

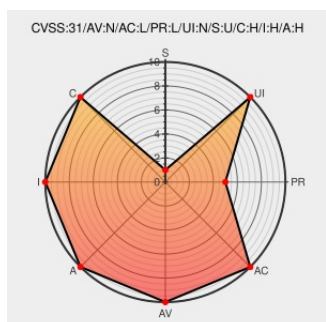


CVE-2019-1003005

Published on: 02/06/2019 12:00:00 AM UTC

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

CVE-2019-1003005

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Script Security](#) from [Jenkins](#) contain the following vulnerability:

A sandbox bypass vulnerability exists in Jenkins Script Security Plugin 1.50 and earlier in

src/main/java/org/jenkinsci/plugins/scriptsecurity/sandbox/groovy/SecureGroovyScript.java that allows attackers with Overall/Read permission to provide a Groovy script to an HTTP endpoint that can result in arbitrary code execution on the Jenkins master JVM.

CVE-2019-1003005 has been assigned by [jenkinsci-cert@googlegroups.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Jenkins project](#) - **Jenkins Script Security Plugin** version = **1.50 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 RHSA-2019:0739
Jenkins Security Advisory 2019-01-28	Vendor Advisory jenkins.io text/html	 CONFIRM jenkins.io/security/advisory/2019-01-28/#SECURITY-1292
Jenkins Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/166778/Jenkins-Remote-Code-Execution.html

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	Script Security	All	All	All	All

cpe:2.3:a:jenkins:script_security:*:*:*:*:jenkins:*:*

No vendor comments have been submitted for this CVE

[← 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 registered 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](#)