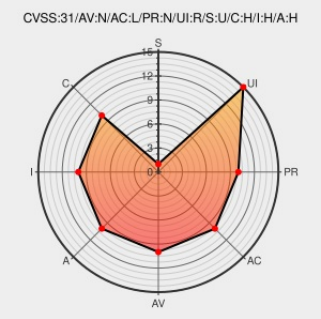
CVE-2023-24437

Published on: Not Yet Published

Last Modified on: 02/02/2023 03:43:00 PM UTC

CVE-2023-24437

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



Certain versions of Jira Pipeline Steps from Jenkins contain the following vulnerability:

A cross-site request forgery (CSRF) vulnerability in Jenkins JIRA Pipeline Steps Plugin 2.0.165.v8846cf59f3db and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.

CVE-2023-24437 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Jenkins Project** - **Jenkins JIRA Pipeline Steps Plugin** version **<= 2.0.165.v8846cf59f3db**

Affected Vendor/Software: **Jenkins Project** - **Jenkins JIRA Pipeline Steps Plugin** version **?> 2.0.165.v8846cf59f3db**

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
Jenkins Security Advisory 2023-01-24	www.jenkins.io text/html	MISC www.jenkins.io/security/advisory/2023-01-24/#SECURITY-2786

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Jira Pipeline Steps	All	All	All	All

cpe:2.3:a:jenkins:jira_pipeline_steps:*:*:*:*:*:jenkins:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-24437 : A cross-site request forgery CSRF vulnerability in Jenkins JIRA Pipeline Steps Plugin 2.0.165.v8… twitter.com/i/web/status/1…	2023-01-26 22:15:24

← Previous ID

Next ID→