



CVE-2019-16538

Published on: 11/21/2019 12:00:00 AM UTC

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

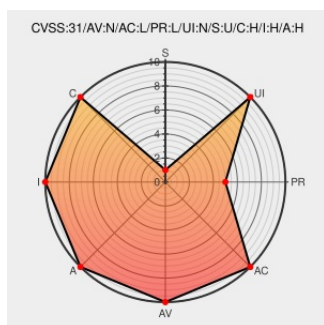
CVE-2019-16538

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

A sandbox bypass vulnerability in Jenkins Script Security Plugin 1.67 and earlier related to the handling of default parameter expressions in closures allowed attackers to execute arbitrary code in sandboxed scripts.

CVE-2019-16538 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 = **1.67 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
Jenkins Security Advisory 2019-11-21	Vendor Advisory jenkins.io	CONFIRM jenkins.io/security/advisory/2019-11-21/#SECURITY-1658

jenkins

text/html

oss-security - Multiple vulnerabilities in Jenkins plugins

Mailing List

Third Party Advisory

www.openwall.com

text/html

 MLIST [oss-security] 20191121 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	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 →