

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Security Updates- Zimbra Collaboration Suite

Tracking #:432319324

Date:22-07-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Zimbra has released security updates to address nine security vulnerabilities affecting multiple components of the Zimbra Collaboration Suite.

TECHNICAL DETAILS:

Zimbra has released Daffodil v10.1.20 to address nine security vulnerabilities affecting multiple components of the Zimbra Collaboration Suite. The update includes a critical command injection vulnerability in the SNMP monitoring component, multiple stored Cross-Site Scripting (XSS) vulnerabilities in the Classic Web Client, a mail forwarding restriction bypass (CVE-2026-50055), a Server-Side Request Forgery (SSRF) vulnerability in the Nextcloud integration, and additional access control and authorization flaws.

The command injection vulnerability could allow attackers to execute arbitrary commands on affected servers when SNMP notifications are enabled, potentially leading to complete system compromise. The XSS vulnerabilities could enable attackers to execute malicious JavaScript in users' browsers, resulting in credential theft, session hijacking, and unauthorized actions.

Although there is no evidence of active exploitation at the time of publication, email collaboration platforms remain attractive targets for threat actors. Organizations are strongly advised to apply the latest security update immediately.

Vulnerability Details:

- Critical Command Injection – SNMP Monitoring Component
- Stored Cross-Site Scripting (XSS) – Malicious Attachment Filenames
- Stored Cross-Site Scripting (XSS) – Crafted Fields
- Stored Cross-Site Scripting (XSS) – Rendered Crafted Fields
- Stored Cross-Site Scripting (XSS) – Crafted Attachments
- CVE-2026-50055 – Mail Forwarding Restriction Bypass
- Access Control Issue – EWS Extension
- Authorization Issue – Mailbox Delegation
- Server-Side Request Forgery (SSRF) – Nextcloud Integration

Affected Products

- Zimbra Collaboration Suite (Daffodil)
- Versions prior to 10.1.20

Fixed Version

- Zimbra Daffodil v10.1.20

RECOMMENDATIONS:

Immediate Actions:

- Upgrade immediately Zimbra Daffodil to fixed version or latest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20