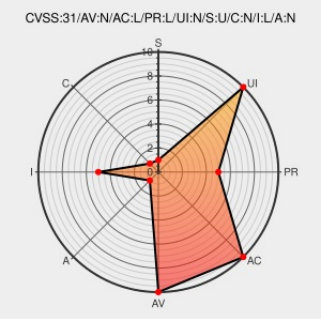
CVE-2019-10409

Published on: 09/25/2019 12:00:00 AM UTC

Last Modified on: 10/25/2023 06:16:00 PM UTC

CVE-2019-10409

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Project Inheritance from Jenkins contain the following vulnerability:

A missing permission check in Jenkins Project Inheritance Plugin 2.0.0 and earlier allowed attackers with Overall/Read permission to trigger project generation from templates.

CVE-2019-10409 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins Project Inheritance Plugin** version **= 2.0.0 and earlier**

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
oss-security - Multiple vulnerabilities in Jenkins and Jenkins plugins	Mailing List Third Party Advisory	MLIST [oss-security] 20190925 Multiple vulnerabilities in Jenkins and Jenkins plugins

	Third Party Advisory www.openwall.com text/html	
Jenkins Security Advisory 2019-09-25	Vendor Advisory jenkins.io text/html	CONFIRM jenkins.io/security/advisory/2019-09-25/#SECURITY-401

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Project Inheritance	All	All	All	All

cpe:2.3:a:jenkins:project_inheritance:*:*:*:*:*:jenkins:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→