مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Zimbra Collaboration Suite (ZCS)

Tracking #:432317792

Date:09-10-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed an actively exploited zero-day vulnerability in Synacor Zimbra Collaboration Suite (ZCS) Classic Web Client allows attackers to execute arbitrary JavaScript in a user's session via malicious ICS calendar invitation files.

TECHNICAL DETAILS:

A new zero-day XSS vulnerability (CVE-2025-27915) affects the Zimbra Collaboration Suite (ZCS) Classic Web Client and is actively being exploited in the wild. Attackers can hijack user sessions simply by sending malicious calendar invitation (ICS) files; successful exploitation enables unauthorized access and data exfiltration.

Vulnerability Details

- **CVE-2025-27915**
- Type: Cross-Site Scripting (XSS)
- The vulnerability arises from insufficient sanitization of HTML content within ICS (calendar invitation) files viewed in the Classic Web Client. Attackers craft ICS entries embedding JavaScript code via the event's ontoggle attribute. When a user views an email with a malicious ICS attachment, the embedded script is executed in the user's session context, providing attackers with full access equivalent to the victim.

Successful exploitation enables:

- Theft of credentials and sensitive communications
- Unauthorized access to distribution lists and shared folders
- Long-term espionage foothold in targeted inboxes
- Potential lateral movement and organizational compromise

Affected Product:

- Zimbra Collaboration Suite Classic Web Client

Affected Versions:

- Zimbra Collaboration (ZCS) 9.0, 10.0 and 10.1

Fixed Versions:

- ZCS 9.0.0 Patch 46 or later
- ZCS 10.0.15 or later
- ZCS 10.1.9 or later

RECOMMENDATIONS:

- Apply Zimbra-provided latest patches or workarounds as soon as possible.
- Monitor for suspicious ICS attachments and unauthorized mail filter changes.
- Educate users to avoid opening unexpected ICS files.
- Strengthen email filtering to detect oversized or malicious ICS files.

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://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://nvd.nist.gov/vuln/detail/CVE-2025-27915