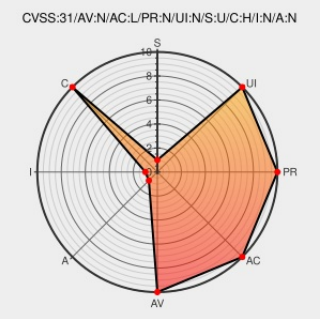
CVE-2019-10371

Published on: 08/07/2019 12:00:00 AM UTC

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

CVE-2019-10371

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



Certain versions of Gitlab Oauth from Jenkins contain the following vulnerability:

A session fixation vulnerability in Jenkins Gitlab Authentication Plugin 1.4 and earlier in GitLabSecurityRealm.java allows unauthorized attackers to impersonate another user if they can control the pre-authentication session.

CVE-2019-10371 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins Gitlab Authentication Plugin** version **= 1.4 and earlier**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
oss-security - Multiple vulnerabilities in Jenkins plugins	Mailing List Third Party Advisory	MLIST [oss-security] 20190807 Multiple vulnerabilities in Jenkins plugins

plugins	Third Party Advisory www.openwall.com text/html	jenkins plugins
Jenkins Security Advisory 2019-08-07	Vendor Advisory jenkins.io text/html	CONFIRM jenkins.io/security/advisory/2019-08-07/#SECURITY-795

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Gitlab Oauth	All	All	All	All

cpe:2.3:a:jenkins:gitlab_oauth:*:*:*:*:*:jenkins:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→