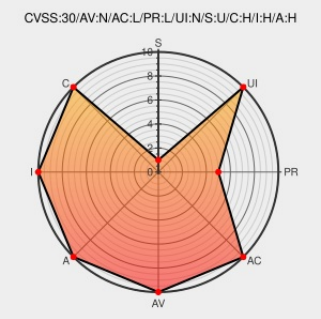
CVE-2018-1000866

Published on: 12/10/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:31 PM UTC

CVE-2018-1000866

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



Certain versions of Pipeline from Jenkins contain the following vulnerability:

A sandbox bypass vulnerability exists in Pipeline: Groovy Plugin 2.59 and earlier in groovy-sandbox/src/main/java/org/kohsuke/groovy/sandbox/SandboxTransformer.java, groovy-cps/lib/src/main/java/com/cloudbees/groovy/cps/SandboxCpsTransformer.java that allows attackers with Job/Configure permission, or unauthorized attackers with SCM commit privileges and corresponding pipelines based on Jenkinsfiles set up in Jenkins, to execute arbitrary code on the Jenkins master JVM

CVE-2018-1000866 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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

CVE References

Description	Tags	Link
Jenkins Security Advisory 2018-10-29	Vendor Advisory jenkins.io text/html	CONFIRM jenkins.io/security/advisory/2018-10-29/#SECURITY-1186
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHBA-2019:0326
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHBA-2019:0327

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	Pipeline	_groovy	All	All	All
Application	Jenkins	Pipeline	_groovy	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All

cpe:2.3:a:jenkins:pipeline:_groovy:*:*:*:*:*:jenkins:*:

cpe:2.3:a:jenkins:pipeline\:_groovy:*:*:*:*:*:jenkins:*:

cpe:2.3:a:redhat:openshift_container_platform:3.11:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:3.11:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→