

CVE-2024-27443

Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability

CISA KEV since May 19, 2025

Actively exploited

An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. A Cross-Site Scripting (XSS) vulnerability exists in the CalendarInvite feature of the Zimbra webmail classic user interface, because of improper input validation in the handling of the calendar header. An attacker can exploit this via an email message containing a crafted calendar header with an embedded XSS payload. When a victim views this message in the Zimbra webmail classic interface, the payload is executed in the context of the victim's session, potentially leading to execution of arbitrary JavaScript code.

EVRS 75_{/100} Urgent priority	CVSS V3.1 6.1 Medium · NVD	EPSS 0.246 97.9th percentile · FIRST	CISA DEADLINE Jun 9, 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	0.246 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.1	☐ 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

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
collaboration	≥ 10.0.0 < 10.0.7 9.0.0	10.0.7	NVD

Sources

Vendor guidance	wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes	Additional guidance	wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P39#Security_Fixes
Additional guidance	cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2024-27443	Additional guidance	welivesecurity.com/en/eset-research/operation-roundpress/
wiki.zimbra.com	wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P46#Security_Fixes	NVD	nvd.nist.gov/vuln/detail/CVE-2024-27443
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-24646
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-27443		

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