Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Dead.Letter Walking: Unauthenticated RCE Stalks Exim Mail Servers

Date of Publication	Admiralty Code	TA Number
May 20, 2026	A1	TA2026138

Summary

First Seen: May 1, 2026
Affected Products: Exim Internet Mailer
Impact: CVE-2026-45185, known as Dead.Letter, is a critical unauthenticated remote code execution flaw in the Exim mail server, carrying a CVSS score of 9.8. The bug is a use-after-free in the BDAT message body parser that is triggered only on builds compiled with GnuTLS, which makes Debian, Ubuntu, and Debian-derived Linux distributions the primary exposure surface. An attacker needs only network access to a public-facing SMTP server on port 25, 465, or 587 to exploit it, with no credentials, user interaction, or special server configuration required. A successful exploit runs arbitrary code as the Exim service account, enabling mail theft, configuration tampering, and lateral movement. The flaw was disclosed on May 12, 2026 and is fixed in Exim 4.99.3 and matching Debian and Ubuntu packages, but public proof-of-concept code is already circulating, so urgent patching is strongly advised.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-45185	Dead.Letter (Exim Internet Mailer Use-After-Free Vulnerability)	Exim Internet Mailer	✗	✗	✓

Vulnerability Details

#1 CVE-2026-45185, nicknamed Dead.Letter, is a critical use-after-free flaw (CWE-416) in the Exim mail server. The bug lives where Exim's GnuTLS-based TLS code meets its BDAT message body parser. When a client sends a BDAT chunk inside a TLS session and the TLS layer shuts down mid-transfer, Exim frees an internal buffer called ssl_xfer_buffer but forgets to clear the pointer and forgets to reset its lower-layer receive functions. A moment later, the parser writes a single byte (a newline character) into that already-freed memory. That one stray byte corrupts heap metadata, and attackers can shape that corruption into full remote code execution.

#2 The flaw affects Exim versions 4.97 through 4.99.2, but only when the software was built with GnuTLS (USE_GNUTLS=yes). Builds linked against OpenSSL are completely safe. This means the real-world exposure sits almost entirely on Debian, Ubuntu (including 24.04 LTS), and Debian-based Linux distributions, which ship GnuTLS-linked Exim by default. Red Hat and SUSE systems, which usually use OpenSSL builds, are not affected by this specific path.

#3 Attackers do not need a username, password, or any prior access. They simply need to open a TLS connection to a public-facing SMTP server on port 25, 465, or 587 and use the standard CHUNKING (BDAT) extension. Both STARTTLS and CHUNKING are advertised by default on most Exim servers, so no special server configuration is required. The vulnerability carries a CVSS v3.1 score of 9.8 (Critical).

#4 A successful attack lets an unauthenticated remote attacker run arbitrary code as the Exim service account, which on most systems has enough privilege to bind to mail ports and read the mail spool, opening the door to mail theft, ACL tampering, and pivoting deeper into the network.

#5 The bug was discovered by XBOW Security Lab and reported to Exim on May 1, 2026. It was publicly disclosed on May 12, 2026, and is fixed in Exim 4.99.3, with matching patches available from Debian and Ubuntu. Public proof-of-concept code and detection scripts are already circulating, so patching urgently is strongly recommended.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-45185	Exim Internet Mailer 4.97 through 4.99.2 (GnuTLS builds only)	cpe:2.3:a:exim:exim:*:*:*:*:*:*:*:*	CWE-416

Recommendations

Upgrade Exim to the Patched Version Immediately: Update Exim to version 4.99.3 or later, which is the official fix released on May 12, 2026. For Debian and Ubuntu systems, install the coordinated security packages through apt-get update && apt-get install --only-upgrade exim4 and restart the Exim service. After patching, verify the running binary matches the fixed version using exim -bV rather than relying on the package version string alone.

Apply a Temporary Workaround if Patching Is Delayed: If you cannot upgrade immediately, add chunking_advertise_hosts = (with an empty value) to the main section of your Exim configuration and restart the service. This stops Exim from advertising the CHUNKING extension and blocks the BDAT attack path that triggers the vulnerability. Note that this is a stopgap, not a fix, and may affect mail delivery from senders that rely on BDAT for large messages.

Restrict Network Exposure of Mail Ports: Limit access to TCP ports 25, 465, and 587 at the firewall level to only the known relay peers, partners, and authenticated submission clients that genuinely need to reach the mail server. Internet-wide exposure of SMTP ports should be avoided wherever the business function does not require it, reducing the attack surface for this and future SMTP-layer vulnerabilities.

Inventory and Audit All Exim Deployments: Identify every internet-facing mail server in your estate, including legacy relays, acquired systems, and hosting-provider defaults that may have been forgotten. For each one, confirm the Exim version and TLS backend (GnuTLS versus OpenSSL) using exim -bV or the publicly available Dead.Letter detection scripts, since only GnuTLS builds are exposed and shadow mail infrastructure is the most common source of unpatched, vulnerable systems.

Strengthen Vulnerability Management and Service Hardening: Maintain an up-to-date inventory of mail software versions and patch levels, subscribe to upstream Exim, Debian, and Ubuntu security advisories, and integrate vulnerability detection into routine configuration management. In parallel, harden the Exim systemd service with directives such as NoNewPrivileges=yes, MemoryDenyWriteExecute=yes, ProtectSystem=strict, and PrivateTmp=yes, and confirm full ASLR (kernel.randomize_va_space=2) is enabled to limit the impact of any future memory corruption flaw in the same component.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
	T1203: Exploitation for Client Execution	
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
Discovery	T1082: System Information Discovery	

Tactic	Technique	Sub-technique
Collection	T1114: Email Collection	T1114.002: Remote Email Collection
Exfiltration	T1041: Exfiltration Over C2 Channel	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.005: Exploits
Command and Control	T1071: Application Layer Protocol	T1071.003: Mail Protocols
Impact	T1499: Endpoint Denial of Service	

Patch Link

https://exim.org/static/doc/security/EXIM-Security-2026-05-01.1/

References

https://xbow.com/blog/dead-letter-cve-2026-45185-xbow-found-rce-exim

https://www.cycognito.com/blog/emerging-threat-cve-2026-45185-exim-remote-code-execution-via-bdat-over-gnutls/

https://exim.org/static/doc/security/EXIM-Security-2026-05-01.1/

https://www.openwall.com/lists/oss-security/2026/05/12/25

https://github.com/liamromanis101/Dead.Letter-CVE-2026-45185

https://github.com/materaj2/cve-2026-45185-detection-script

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

May 20, 2026 • 09:30 AM

More at www.hivepro.com