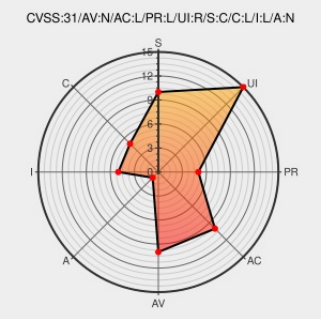
CVE-2020-2175

Published on: 04/07/2020 12:00:00 AM UTC

Last Modified on: 11/02/2023 09:42:00 PM UTC

CVE-2020-2175

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



Certain versions of Fitnesse from Jenkins contain the following vulnerability:

Jenkins FitNesse Plugin 1.31 and earlier does not correctly escape report contents before showing them on the Jenkins UI, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users able to control the XML input files processed by the plugin.

CVE-2020-2175 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins FitNesse Plugin** version **<= 1.31**

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
oss-security - Multiple vulnerabilities in Jenkins plugins	www.openwall.com text/html	MLIST [oss-security] 20200407 Multiple vulnerabilities in Jenkins plugins

Jenkins Security Advisory 2020-04-07	Third Party Advisory jenkins.io text/html	CONFIRM jenkins.io/security/advisory/2020-04-07/#SECURITY-1801

Related QID Numbers

372574 Jenkins Plugins Multiple Security Vulnerabilities(Jenkins Security Advisory 2020-04-07)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Fitnesse	All	All	All	All

cpe:2.3:a:jenkins:fitnesse:*:*:*:*:*:jenkins:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→