



CVE-2022-20614

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

Summary

CVE	CVE-2022-20614
State	PUBLIC
Assigner	jenkinsci-cert@googlegroups.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-12 20:15:00 UTC
Updated	2023-11-22 21:30:00 UTC
Description	A missing permission check in Jenkins Mailer Plugin 391.ve4a_38c1b_cf4b_ and earlier allows attackers with Overall/Read

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Mailer	All	All	All	All
Application	Jenkins	Mailer	391.ve4a_38c1b_cf4b_	-	All	All
Application	Jenkins	Mailer	All	All	All	All
Application	Oracle	Communications Cloud Native Core Automated Test Suite	1.9.0	All	All	All

References

Reference	Source	Link	Tags
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
oss-security - Multiple vulnerabilities in Jenkins and Jenkins plugins	MLIST	www.openwall.com	
Jenkins Security Advisory 2022-01-12	CONFIRM	www.jenkins.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[376410](#) Jenkins Plugins Multiple Security Vulnerabilities (Jenkins Security Advisory 2022-01-12)

© [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](#).

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