

CVE-2020-7796

Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery Vulnerability

CISA KEV since Feb 17, 2026

Actively exploited

Zimbra Collaboration Suite (ZCS) before 8.8.15 Patch 7 allows SSRF when WebEx zimlet is installed and zimlet JSP is enabled.

EVRS 86 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.844 99.7th percentile · FIRST	CISA DEADLINE Mar 10, 2026 CISA federal deadline · Overdue by 7 months
--	--	--	--

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 year
☒ EPSS	0.844 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

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
zimbra collaboration suite	< 8.8.15 8.8.15	8.8.15	NVD

Sources

Vendor guidance	wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P7	NVD	nvd.nist.gov/vuln/detail/CVE-2020-7796
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-28728
Current data	evulnable.com/vulnerability-management/cve/CVE-2020-7796		

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