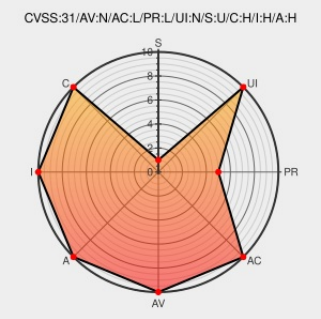
CVE-2020-2167

Published on: 03/25/2020 12:00:00 AM UTC

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

CVE-2020-2167

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



Certain versions of Openshift Pipeline from Jenkins contain the following vulnerability:

Jenkins OpenShift Pipeline Plugin 1.0.56 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.

CVE-2020-2167 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins OpenShift Pipeline Plugin** version **<= 1.0.56**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Jenkins Security Advisory 2020-03-25	Vendor Advisory jenkins.io	CONFIRM jenkins.io/security/advisory/2020-03-25/#SECURITY-1739

	text/html	
oss-security - Multiple vulnerabilities in Jenkins and Jenkins plugins	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20200325 Multiple vulnerabilities in Jenkins and 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	Openshift Pipeline	All	All	All	All

cpe:2.3:a:jenkins:openshift_pipeline:*:*:*:*:*:jenkins:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→