

CVE-2024-45519

Synacor Zimbra Collaboration Suite (ZCS) Command Execution Vulnerability

Exigent

CISA KEV since Oct 3, 2024

Actively exploited

The postjournal service in Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1 sometimes allows unauthenticated users to execute commands.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.97th percentile · FIRST	CISA DEADLINE Oct 24, 2024 KEV since 2024 · 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 mitigations per vendor instructions 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 ≥ 10.0.0 < 10.0.9 8.8.15 9.0.0 10.1.0	8.8.15 · 10.0.9	NVD

Sources

Vendor guidance github.com/advisories/GHSA-fr4c-ch83-r968

wiki.zimbra.com wiki.zimbra.com/wiki/Zimbra_Security_Advisories

NVD nvd.nist.gov/vuln/detail/CVE-2024-45519

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-41520

Current data evulnable.com/vulnerability-management/cve/CVE-2024-45519

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