REPUBLIC OF KENYA

NATIONAL COMPUTER AND CYBERCRIMES COORDINATION COMMITTEE (NC4)

NATIONAL CYBERSECURITY ADVISORY

SECURITY OF ZIMBRA COLLABORATION EMAIL SYSTEMS

Classification: ADVISORY | Severity: HIGH | Date: 1 October 2026

Audience: All government institutions, county governments, critical-sector operators, businesses, educational and healthcare institutions, service providers, and other entities in Kenya hosting, administering or using Zimbra Collaboration, including outsourced and cloud-hosted deployments.

1. Advisory summary

NC4 draws attention to serious security vulnerabilities affecting Zimbra Collaboration email environments and the elevated risk associated with outdated or poorly maintained installations. Exploitation may permit unauthorized execution of commands, compromise of email accounts, theft or manipulation of sensitive correspondence, persistence on mail servers and disruption of essential communications.

Organizations must establish their precise product version, patch level, enabled components and exposure; implement applicable supported security updates; assess systems for indicators of compromise; and develop a secure migration plan for unsupported deployments. Patching alone must not be treated as proof that a previously exposed server is trustworthy.

2. Vulnerabilities requiring attention

Issue	Security relevance / required consideration
CVE-2024-45519 — postjournal command execution	Critical unauthenticated command execution in affected Zimbra versions when the vulnerable service is present/exposed. Known exploited vulnerability; verify service state and remediate.
CVE-2026-73570 — SNMP monitoring command injection	Command injection in SNMP monitoring when SNMP notifications are enabled; fix documented in Zimbra 10.1.20. Review exposure and logs.
Additional fixes in 10.1.20 and 10.1.21	Stored XSS, authorization or mail-forwarding control issues, password-recovery weaknesses, WebDAV authentication restrictions and integration vulnerabilities. Review applicability to installed edition and features.
Unsupported legacy versions	Zimbra 8.8.15 ended technical guidance on 31 December 2024; migrating to a supported, maintained branch is necessary.

The vendor release listing identifies 10.1.21 as the most recent 10.1 patch verified for this advisory. Before implementation, administrators must recheck the official release and security advisory pages for newer fixes, edition-specific requirements and supported upgrade paths.

3. Required immediate actions

- Inventory every Zimbra instance, including production, disaster recovery, test and third-party managed systems. Record versions, OS, patch levels, exposed services, installed extensions and account ownership.
- Identify publicly reachable administrative, webmail, SOAP, proxy, SMTP and monitoring interfaces. Restrict administrative access using VPN or approved management networks and least privilege; disable unnecessary features and services.
- Apply the latest supported vendor security patch appropriate to the installed release and edition, following a tested maintenance and rollback plan. Do not assume an unsupported branch is secure because its final patch was installed.
- Where postjournal or SNMP monitoring is unnecessary, disable the vulnerable component as a temporary risk-reduction measure consistent with vendor guidance; this does not replace supported updates.
- Enforce MFA for supported user and privileged access; review delegated rights, password-recovery settings, active sessions, application passwords and mail forwarding rules.
- Confirm independent, immutable or offline backups of mail data and configuration, and test restoration into an isolated environment.

4. Compromise assessment and incident handling

Administrators should investigate suspicious activity before declaring a vulnerable system clean. Review mail and reverse-proxy logs, operating-system authentication records, Zimbra audit and mailbox logs, scheduled tasks, startup services, new or modified JSP/web files, unexplained archive or staging directories, suspicious outgoing traffic, new administrator privileges, abnormal forwarding rules and unusual access to credential stores.

- If suspicious activity is identified, activate incident response, preserve relevant logs and forensic evidence, and isolate affected hosts or services in a manner proportionate to the operational risk.
- Rotate exposed passwords, API or authentication tokens, service credentials, SSH keys and trusted administrative credentials from a known-clean system; invalidate active sessions where feasible.
- Investigate mailbox access and exfiltration, malicious inbox or forwarding rules, delegated account access, and potential movement into connected identity, backup or virtualization systems.
- For confirmed host compromise, prefer rebuilding from trusted operating-system and application media, followed by controlled data restoration. Do not return the original compromised virtual machine directly to production.
- Coordinate evidence preservation, containment, recovery and reporting with NC4 and applicable institutional response teams.

5. Strategic remediation and migration

Organizations retaining end-of-support Zimbra installations should approve a time-bound migration to a supported and maintained release or another appropriately secured enterprise email platform. The transition should encompass the underlying operating system, server and hypervisor patching, network segmentation, firewall policy, centralized logging, endpoint/server detection, privileged-access controls, backup integrity and recovery testing. Any migration must validate mailbox integrity, identities, routing, TLS certificates, SPF/DKIM/DMARC and mail continuity before cutover.

6. Recommended implementation and assurance schedule

Priority	Action / evidence expected
Within 24 hours	Identify exposed installations; verify version and affected features; reduce unnecessary public exposure; begin log preservation and threat hunting.
Within 72 hours	Complete risk-based patching or documented compensating controls; assess suspicious activity; review privileged accounts, forwarding rules and backups.
Within 14 days	Submit internal remediation status to management; validate monitoring, recovery testing and migration decisions for any unsupported installations.
Within 30 days	Approve and track a funded, risk-prioritized migration/hardening plan, including owners, milestones and evidence of closure.

The above schedule is an operational recommendation for this advisory, not a representation of a new statutory reporting deadline. Where an active incident is suspected, reporting and response must not wait for these milestones.

7. Reporting and coordination

Entities that detect attempted or confirmed exploitation, unauthorized mailbox access, malicious persistence, data exposure or service disruption should promptly activate their incident response procedures and report through NC4's official incident-reporting channels at https://nc4.go.ke. Retain relevant event timelines, affected versions, IP indicators, log extracts and preserved evidence; do not publish sensitive incident details.

Official technical references

Zimbra Security Advisories: https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

Zimbra 10.1.21 release notes: https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.21

Zimbra 10.1.20 release notes: https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20

Zimbra release support and patch listing: https://wiki.zimbra.com/wiki/Zimbra_Releases

NIST NVD, CVE-2024-45519: https://nvd.nist.gov/vuln/detail/CVE-2024-45519

Issued for cybersecurity awareness and coordinated risk reduction. Institutional owners remain responsible for validating product applicability, obtaining vendor guidance and implementing proportionate controls.