

CVE-2022-41352

Synacor Zimbra Collaboration Suite (ZCS) Arbitrary File Upload Vulnerability

Exigent
CISA KEV since Oct 20, 2022
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15 and 9.0. An attacker can upload arbitrary files through amavis via a cpio loophole (extraction to /opt/zimbra/jetty/webapps/zimbra/public) that can lead to incorrect access to any other user accounts. Zimbra recommends pax over cpio. Also, pax is in the prerequisites of Zimbra on Ubuntu; however, pax is no longer part of a default Red Hat installation after RHEL 6 (or CentOS 6). Once pax is installed, amavis automatically prefers it over cpio.

EVRS 93 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.955 99.87th percentile · FIRST	CISA DEADLINE Nov 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.955 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	9.0.0 8.8.15	no fixed version listed	NVD

Sources

Vendor guidance	wiki.zimbra.com/wiki/Security_Center	Additional guidance	forums.zimbra.org/viewtopic.php?t=71153&p=306532
NVD	nvd.nist.gov/vuln/detail/CVE-2022-41352	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-44557	Current data	evulnable.com/vulnerability-management/cve/CVE-2022-41352

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