

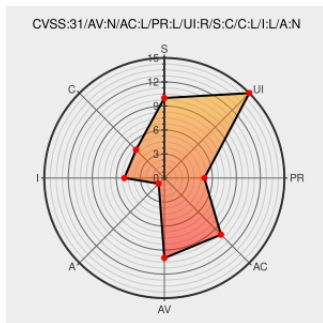


CVE-2020-2317

Published on: 11/04/2020 12:00:00 AM UTC

Last Modified on: 11/02/2023 10:10:00 PM UTC

CVE-2020-2317

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

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

Jenkins FindBugs Plugin 5.0.0 and earlier does not escape the annotation message in tooltips, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide report files to Jenkins FindBugs Plugin's post build step.

CVE-2020-2317 has been assigned by [jenkinsci-cert@googlegroups.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Jenkins project](#) - **Jenkins FindBugs Plugin** version **not down converted**

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link
Jenkins Security Advisory 2020-11-04	Vendor Advisory www.jenkins.io	CONFIRM www.jenkins.io/security/advisory/2020-11-04/#SECURITY-1918

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	Findbugs	All	All	All	All
cpe:2.3:a:jenkins:findbugs:*:*:*:*:jenkins:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→