



CVE-2022-3569

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

Summary

CVE	CVE-2022-3569
State	PUBLIC
Assigner	cve@rapid7.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-17 23:15:00 UTC
Updated	2023-07-21 21:04:00 UTC
Description	Due to an issue with incorrect sudo permissions, Zimbra Collaboration Suite (ZCS) suffers from a local privilege escalation

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Synacor	Zimbra Collaboration Suite	All	All	All	All

References

Reference	Source	Link
Zimbra Privilege Escalation ~ Packet Storm	MISC	packetstorms
Check in zimbra_postfix_priv_esc.rb by rbowes-r7 · Pull Request #17141 · rapid7/metasploit-framework · GitHub	MISC	github.com
JavaScript is not available.	MISC	twitter.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Originally reported by Twitter user @ldsopreload, validated by Ron Bowes of Rapid7

There are currently no legacy QID mappings associated with this CVE.

© [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](#)