Synacor Zimbra Collaboration Suite (ZCS) Arbitrary File Upload Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-27925
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-21 00:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	Zimbra Collaboration (aka ZCS) 8.8.15 and 9.0 has mboximport functionality that receives a ZIP archive and extracts files fr

Risk And Classification

EPSS: 0.943100000 probability, percentile 0.999500000 (date 2026-05-16)

CISA KEV: Listed on 2022-08-11; due 2022-09-01; ransomware use Known

Problem Types: CWE-22

CISA Known Exploited Vulnerability

Vendor	Synacor
Product	Zimbra Collaboration Suite (ZCS)
Name	Synacor Zimbra Collaboration Suite (ZCS) Arbitrary File Upload Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://blog.zimbra.com/2022/08/authentication-bypass-in-mailboximportservlet-vulnerability/; https://nvd.nist.gov/vuln/detail/CVE-2022-27925

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zimbra	Collaboration	8.8.15	-	All	All
Application	Zimbra	Collaboration	9.0.0	-	All	All

References

Reference	Source	Link	Tags
packetstormsecurity.com/files/168146/Zimbra-Zip-Path-Traversal.html	MISC	packetstormsecurity.com	
wiki.zimbra.com/wiki/Zimbra_Security_Advisories	MISC	wiki.zimbra.com	

wiki.zimbra.com/wiki/Zimbra_Security_Advisories	MISC	wiki.zimbra.com	
wiki.zimbra.com/wiki/Security_Center	MISC	wiki.zimbra.com	
Zimbra Releases/9.0.0/P24 - Zimbra :: Tech Center	MISC	wiki.zimbra.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

376769 Zimbra Collaboration Multiple Vulnerabilities

378336 Zimbra Collaboration Suite (ZCS) Multiple Vulnerabilities

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**