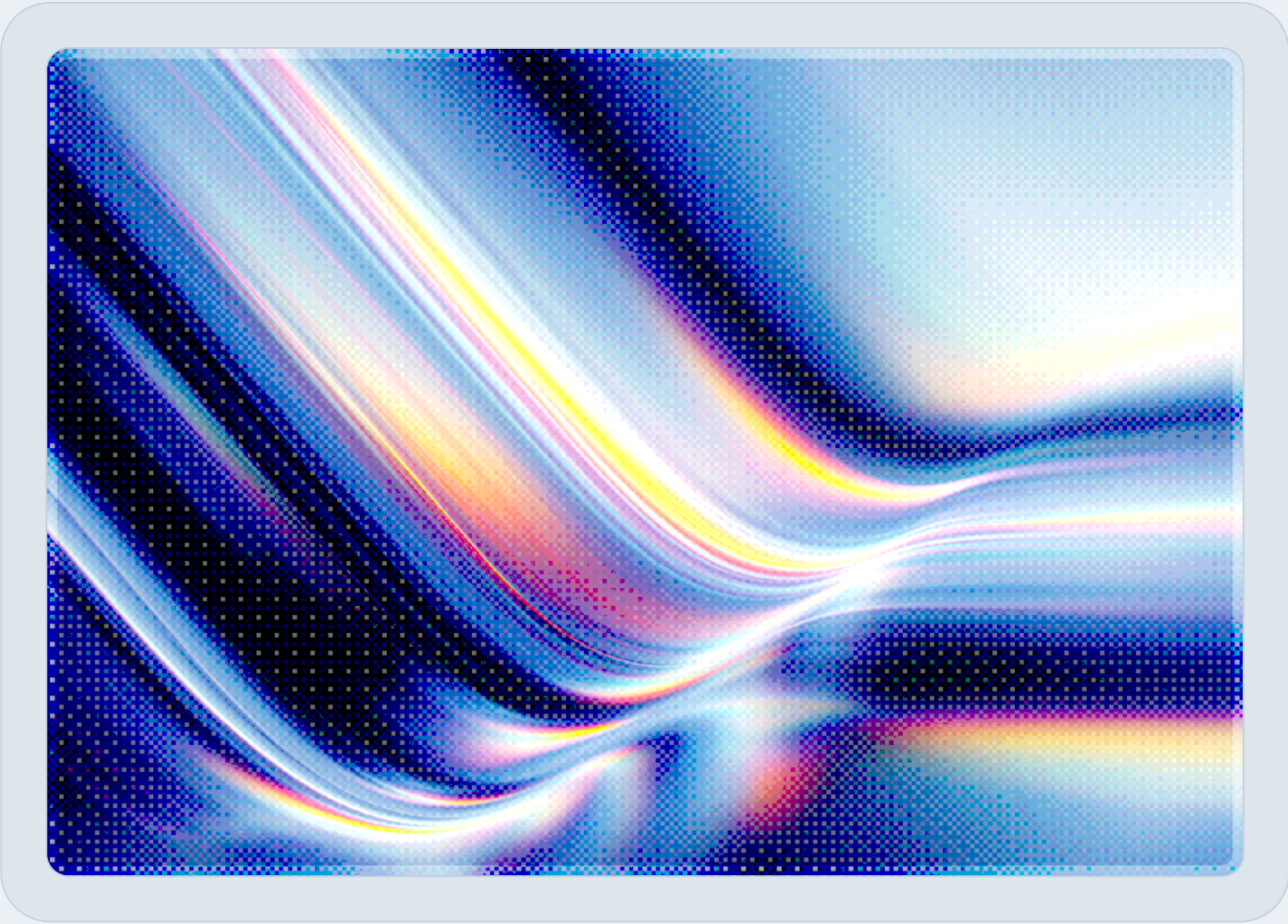
CSAI Foundation | Cloud Security Alliance

