

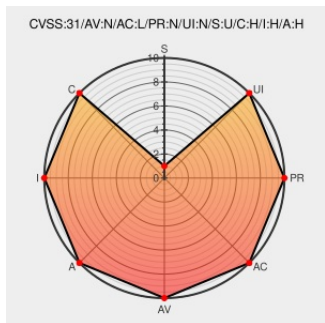


CVE-2022-37042

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:22:00 PM UTC

CVE-2022-37042

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Collaboration](#) from [Zimbra](#) contain the following vulnerability:

Zimbra Collaboration Suite (ZCS) 8.8.15 and 9.0 has mboximport functionality that receives a ZIP archive and extracts files from it. By bypassing authentication (i.e., not having an authtoken), an attacker can upload arbitrary files to the system, leading to directory traversal and remote code execution. NOTE: this issue exists because of an incomplete fix for CVE-2022-27925.

CVE-2022-37042 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
No Description Provided	packetstormsecurity.com Inactive Link Not Archived	MISC packetstormsecurity.com/files/168146/Zimbra-Zip-Path-Traversal.html
Zimbra Security Advisories - Zimbra :: Tech Center	wiki.zimbra.com text/html	MISC wiki.zimbra.com/wiki/Zimbra_Security_Advisories
Security Center - Zimbra :: Tech Center	wiki.zimbra.com text/html	MISC wiki.zimbra.com/wiki/Security_Center

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

Related QID Numbers

[377759](#) Zimbra Collaboration Suite Authentication Bypass Vulnerability

Exploit/POC from Github

Zimbra CVE-2022-37042 Nuclei weaponized template

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:zimbra:collaboration:8.8.15:-:*:*:*:*:

cpe:2.3:a:zimbra:collaboration:9.0.0:-:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @stevenadair	We caught another zero-day in the wild (CVE-2022-37042)! This time it was an authentication bypass that was used to... twitter.com/i/web/status/1...	2022-08-11 14:26:18
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-37042 Zimbra Collaboration Suite (ZCS) 8.8.15 and 9.0 has mboximport fu... twitter.com/i/web/status/1...	2022-08-11 21:56:00
 @TheHackersNews	Researchers warn of mass exploitation of the RCE #vulnerability in #Zimbra (CVE-2022-27925 and CVE-2022-37042), whi... twitter.com/i/web/status/1...	2022-08-12 06:14:53
 @_DrFrusci	Researchers warn of mass exploitation of the RCE #vulnerability in #Zimbra (CVE-2022-27925 and CVE-2022-37042), whi... twitter.com/i/web/status/1...	2022-08-12 06:15:09
 @IT_news_for_all	Researchers warn of mass exploitation of the RCE vulnerability in Zimbra (CVE-2022-27925 and CVE-2022-37042), which... twitter.com/i/web/status/1...	2022-08-12 06:17:02
 @trip_elix	"Researchers warn of mass exploitation of the RCE #vulnerability in #Zimbra (CVE-2022-27925 and CVE-2022-37042), wh... twitter.com/i/web/status/1...	2022-08-12 06:22:37
 @Swati_THN	Researchers warn of mass exploitation of the RCE #vulnerability in #Zimbra (CVE-2022-27925 and CVE-2022-37042), whi... twitter.com/i/web/status/1...	2022-08-12 06:35:00
 @unix_root	Researchers warn of mass exploitation of the RCE #vulnerability in #Zimbra (CVE-2022-27925 and CVE-2022-37042), whi... twitter.com/i/web/status/1...	2022-08-12 07:35:00
 @EchelonEyes	Две уязвимости в Zimbra, согласно отчету компании Volexity, CVE-2022-27925 и CVE-2022-37042, могут эксплуатировать... twitter.com/i/web/status/1...	2022-08-12 08:03:36
 @security_wang	Researchers warn of mass exploitation of the RCE #vulnerability in #Zimbra (CVE-2022-27925 and CVE-2022-37042), whi... twitter.com/i/web/status/1...	2022-08-12 09:35:00
 @EduardKovacs	A new zero-day vulnerability tracked as CVE-2022-37042 has been exploited since at least June to hack over 1,000 Zi... twitter.com/i/web/status/1...	2022-08-12 11:03:00

 @Shadowserver	@Volexity Please note this vulnerability now has CVE-2022-37042 re-assigned to it: Patch i... twitter.com/i/web/status/1...	2022-08-12 12:58:58
 @CVEtrends	Top 3 trending CVEs on Twitter Past 24 hrs: CVE-2022-37042: 1.5M (audience size) CVE-2022-27925: 1.4M CVE-2017-019... twitter.com/i/web/status/1...	2022-08-12 13:00:02
 @serghei	Threat actors are exploiting a recently addressed authentication bypass security vulnerability (CVE-2022-37042) to... twitter.com/i/web/status/1...	2022-08-12 14:29:37
 @YourAnonRiots	Researchers warn of mass exploitation of the RCE #vulnerability in #Zimbra (CVE-2022-27925 and CVE-2022-37042), whi... twitter.com/i/web/status/1...	2022-08-12 14:29:51
 @CVEreport	CVE-2022-37042 : Zimbra Collaboration Suite ZCS 8.8.15 and 9.0 has mboximport functionality that receives a ZIP a... twitter.com/i/web/status/1...	2022-08-12 15:27:06
 @inthewildio	CVE-2022-27925 is getting exploited #inthewild. Find out more at inthewild.io/vuln/CVE-2022-... CVE-2022-37042 is getting... twitter.com/i/web/status/1...	2022-08-12 15:37:41
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-37042 - Zimbra Collaboration Suite (ZCS) 8.8.15 and 9.0 has mboximport functi... twitter.com/i/web/status/1...	2022-08-12 15:42:16
 @dulenkp	There is great possibility of exploitation of the RCE #vulnerability in #Zimbra (CVE-2022-27925 and CVE-2022-37042... twitter.com/i/web/status/1...	2022-08-12 20:23:37
 /r/netcve	CVE-2022-37042	2022-08-12 16:38:38
 /r/CrowdSec	Block Illegal Users	2023-01-25 19:09:21
 /r/CrowdSec	Struggling to update my install	2023-07-05 20:02:21

[← Previous ID](#)
[Next ID→](#)

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)