repository to detect shell processes (bash, sh, python) spawned by the web service UID. Capture network traffic to/from the appliance with 'tcpdump -i eth0 -w /evidence/seppmail_$(date +%s).pcap port 443 or port 25' and analyze in Wireshark filtering on suspicious POST bodies to '/lft/' or '/gina/' URI prefixes.

Evidence: Preserve SEPPMail web server access logs ('/var/log/seppmail/access.log' or Apache/nginx equivalent) covering the full exposure window back to the last known-good state. Extract mail relay logs (typically '/var/log/seppmail/mail.log' or Postfix/Exim equivalents) and look for unexpected relay entries, mail header injection artifacts, or BCC/forwarding rules added post-exploitation (MITRE T1114). Capture '/var/log/auth.log' or '/var/log/secure' for unexpected SSH logins or sudo escalations by the web service account. Check '/etc/crontab', '/var/spool/cron/', and '/etc/cron.d/' for persistence mechanisms dropped via RCE. Review '/tmp/', '/var/tmp/', and the SEPPMail application's working directory for uploaded webshells or dropper binaries with creation timestamps falling after the vulnerability's public disclosure date.

Step 3: Eradication — Upgrade all SEPPMail Secure E-Mail Gateway instances to version 15.0.4. Do not treat versions 15.0.2.1 through 15.0.3 as fully remediated; InfoGuard Labs confirmed those releases addressed only a subset of the disclosed vulnerabilities. Obtain the upgrade package directly from SEPPMail's official vendor channel.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), 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 applying the 15.0.4 upgrade package from the official SEPPMail vendor portal, verify the package's cryptographic hash against the vendor-published checksum using 'sha256sum seppmail-15.0.4-upgrade.pkg' — do not install a package whose hash does not match, as supply-chain tampering is a realistic post-exploit scenario. If the appliance cannot be upgraded in-place due to suspected compromise, provision a clean 15.0.4 instance from a verified image, migrate only validated configuration (reviewed line-by-line for injected rules), and retire the suspect appliance. Document the version string before and after upgrade by running the appliance's built-in version check command and saving output to your incident record.

Evidence: Before patching, take a final forensic snapshot: collect '/etc/passwd' and '/etc/shadow' (for unauthorized account detection), all SSH authorized_keys files under '/root/.ssh/' and any service account home directories, the full mail routing configuration ('/etc/seppmail/' or equivalent config directory), and a list of all installed packages ('dpkg -l > /evidence/packages_pre_patch.txt' or 'rpm -qa > /evidence/packages_pre_patch.txt'). Hash all collected files with SHA-256 ('sha256sum /evidence/* > /evidence/manifest.sha256') to establish a forensic chain of custody before the upgrade modifies the system state.

Step 4: Recovery — After upgrading to 15.0.4, verify appliance integrity: confirm version string, review configuration files for unauthorized changes, audit active mail routing rules, and validate that no unauthorized accounts or SSH keys were added. Monitor mail flow logs for evidence of interception or manipulation (T1114, T1557) for at least 30 days post-remediation. Reset credentials for any accounts that authenticated against the appliance prior to patching.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-11 (Audit Record Retention), NIST IA-5 (Authenticator Management), NIST CM-6 (Configuration Settings), CIS 5.2 (Use Unique Passwords), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process), MITRE ATT&CK T1114 (Email Collection), MITRE ATT&CK T1557 (Adversary-in-the-Middle)

Compensating: Run 'diff -r /evidence/config_pre_patch/ /etc/seppmail/' to compare the pre-patch configuration snapshot against the post-upgrade state and identify any unauthorized routing rules, BCC forwarding entries, or mail relay modifications inserted during the compromise window. Audit SSH authorized_keys with 'find / -name authorized_keys -exec cat {} \; 2>/dev/null' and compare against your known-good baseline. For 30-day mail interception monitoring without a SIEM, configure a daily cron job: '0 6 * * * grep -E "(bcc|forward|redirect)" /var/log/seppmail/mail.log >> /var/log/seppmail/interception_watch.log' and review weekly. Force password resets for all SEPPMail admin accounts and any accounts whose credentials transited the appliance during the exposure window.

Evidence: Collect post-upgrade mail routing configuration in full and diff against your last known-good backup. Extract mail delivery logs for the 30-day monitoring window, flagging messages with anomalous header modifications, unexpected relay hops, or BCC recipients not present in the original envelope (indicative of T1114 silent collection). Capture '/var/log/seppmail/admin.log' or equivalent for any administrative actions taken during the suspected compromise window. Preserve all evidence collected during Steps 1-3 in an immutable, access-controlled evidence store (NIST AU-9) for potential regulatory disclosure requirements.