Zimbra SNMP Flaw Under Active Exploitation (CVE-2026-73570)

2026-08-26

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

- CVE-2026-73570 is an unauthenticated OS command injection flaw (CVSS 3.1: 8.9) in the optional SNMP notification component of Zimbra Collaboration Suite (ZCS), patched in version 10.1.20 on July 20, 2026, and now under active exploitation.
- The Shadowserver Foundation and CERT Polska have tracked compromises climbing from roughly 155 internet-facing instances on August 20 to at least 274 by August 22, a level that persisted with no reported decline through at least August 25, with more than 8,200 vulnerable ZCS servers still unpatched as of this writing.
- CISA added the flaw to its Known Exploited Vulnerabilities (KEV) catalog on August 21, 2026, triggering a three-day federal remediation deadline under Binding Operational Directive (BOD) 26-04.
- No named threat actor has been publicly attributed to the CVE-2026-73570 mass-exploitation campaign; this is distinct from, but occurs against the backdrop of, a documented, ongoing Russian state-backed espionage campaign against Zimbra webmail disclosed one month earlier in a joint CISA, NSA, and FBI advisory.
- Organizations running ZCS should treat any instance with the optional zimbra-snmp package installed as presumptively targeted, patch to 10.1.20 or later immediately, and separately verify they are also current on the November 2025 fix for the unrelated zero-click flaw exploited by the Russian group LAUNDRY BEAR.

Background

Zimbra Collaboration Suite is a widely deployed open-source and commercially licensed email and collaboration platform used by government agencies, defense contractors, universities, and mid-sized enterprises that prefer to self-host webmail rather than migrate to a cloud provider such as Microsoft 365 or Google Workspace. That self-hosted, internet-facing footprint has made Zimbra a recurring target for both financially motivated intrusion crews and state-sponsored espionage operations over the past several years, a pattern documented in prior reporting on the platform [1][3], and one that continued through the summer of 2026 with two separate, unrelated security incidents affecting the platform in quick succession.

The more recent of the two is CVE-2026-73570, a command injection vulnerability in the way ZCS processes SNMP notifications. The flaw exists only when an administrator has installed the optional zimbra-snmp package and enabled SNMP notifications, a non-default configuration used for infrastructure monitoring [1][2]. Because the input-sanitization failure occurs before authentication, an attacker who can reach the affected service over the network can send a specially crafted request that results in arbitrary operating system command execution as the zimbra user, with no credentials or user interaction required [1][3]. The flaw was first disclosed on June 26, 2026, and Zimbra shipped a fix roughly three weeks later in ZCS 10.1.20, released July 20, 2026 [2][3][4].

The vulnerability then sat quietly for roughly four weeks after the patch became available. That changed in mid-August, when CERT Polska flagged evidence of in-the-wild exploitation, and the Shadowserver Foundation began publishing daily scan data showing a rapidly growing population of compromised, internet-facing ZCS servers [4][5]. CISA added CVE-2026-73570 to its KEV catalog on August 21, 2026, which under the risk-based patching framework established by BOD 26-04 set a three-day remediation deadline of August 24 for U.S. federal civilian executive branch agencies [3][6]. As of that deadline, Shadowserver's scans still showed thousands of unpatched, internet-facing instances alongside several hundred confirmed compromises, illustrating the gap that persists between a KEV listing and full remediation across a large, decentralized population of self-hosted mail servers.

This SNMP flaw is not, however, the vulnerability referenced in the joint advisory that CISA, the NSA, the FBI, and international partners published on July 23, 2026, warning Zimbra customers of "ongoing Russian state-supported malicious threat activity" [7][8]. That advisory concerns a separate, earlier-disclosed flaw, CVE-2025-66376, and a distinct threat actor tracked as LAUNDRY BEAR (Microsoft's designation is Void Blizzard) [8][9]. The two campaigns are unrelated in mechanism and, to date, in attribution, but they involve the same platform, overlap in the population of exposed organizations, and together illustrate why Zimbra administrators need to track more than one active threat stream this quarter. The remainder of this note treats CVE-2026-73570 as the primary subject, then places it in the context of the LAUNDRY BEAR campaign so readers do not conflate the two.

