

CVE-2022-27925

Synacor Zimbra Collaboration Suite (ZCS) Arbitrary File Upload Vulnerability

CISA KEV since Aug 11, 2022

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

Zimbra Collaboration (aka ZCS) 8.8.15 and 9.0 has mboximport functionality that receives a ZIP archive and extracts files from it. An authenticated user with administrator rights has the ability to upload arbitrary files to the system, leading to directory traversal.

EVRS 90/100 Immediate priority	CVSS V3.1 7.2 High · NVD	EPSS 0.987 99.92nd percentile · FIRST	CISA DEADLINE Sep 1, 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.987 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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	8.8.15 9.0.0	no fixed version listed	NVD

Sources

Vendor guidance wiki.zimbra.com/wiki/Security_Center

blog.zimbra.com blog.zimbra.com/2022/08/authentication-bypass-in-mailboximportervlet-vulnerability/

NVD nvd.nist.gov/vuln/detail/CVE-2022-27925

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-32413

Current data evulnable.com/vulnerability-management/cve/CVE-2022-27925

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