GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

24 August 2026

Advisory 195: CVE-2026-73570_Zimbra Collaboration Suite OS Command Injection Vulnerability

Release Date: 21st August 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate self-hosted mail and collaboration infrastructure, including government agencies, Internet Service Providers, tertiary institutions and regional bodies. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-73570 is a high-severity OS command injection vulnerability (CWE-78) in Zimbra Collaboration Suite (ZCS), an on-premise email and collaboration platform. It carries a CVSS Base Score of 8.9 and allows a remote, unauthenticated attacker to execute arbitrary operating system commands with the privileges of the zimbra service account.
The flaw arises from improper sanitisation of untrusted input during SNMP notification processing. Where the optional zimbra-snmp package is installed and SNMP notifications are enabled, an attacker can send specially crafted SMTP requests whose content reaches an operating system command context, resulting in remote code execution. No authentication, credentials or user interaction are required.

What are the systems affected?

Affected systems are on-premise Zimbra Collaboration Suite deployments where the optional zimbra-snmp package is installed and SNMP notifications are enabled via the snmp_notify parameter, with the swatchdog service running. The swatchdog service is enabled by default when SNMP notifications are turned on.

Zimbra Collaboration Suite, all versions prior to 10.1.20 - (Affected)
Zimbra Collaboration Suite 10.1.20 and later - (Not affected, patched)

Organisations should not assume they are unaffected on the basis that SNMP is an internal monitoring protocol

What does this mean?

This flaw requires no initial access step: the only prerequisite is unauthenticated network reachability to the mail server, which by the nature of the service is ordinarily internet-facing.

Step 1 - Unauthenticated Network Access
The attacker connects to an internet-reachable Zimbra server. No credentials, phishing or prior foothold are required.

Step 2 - Crafted SMTP Request
The attacker sends a specially crafted SMTP request containing payload content that will subsequently be handled by the SNMP notification workflow.

Step 3 - Command Injection (CVE-2026-73570)
Because the untrusted input is not properly neutralised before being passed to an operating system command, the injected payload executes as the zimbra user, granting the attacker command execution on the mail server.

Step 4 - Persistence and Data Access
The zimbra account controls the mail stores. Observed post-exploitation activity includes deployment of web shells to maintain access, reading and exfiltration of mailbox contents, harvesting of stored credentials and authentication material, modification of application files, and lateral movement to other systems on the same network.

CERTVU assesses the risk to any unpatched, internet-reachable Zimbra deployment in Vanuatu as high and immediate. A compromised mail server is not an isolated mail problem: it holds the correspondence, address books, credentials and authentication material of the organisation it serves, and generally has broad internal network reach.

Mitigation process

CERTVU recommends the following:

1. **Update Zimbra Collaboration Suite Immediately**

Update Zimbra Collaboration Suite to version 10.1.20 or later. This vulnerability is listed on the CISA Known Exploited Vulnerabilities catalog with a remediation due date of 24 August 2026, and active exploitation has been confirmed by CERT Polska. Treat any unpatched, internet-reachable Zimbra server as an emergency rather than a scheduled update.

2. Determine Whether the Vulnerable Components Are Present

Verify whether the optional zimbra-snmp package is installed and whether SNMP notifications are enabled via the snmp_notify parameter, together with the swatchdog service. Where SNMP notifications are not operationally required, disabling them removes the vulnerable path as an interim measure until the update can be applied.

3. Assume Compromise and Hunt

Any Zimbra server that was unpatched and internet-reachable should be treated as potentially compromised. Review the indicators of compromise listed above, preserve relevant logs and suspicious files for analysis, and isolate affected systems where evidence of intrusion is identified.

4. Report

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-73570
2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3. https://www.cisa.gov/news-events/alerts/2026/08/21/cisa-adds-one-known-exploited-vulnerability-catalog
4. https://nvd.nist.gov/vuln/detail/CVE-2026-73570
5. https://cwe.mitre.org/data/definitions/78.html