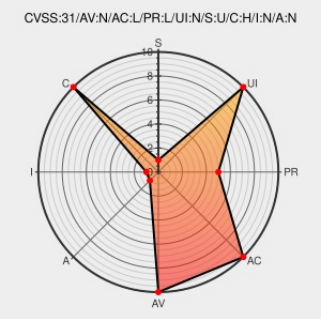
CVE-2021-21637

Published on: 03/30/2021 12:00:00 AM UTC

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

CVE-2021-21637

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



Certain versions of Team Foundation Server from Jenkins contain the following vulnerability:

A missing permission check in Jenkins Team Foundation Server Plugin 5.157.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.

CVE-2021-21637 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins Team Foundation Server Plugin** version **not down converted**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link

oss-security - Multiple vulnerabilities in Jenkins plugins	www.openwall.com text/html	MLIST [oss-security] 20210330 Multiple vulnerabilities in Jenkins plugins
Jenkins Security Advisory 2021-03-30	www.jenkins.io text/html	CONFIRM www.jenkins.io/security/advisory/2021-03-30/#SECURITY-2283%20(2)

Related QID Numbers

375473 Jenkins Multiple Plugins Security Vulnerabilities(Jenkins Security Advisory 2021-03-30)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Team Foundation Server	All	All	All	All

cpe:2.3:a:jenkins:team_foundation_server:*:*:*:*:*:jenkins:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report