Security Analysis

The SNMP command injection flaw and its exploitation

CVE-2026-73570 is rated CVSS 3.1 8.9, reflecting network-based, unauthenticated, low-complexity exploitation with high impact on confidentiality, integrity, and availability [2]. Public technical writeups describe the attack as a specially crafted SMTP request that triggers command execution during SNMP notification processing, giving the attacker code execution as the zimbra service account rather than

root, though that level of access is typically sufficient to read mailbox data, deploy webshells into Zimbra's Jetty application directories, or pivot further into the host [1][3]. Because the flaw requires the optional zimbra-snmp package and SNMP notifications to be enabled, exposure is narrower than it would be for a default-configuration bug, but it is far from rare in practice: Shadowserver's scanning identified more than 8,200 internet-facing ZCS instances still running versions prior to 10.1.20 as of late August, a subset of which are configured in the vulnerable state [3][5].

Exploitation activity accelerated quickly once it began. CERT Polska's initial report in mid-August prompted Shadowserver to begin daily tracking, which recorded roughly 155 compromised instances on August 20, climbing to at least 274 by August 22, a level that persisted through at least August 25 with no reported decline [4][5][10]. Shadowserver's scanning also identified a broad geographic footprint of vulnerable, internet-facing instances rather than a concentration in any single region, with roughly 4,400 exposed servers located in Europe and a similar number in Asia [10]. Guidance from CERT Polska and downstream vendor bulletins recommends checking Zimbra logs for unexpected service restarts and scanning the Jetty webapps directories and /tmp for files created within the prior thirty days as indicators of compromise [1][3].

No security vendor, government agency, or research organization has published attribution linking a specific threat actor or nation to the CVE-2026-73570 exploitation wave as of this writing. Several outlets covering the incident note, as background, that Zimbra has previously been targeted by Russian state-linked groups including APT28, APT29 (Midnight Blizzard), and Winter Vivern in earlier, unrelated campaigns, but none of that reporting extends attribution to the current SNMP-flaw exploitation [1][3]. Readers should treat the actor behind this specific campaign as unknown; the pattern is consistent with either an opportunistic criminal operation building initial access for resale, or reconnaissance by a more sophisticated actor that has not yet been identified.

The separate, confirmed Russian state-backed campaign

The joint CISA/NSA/FBI advisory published July 23, 2026, describes a materially different threat: a sustained phishing and zero-click exploitation campaign against Zimbra webmail attributed to LAUNDRY BEAR, a Russian state-supported actor Microsoft tracks as Void Blizzard [7][8][9]. That campaign exploits CVE-2025-66376, a stored cross-site scripting flaw in the classic ZCS web interface that abuses CSS @import directives and a Base64-encoded payload embedded in an SVG element's "onload" attribute. Unlike the SNMP flaw, this vulnerability requires no privileged network access and no crafted authentication-bypassing request; it triggers automatically the moment a targeted user previews a malicious email in a vulnerable webmail client, with no click required [9][11]. Using a custom exfiltration tool the advisory calls Ulej, LAUNDRY BEAR has harvested roughly ninety days of email history, session cookies, and multi-factor authentication codes from more than ten targeted organizations since at least

July 2025, concentrated among Western government agencies, defense industrial base contractors, law enforcement, and NGOs [8][9]. Zimbra patched CVE-2025-66376 in November 2025 (versions 10.1.13 and 10.0.18), and the July 2026 advisory's core message is that a meaningful population of Zimbra customers has still not applied that fix roughly eight months later [8][9].

Table 1 summarizes the two campaigns side by side to make the distinction clear for defenders who may otherwise conflate them.