Step 5: Post-Incident — Review network segmentation controls for email gateway appliances; externally accessible management interfaces and LFT/GINA components should sit behind WAF or IP allowlist controls. Assess whether a vulnerability disclosure monitoring process would have surfaced this advisory earlier. Add SEPPMail to your asset inventory's patch-tracking scope and establish a repeatable cadence for vendor advisory review.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), NIST CM-8 (System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.2 (Establish and Maintain a Secure Configuration

Process for Network Infrastructure)

Compensating: Subscribe to the SEPPMail vendor security advisory RSS feed or mailing list and to InfoGuard Labs' disclosure feed (labs.infoguard.ch) to ensure future disclosures are received at time of publication rather than discovered reactively. Add SEPPMail appliance version to your osquery asset inventory using a custom query: 'SELECT * FROM file WHERE path = "/opt/seppmail/etc/version.txt";' scheduled weekly to detect version drift. Implement a WAF rule (ModSecurity or equivalent) blocking requests to '/lft/' and '/gina/' URI paths from non-allowlisted source IPs as a durable compensating control, and document it as such in your risk register pending network redesign. Conduct a 30-minute lessons-learned session using the NIST 800-61r3 §4 post-incident template and document time-to-detect, time-to-contain, and any regulatory notification obligations triggered.

Evidence: Compile the complete incident timeline from log evidence collected in Steps 1-4 — first appearance of path traversal probes in access logs, first confirmed exploitation indicator, time of containment action, and time of full remediation — to populate the post-incident report and identify detection gaps. Retain all forensic artifacts (disk images, log exports, network captures, configuration diffs) for a minimum of 12 months per NIST AU-11, or longer if regulatory obligations (e.g., GDPR breach notification, HIPAA) apply given that the SEPPMail appliance processes email which may contain PII or PHI.

Detection Guidance

Focus detection on the LFT and GINA UI components. In web/application access logs, look for: path traversal patterns ('../', '%2e%2e%2f', '%252e%252e') in request URIs; template injection syntax ('{{', '${', '#{', '<%=') in parameter values; unusually large or malformed POST bodies to deserialization endpoints (CWE-502 exploitation). At the OS/process level on the appliance, watch for unexpected child processes spawned by the mail gateway service, new cron entries, or additions to /etc/passwd or SSH authorized_keys. For T1114 (Email Collection) and T1557 (Adversary-in-the-Middle), review mail relay logs for anomalous BCC routing, unexpected forwarding rules, or duplicate delivery records. No public IOCs (IPs, domains, hashes) have been confirmed for active exploitation of this vulnerability set at time of this assessment; EPSS score of 0.57% (68th percentile) indicates this vulnerability is more likely to be exploited than 68% of other known CVEs - treat as elevated exploitation probability. Absence of confirmed IOCs may reflect early disclosure phase, not low risk.

Framework Mappings

MITRE-ATTACK

- **T1557** — Adversary-in-the-Middle
- **T1190** — Exploit Public-Facing Application
- **T1070.002** — Clear Linux or Mac System Logs
- **T1083** — File and Directory Discovery
- **T1036** — Masquerading
- **T1059.003** — Windows Command Shell
- **T1548** — Abuse Elevation Control Mechanism
- **T1565** — Data Manipulation
- **T1114** — Email Collection
- **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
- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **16.10** — Apply Secure Design Principles in Application Architectures
- **16.12** — Implement Code-Level Security Checks
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1557	Adversary-in-the-Middle	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1070.002	Clear Linux or Mac System Logs	Defense-Evasion
T1083	File and Directory Discovery	Discovery
T1036	Masquerading	Defense-Evasion
T1059.003	Windows Command Shell	Execution

Technique ID	Technique Name	Tactic
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1565	Data Manipulation	Impact
T1114	Email Collection	Collection
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/seppmail-secure-e-mail-gateway.html	T3
CVE-2026-2743 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-2743	T1
CVE-2026-34043 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2026-34043	T3
About CVE 2026-30923 and 2026-42268 | Modsecurity Project	https://modsecurity.org/20260428/about-cve-2026-30923-and-2026-42268/	T3
SeppMail Secure E-Mail Gateway: Critical RCE and LFI Vulnerabilities	https://labs.infoguard.ch/posts/seppmail_secure_e-mail_gateway_rce_...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-2743, CVE-2026-7864, CVE-...	T1

Generated 2026-05-19 13:51 UTC by TJS Security Command Center