مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Active Exploitation of Zimbra XSS Vulnerability

Tracking #:432318818

Date:21-04-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Cross-Site Scripting (XSS) vulnerability affecting the Classic Web UI of Zimbra Collaboration Suite is now actively exploited in the wild.

TECHNICAL DETAILS:

A Cross-Site Scripting (XSS) vulnerability affecting the Classic Web UI of Zimbra Collaboration Suite is now actively exploited in the wild. The flaw allows remote attackers to execute arbitrary JavaScript within a victim's browser session simply by sending a crafted email. No user interaction beyond viewing the message is required, making this a high-risk, low-complexity attack vector.

Vulnerability Details

- CVE ID: CVE-2025-48700
- Vulnerability Type: Cross-Site Scripting (XSS)
- Attack Vector: Remote (via crafted email content)
- User Interaction: Required (only opening/viewing email)
- Exploit Maturity: Actively exploited
- Successful exploitation can result in:
  - Session hijacking
  - Unauthorized mailbox access
  - Data exfiltration
  - Potential lateral movement within enterprise environments

Patched Versions:

- 8.8.15 Patch 47
- 9.0.0 Patch 43
- 10.0.12
- 10.1.4

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade Zimbra Collaboration Suite to patched versions immediately.

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_Security_Advisories