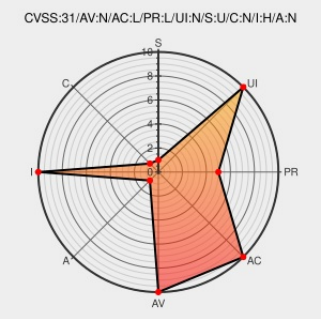
CVE-2020-2278

Published on: 09/16/2020 12:00:00 AM UTC

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

CVE-2020-2278

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



Certain versions of Storable Configs from Jenkins contain the following vulnerability:

Jenkins Storable Configs Plugin 1.0 and earlier does not restrict the user-specified file name, allowing attackers with Job/Configure permission to replace any other '.xml' file on the Jenkins controller with a job config.xml file's content.

CVE-2020-2278 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins Storable Configs 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	NONE	HIGH	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
Jenkins Security Advisory 2020-09-16	www.jenkins.io text/html	CONFIRM www.jenkins.io/security/advisory/2020-09-16/#SECURITY-1968%20(2)

oss-security - Multiple vulnerabilities in Jenkins plugins	Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20200916 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	Storable Configs	All	All	All	All

cpe:2.3:a:jenkins:storable_configs:*:*:*:*:*:jenkins:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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