Dimension	CVE-2026-73570 (SNMP command injection)	CVE-2025-66376 (zero-click XSS)
Vulnerability class	Unauthenticated OS command injection	Stored cross-site scripting via CSS/SVG payload
Trigger	Crafted SMTP request to SNMP notification handler	Victim previews malicious HTML email (no click needed)
Prerequisite	zimbra-snmp package installed, SNMP notifications enabled	Vulnerable classic webmail UI, no special configuration
CVSS 3.1	8.9	Not published in available reporting
Patched in	ZCS 10.1.20 (July 20, 2026)	ZCS 10.1.13 / 10.0.18 (November 2025)
Attribution	Unattributed as of August 26, 2026	LAUNDRY BEAR / Void Blizzard (Russia), per CISA/NSA/FBI
Objective (assessed)	Unclear; consistent with opportunistic access	Email, credential, and session-token exfiltration (espionage)
Scale confirmed	At least 274 compromised instances (Aug. 2026)	10+ organizations since July 2025

Taken together, the two incidents reinforce a single operational conclusion: an internet-facing Zimbra deployment carries risk from multiple independent threat streams simultaneously, and version currency has to be verified against each disclosed CVE individually rather than assumed from a single recent update.

Recommendations

Immediate Actions

Organizations running Zimbra Collaboration Suite should confirm their patch level against both fixes discussed in this note rather than assuming a single upgrade addresses everything. Upgrade to ZCS 10.1.20 or later to close CVE-2026-73570, and separately verify the instance is also at or above 10.1.13/10.0.18 to close CVE-2025-66376, since an organization could be current on one fix and not the other depending on when it last patched. For any instance where the zimbra-snmp package is installed, disable SNMP notifications or restrict network access to the SNMP-handling service until the upgrade is confirmed, and review /var/log/zimbra.log for unexpected service restarts and the Jetty webapps directories and /tmp for files created in the past thirty days as potential indicators of the SNMP-flaw exploitation [1][3]. Federal civilian agencies subject to BOD 26-04 should treat the August 24 KEV deadline as already passed and prioritize any remaining unpatched instances as an emergency change.

Short-Term Mitigations

Beyond patching, security teams should rotate any credentials or session tokens that may have been exposed through either vulnerability, particularly for accounts with administrative access to the Zimbra instance, and audit authentication logs for anomalous session activity predating the patch. Because the SNMP flaw grants command execution as the zimbra service account, incident responders should treat any confirmed compromise as a full mailbox-data exposure event rather than a contained service disruption, and extend log retention and review to cover at least the thirty days preceding detection. Organizations that have not yet inventoried whether the optional zimbra-snmp package is installed and enabled across their fleet should do so now, since exposure to CVE-2026-73570 depends entirely on that non-default configuration choice.

Strategic Considerations

The recurrence of serious, independently exploited vulnerabilities in Zimbra within a matter of months argues for treating self-hosted webmail as a persistently high-risk asset class warranting an accelerated internal patch SLA, similar to the treatment CSA has recommended for other frequently targeted on-premises collaboration platforms. Security teams should also build detection content specific to each disclosed Zimbra CVE rather than relying on generic web-application monitoring, since the SNMP command injection and the zero-click XSS campaign leave different forensic footprints. Finally,

organizations weighing the long-term cost of maintaining internet-facing, self-hosted collaboration infrastructure against migration to a managed or cloud-hosted alternative should factor this pattern of recurring, independently attributed exploitation into that calculus.

CSA Resource Alignment

CISA's addition of CVE-2026-73570 to the KEV catalog under the BOD 26-04 risk-based patching framework mirrors a dynamic CSA examined in detail in CISA BOD 26-04: AI Threat Forces 3-Day Critical Patch Mandate [12], which analyzed how the directive's four-variable risk matrix — public exposure, KEV listing, automatability, and technical impact — routes a critical, unauthenticated, internet-exposed vulnerability to the most urgent remediation tier regardless of the underlying platform. The same reasoning applies directly here: an unauthenticated, network-exploitable command injection in a widely deployed collaboration platform meets every criterion for the shortest BOD 26-04 remediation window, and organizations should expect similar three-day deadlines whenever comparably severe flaws in internet-facing infrastructure reach KEV status.

