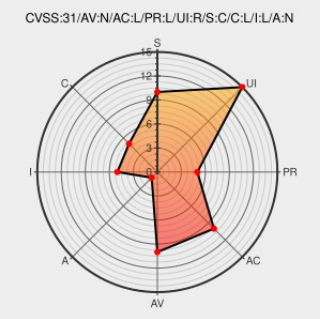
CVE-2020-2161

Published on: 03/25/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:09 PM UTC

CVE-2020-2161

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Jenkins from Jenkins contain the following vulnerability:

Jenkins 2.227 and earlier, LTS 2.204.5 and earlier does not properly escape node labels that are shown in the form validation for label expressions on job configuration pages, resulting in a stored XSS vulnerability exploitable by users able to define node labels.

CVE-2020-2161 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins** version **<= 2.227**

Affected Vendor/Software: **Jenkins project** - **Jenkins** version **<= LTS 2.204.5**

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 2020-03-25	Vendor Advisory jenkins.io text/html	CONFIRM jenkins.io/security/advisory/2020-03-25/#SECURITY-1781
oss-security - Multiple vulnerabilities in Jenkins and Jenkins plugins	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20200325 Multiple vulnerabilities in Jenkins and 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.

Related QID Numbers

501019 Alpine Linux Security Update for jenkins

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→