



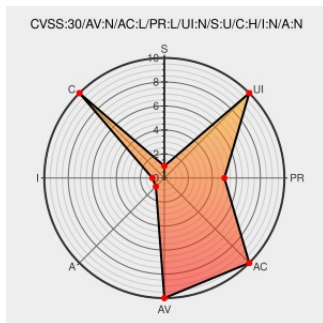
Last Modified on: 03/23/2021 11:24:30 PM UTC

CVE-2018-1000997

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

A path traversal vulnerability exists in the Stapler web framework used by Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in `core/src/main/java/org/kohsuke/stapler/Facet.java`,

groovy/src/main/java/org/kohsuke/stapler/jelly/groovy/GroovyFacet.java,
jelly/src/main/java/org/kohsuke/stapler/jelly/JellyFacet.java,
jruby/src/main/java/org/kohsuke/stapler/jelly/jruby/JRubyFacet.java,
jsp/src/main/java/org/kohsuke/stapler/jsp/JSPFacet.java that allows attackers to render
routable objects using any view in Jenkins, exposing internal information about those objects
not intended to be viewed, such as their toString() representation.

CVE-2018-1000997 has been assigned by [M cve@mitre.org](mailto: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 2018-10-10	Vendor Advisory jenkins.io text/html	 CONFIRM jenkins.io/security/advisory/2018-10-10/#SECURITY-867

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	Jenkins	All	All	All	All
Application	Jenkins	Jenkins	All	All	All	All
cpe:2.3:a:jenkins:jenkins:*.*.*:lts:*.*:						
cpe:2.3:a:jenkins: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