The pattern of a widely deployed, on-premises collaboration platform carrying a long history of KEV entries and a persistently large unpatched population is not unique to Zimbra. Microsoft SharePoint Server, another self-hosted enterprise platform with a comparable deployment footprint, has had 14 vulnerabilities added to the KEV catalog since November 2021, eight of which were also exploited in ransomware attacks, according to reporting on CISA: Microsoft SharePoint Flaw Now Exploited in Ransomware Attacks [13]. Both cases illustrate the same structural lesson: vendor patch availability does not translate quickly into fleet-wide remediation for self-hosted enterprise software, leaving a large and durable window of opportunity for opportunistic exploitation long after a fix ships.

The gap between Zimbra's July 20 patch release and confirmed active exploitation roughly four weeks later, against a backdrop of more than 8,200 vulnerable internet-facing instances still discoverable by public scanning, illustrates a broader exposure-management principle: environmental exposure and exploit signal, not static CVSS severity scores in isolation, should drive remediation prioritization, and backlogs are better tracked against CISA KEV status than against CVSS alone. That reasoning applies directly to security teams deciding how urgently to prioritize a Zimbra upgrade cycle that touches optional, non-default services many administrators may not realize are internet-reachable. Organizations mapping their vulnerability management practices to a formal controls framework should reference the vulnerability and threat management control objectives in CSA's AI Controls Matrix (AICM) v1.1 [14], which underpin the prioritization logic these examples illustrate for AI-era patch management.

References

[1] The Hacker News. "Attackers Exploit Zimbra SNMP Flaw for Unauthenticated Remote Code Execution." The Hacker News, August 2026.

[2] RedLegg. "Security Bulletin: OS Command Injection in Zimbra Collaboration Suite SNMP Notification Processing." RedLegg, August 2026.

[3] BleepingComputer. "CISA Orders Urgent Patching of Actively Exploited Zimbra Flaw." BleepingComputer, August 2026.

[4] Help Net Security. "Unpatched Zimbra Servers Are Falling to CVE-2026-73570 Attacks." Help Net Security, August 25, 2026.

[5] BleepingComputer. "Hackers Breached Over 270 Zimbra Servers in Ongoing Attacks." BleepingComputer, August 2026.

[6] CISA. "Known Exploited Vulnerabilities Catalog." Cybersecurity and Infrastructure Security Agency, accessed August 2026.

[7] CISA. "CISA, NSA, FBI and Partners Warn Zimbra Collaboration Suite Users of Ongoing Russian State-Supported Malicious Threat Activity." CISA, July 23, 2026.

[8] CISA. "Russian State-Supported Cyber Actors Conduct Phishing Campaign Targeting Users of Zimbra Collaboration Suite (AA26-204A)." CISA, NSA, FBI, July 23, 2026.

[9] Industrial Cyber. "Russian Hacker Group Laundry Bear Exploits Zimbra Zero-Click Flaw to Target Western Government, Critical Infrastructure." Industrial Cyber, July 2026.

[10] BetaNews. "Zimbra SNMP Flaw Actively Exploited, 274 Servers Hit." BetaNews, August 2026.

[11] Computer Weekly. "Russian APT Laundry Bear Perfects Zero-Click Phishing Attack." Computer Weekly, July 2026.

[12] Cloud Security Alliance. "CISA BOD 26-04: AI Threat Forces 3-Day Critical Patch Mandate." CSA AI Safety Initiative, June 13, 2026.

[13] BleepingComputer. "CISA: Microsoft SharePoint Flaw Now Exploited in Ransomware Attacks." BleepingComputer, August 11, 2026.

© 2026 Cloud Security Alliance. AI-assisted Rapid Research.

[14] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2026.