

CVE-2025-27915

Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability

CISA KEV since Oct 7, 2025

Actively exploited

An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0 and 10.1. A stored cross-site scripting (XSS) vulnerability exists in the Classic Web Client due to insufficient sanitization of HTML content in ICS files. When a user views an e-mail message containing a malicious ICS entry, its embedded JavaScript executes via an ontoggle event inside a <details> tag.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 5.4 Medium · NVD	EPSS 0.041 90.6th percentile · FIRST	CISA DEADLINE Oct 28, 2025 KEV since 2025 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.041 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

This allows an attacker to run arbitrary JavaScript within the victim's session, potentially leading to unauthorized actions such as setting e-mail filters to redirect messages to an attacker-controlled address. As a result, an attacker can perform unauthorized actions on the victim's account, including e-mail redirection and data exfiltration.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
zimbra collaboration suite	$\geq 10.0.0 < 10.0.13$ $\geq 10.1.0 < 10.1.5$ 9.0.0	10.0.13 · 10.1.5	NVD

Sources

Vendor guidance	strikeready.com/blog/0day-ics-attack-in-the-wild/	wiki.zimbra.com	wiki.zimbra.com/wiki/Security_Center
NVD	nvd.nist.gov/vuln/detail/CVE-2025-27915	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-7823	Current data	evulnable.com/vulnerability-management/cve/CVE-2025-27915

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.