



Synacor Zimbra Collaboration Suite (ZCS) Arbitrary File Upload Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-41352
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-26 02:15:00 UTC
Updated	2024-02-01 01:06:00 UTC
Description	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15 and 9.0. An attacker can upload arbitrary files through amav

Risk And Classification

EPSS: 0.939580000 probability, percentile 0.998860000 (date 2026-04-22)

CISA KEV: Listed on 2022-10-20; due 2022-11-10; ransomware use Unknown

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://wiki.zimbra.com/wiki/Security_Center ; https://nvd.nist.gov/vuln/detail/CVE-2022-41352

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
Attacker managed to upload files into Web Client directory - Zimbra Forums	MISC	forums.zimbra.org
wiki.zimbra.com/wiki/Zimbra_Security_Advisories	MISC	wiki.zimbra.com

wiki.zimbra.com/wiki/Security_Center	MISC	wiki.zimbra.com
Zimbra Collaboration Suite TAR Path Traversal ≈ Packet Storm	MISC	packetstormsecurity.com
Zimbra Collaboration Suite High Severity Zero-Day RCE Vulnerability is Exploited in Wild! - SecPod Blog	MISC	www.secpod.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[377618](#) Zimbra Collaboration Remote Code Execution (RCE) Vulnerability

© [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 registered 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