

CVE-2019-9670

Synacor Zimbra Collaboration Suite (ZCS) Improper Restriction of XML External Entity Reference

Exigent

CISA KEV since Jan 10, 2022

Actively exploited

Public exploit module (Metasploit)

mailboxd component in Synacor Zimbra Collaboration Suite 8.7.x before 8.7.11p10 has an XML External Entity injection (XXE) vulnerability, as demonstrated by Autodiscover/Autodiscover.xml.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE Jul 10, 2022 KEV since 2022 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
zimbra collaboration suite	≥ 8.7.0 < 8.7.11 8.7.11	8.7.11	NVD

Sources

Vendor guidance bugzilla.zimbra.com/show_bug.cgi?id=109129

Additional guidance wiki.zimbra.com/wiki/Zimbra_Security_Advisories

NVD nvd.nist.gov/vuln/detail/CVE-2019-9670

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-19036

Current data evulnable.com/vulnerability-management/cve/CVE-2019-9670

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