

ADVISORY !

TLP : CLEAR

DATE : 7th October 2026

REF NO : CERT-NCSOC-0230

ZIMBRA COLLABORATION SUITE REMOTE CODE EXECUTION VULNERABILITY

Severity Level: **High**

Components Affected

- Zimbra Collaboration Suite versions prior to 10.1.20.
- Installations where the optional zimbra-snmp package is installed and SNMP notifications are enabled.

Overview

Microsoft Threat Intelligence has identified and tracked active exploitation of “CVE-2026-73570”, an unauthenticated operating system command injection vulnerability affecting the Zimbra Collaboration Suite.

The vulnerability affects the SNMP notification processing path of Zimbra. An attacker can exploit the vulnerability remotely by sending a specially crafted email to an internet-facing Zimbra server. Successful exploitation may allow the attacker to execute operating system commands without authentication or user interaction.

Microsoft observed exploitation activity involving web shells, reverse shells, credential theft, persistence mechanisms, and attempts to access and collect email data from compromised servers.

Organizations operating internet-facing Zimbra Collaboration Suite servers are strongly advised to identify affected systems and apply the available security update as soon as possible.

Description

“CVE-2026-73570” is an operating system command injection vulnerability caused by improper sanitization of untrusted input during SNMP notification processing.

The vulnerability can be exploited when the optional zimbra-snmp package is installed and SNMP notifications are enabled. A specially crafted SMTP request can cause attacker-controlled input to reach command execution, allowing arbitrary operating system commands to execute with the privileges of the Zimbra service account.

The vulnerability does not require authentication or user interaction.

Zimbra version 10.1.20, released on 20 July 2026, contains the remediation for this vulnerability.

Impact

- Execute arbitrary operating system commands on the affected server.

ADVISORY !

TLP : CLEAR

DATE : 7th October 2026

REF NO : CERT-NCSOC-0230

- Establish unauthorized remote access.
- Deploy web shells or other malicious software.
- Obtain authentication information and credentials.
- Access or collect mailbox data.
- Establish persistence on the compromised server.
- Attempt privilege escalation.
- Use the compromised mail server for further malicious activity.

Solution/ Workarounds

Organizations using Zimbra Collaboration Suite should take the following actions:

- Upgrade all Zimbra Collaboration Suite installations to version 10.1.20 or later.
- Where immediate patching is not possible, uninstall the optional zimbra-snmp package.
- Disable SNMP notifications where they are not required.
- Restrict SNMP and SMTP access to trusted hosts where operationally feasible.
- Minimize direct internet exposure of mail servers.
- Review security and system logs for evidence of exploitation or unexpected command execution.
- Investigate unexpected JSP files, web shells, system services, scheduled tasks, or other persistence mechanisms on affected servers.
- Rotate relevant Zimbra authentication secrets if compromise is suspected.
- If exploitation is confirmed, isolate the affected server and initiate the organization's incident response procedures.

Reference

- <https://www.microsoft.com/en-us/security/blog/2026/09/30/unauthenticated-command-injection-on-internet-facing-mail-servers-tracking-cve-2026-73570/>
- <https://nvd.nist.gov/vuln/detail/CVE-2026-73570>

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.