# EXPLOITED VULNERABILITY ADVISORY: CVE-2026-73570

## Summary

CVE-2026-73570 in Synacor Zimbra Collaboration Suite (ZCS) is being actively exploited in the wild. A remote code execution vulnerability exists in Zimbra Collaboration (ZCS) before 10.1.20 when the optional zimbra-snmp package is installed and SNMP notifications are enabled. Due to improper sanitization of untrusted input during SNMP notification processing, an unauthenticated attacker can send specially crafted SMTP requests that may result in execution of arbitrary operating system commands as the Zimbra user. CISA requires federal remediation by 2026-08-24; under the CRA, exploitation of an affected product must be reported within 24 hours.

## What we know

- **CVE:** CVE-2026-73570
- **Affected:** Synacor Zimbra Collaboration Suite (ZCS)
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-21
- **Severity:** CVSS 8.9 High, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:L)
- **Exploitation likelihood (EPSS):** 1%
- **Weakness:** CWE-78

## Recommended action

Patch CVE-2026-73570 by 2026-08-24. If you cannot patch immediately, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. If you ship an affected product, be ready to file the CRA 24-hour report the moment you find it exploited.

---

*Sources: CISA Known Exploited Vulnerabilities, NIST NVD. Public data; an advisory of active exploitation, not an incident report. Verify applicability to your estate before acting.*