

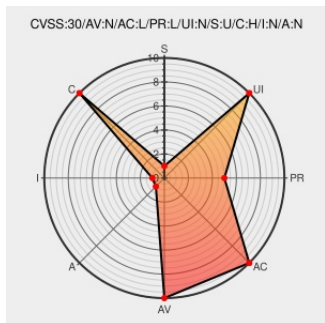


CVE-2017-1000505

Published on: 01/25/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:36 PM UTC

CVE-2017-1000505

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

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

In Jenkins Script Security Plugin version 1.36 and earlier, users with the ability to configure sandboxed Groovy scripts are able to use a type coercion feature in Groovy to create new `File` objects from strings. This allowed reading arbitrary files on the Jenkins master file system. Such a type coercion is now subject to sandbox protection and

considered to be a call to the `new File(String)` constructor for the purpose of in-process script approval.

CVE-2017-1000505 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Jenkins Security Advisory: 2017-12-11	View on Jenkins	CONFIRM jenkins.io/SECURITY/advisory/2017-12-11/

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 →