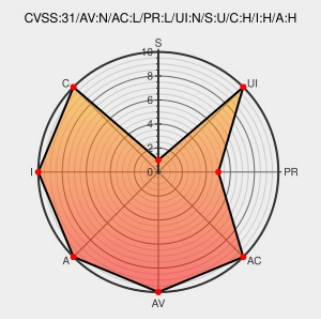
CVE-2019-1003001

Published on: 01/22/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:37 PM UTC

CVE-2019-1003001

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 2.61 and earlier in src/main/java/org/jenkinsci/plugins/workflow/cps/CpsFlowDefinition.java, src/main/java/org/jenkinsci/plugins/workflow/cps/CpsGroovyShellFactory.java that allows attackers with Overall/Read permission to provide a pipeline script to an HTTP endpoint that can result in arbitrary code execution on the Jenkins master JVM.

CVE-2019-1003001 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Jenkins project** - **Pipeline: Groovy Plugin** version **2.61 and earlier**

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
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHBA-2019:0326
Jenkins ACL Bypass / Metaprogramming Remote Code Execution ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/152132/Jenkins-ACL-Bypass-Metaprogramming-Remote-Code-Execution.html
Jenkins Security Advisory 2019-01-08	Vendor Advisory jenkins.io text/html	CONFIRM jenkins.io/security/advisory/2019-01-08/#SECURITY-1266
Jenkins ACL Bypass and Metaprogramming RCE	Third Party Advisory www.rapid7.com text/html	MISC www.rapid7.com/db/modules/exploit/multi/http/jenkins_metaprogramming
Jenkins 2.137 and Pipeline Groovy Plugin 2.61 - ACL Bypass and Metaprogramming Remote Code Execution (Metasploit)	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 46572
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHBA-2019:0327

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Jenkins RCE Proof-of-Concept: SECURITY-1266 / CVE-2019-1003000 (Script Security), CVE-2019-1003001 (Pipeline: Groovy)…

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

Social Mentions

Source	Title	Posted (UTC)
@ipssignatures	It's new to me that proofpoint has a protection/signature/rule for the vulnerability CVE-2019-1003001. … twitter.com/i/web/status/1…	2021-07-29 01:02:00
@ipssignatures	I know 4 other IPSs that have protections/signatures/rules for the vulnerability CVE-2019-1003001. ipssignatures.appspot.com/?cve=CVE-2019-… #S4s5zdukrslf5w	2021-07-29 01:02:00

← Previous ID

Next ID→