



CVE-2022-41249

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

Summary

CVE	CVE-2022-41249
State	PUBLIC
Assigner	jenkinsci-cert@googlegroups.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-21 16:15:00 UTC
Updated	2023-11-01 21:02:00 UTC
Description	A cross-site request forgery (CSRF) vulnerability in Jenkins SCM HttpClient Plugin 1.5 and earlier allows attackers to connect to the Jenkins server and perform actions as the user.

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Scm HttpClient	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - Multiple vulnerabilities in Jenkins and Jenkins plugins	MLIST	www.openwall.com	
Jenkins Security Advisory 2022-09-21	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

730618 Jenkins Cross-Site Scripting (XSS) Vulnerability (Jenkins Security Advisory 2022-09-21)

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