مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical XSS Vulnerability in Zimbra Classic Web Client

Tracking #:432319282

Date:11-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Zimbra has released updates for Zimbra Collaboration Suite (ZCS) to address a critical stored Cross-Site Scripting (XSS) vulnerability affecting the Classic Web Client.

TECHNICAL DETAILS:

Zimbra has released Zimbra Collaboration Suite (ZCS) v10.1.19 to address a critical stored Cross-Site Scripting (XSS) vulnerability affecting the Classic Web Client. The flaw allows attackers to send specially crafted emails containing malicious scripts that execute when a user opens the email.
Successful exploitation could enable attackers to access mailbox contents, steal active session tokens, modify account settings, and compromise user accounts. Although no CVE identifier has been assigned and no active exploitation has been confirmed, similar Zimbra XSS vulnerabilities have been exploited in previous campaigns, making timely patching essential.

Vulnerability Details:

- CVE ID: Not yet assigned
- Severity: Critical
- CVSS Score: Not assigned
- CWE: CWE-79 – Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- Description: Crafted emails can trigger stored XSS in the Classic Web Client, allowing malicious JavaScript to execute within a victim's authenticated browser session.

Fixed Version:

- Zimbra Collaboration Suite (ZCS) 10.1.19

RECOMMENDATIONS:

Immediate Actions:

- Immediately upgrade Zimbra Collaboration Suite to fixed version.

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/10.1.19