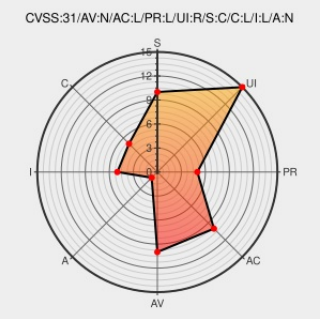
CVE-2022-34786

Published on: Not Yet Published

Last Modified on: 10/25/2023 06:17:00 PM UTC

CVE-2022-34786

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



Certain versions of Rich Text Publisher from Jenkins contain the following vulnerability:

Jenkins Rich Text Publisher Plugin 1.4 and earlier does not escape the HTML message set by its post-build step, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to configure jobs.

CVE-2022-34786 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins Rich Text Publisher 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 2022-06-30	www.jenkins.io text/html	CONFIRM www.jenkins.io/security/advisory/2022-06-30/#SECURITY-2332

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	Rich Text Publisher	All	All	All	All

cpe:2.3:a:jenkins:rich_text_publisher:*:*:*:*:*:jenkins:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-34786 : Jenkins Rich Text Publisher Plugin 1.4 and earlier does not escape the HTML message set by its pos… twitter.com/i/web/status/1…	2022-06-30 17:57:26
@LinInfoSec	Jenkins - CVE-2022-34786: jenkins.io/security/advis…	2022-06-30 21:01:24

← Previous ID

Next ID→