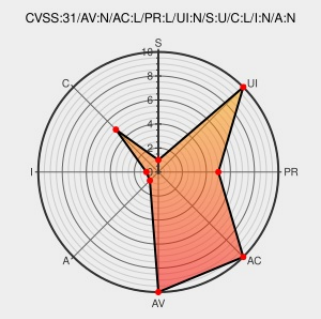
CVE-2021-21625

Published on: 03/18/2021 12:00:00 AM UTC

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

CVE-2021-21625

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



Certain versions of Cloudbees Aws Credentials from Jenkins contain the following vulnerability:

Jenkins CloudBees AWS Credentials Plugin 1.28 and earlier does not perform a permission check in a helper method for HTTP endpoints, allowing attackers with Overall/Read permission to enumerate credentials IDs of AWS credentials stored in Jenkins in some circumstances.

CVE-2021-21625 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins CloudBees AWS Credentials Plugin** version **<= 1.28**

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	LOW	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

Jenkins Security Advisory 2021-03-18	www.jenkins.io text/html	CONFIRM www.jenkins.io/security/advisory/2021-03-18/#SECURITY-2032
oss-security - Multiple vulnerabilities in Jenkins plugins	www.openwall.com text/html	MLIST [oss-security] 20210318 Multiple vulnerabilities in Jenkins plugins

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Cloudbees Aws Credentials	All	All	All	All

cpe:2.3:a:jenkins:cloudbees_aws_credentials:*:*:*:*:*:jenkins:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→