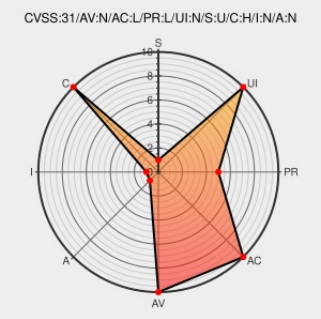
CVE-2022-27201

Published on: Not Yet Published

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

CVE-2022-27201

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



Certain versions of Jenkins from Jenkins contain the following vulnerability:

Jenkins Semantic Versioning Plugin 1.13 and earlier does not restrict execution of an controller/agent message to agents, and implements no limitations about the file path that can be parsed, allowing attackers able to control agent processes to have Jenkins parse a crafted file that uses external entities for extraction of secrets from the Jenkins controller or server-side request forgery.

CVE-2022-27201 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins Semantic Versioning Plugin** version **<= 1.13**

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

Description	Tags	Link
Jenkins Security Advisory 2022-03-15	www.jenkins.io text/html	CONFIRM www.jenkins.io/security/advisory/2022-03-15/#SECURITY-2124
oss-security - Multiple vulnerabilities in Jenkins plugins	www.openwall.com text/html	MLIST [oss-security] 20220315 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	Jenkins	All	All	All	All
Application	Jenkins	Jenkins	All	All	All	All
Application	Jenkins	Semantic Versioning	All	All	All	All

cpe:2.3:a:jenkins:jenkins:*:*:*:*:lts:*:*:*:

cpe:2.3:a:jenkins:jenkins:*:*:*:*:-:*:*:*:

cpe:2.3:a:jenkins:semantic_versioning:*:*:*:*:*:jenkins:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-27201 : Jenkins Semantic Versioning Plugin 1.13 and earlier does not restrict execution of an controller/a… twitter.com/i/web/status/1…	2022-03-15 16:55:27

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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