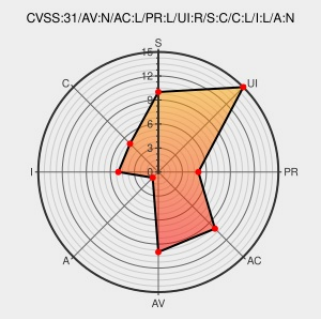
CVE-2021-21660

Published on: 05/25/2021 12:00:00 AM UTC

Last Modified on: 11/03/2023 05:39:00 PM UTC

CVE-2021-21660

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



Certain versions of Markdown Formatter from Jenkins contain the following vulnerability:

Jenkins Markdown Formatter Plugin 0.1.0 and earlier does not sanitize crafted link target URLs, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with the ability to edit any description rendered using the configured markup formatter.

CVE-2021-21660 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Jenkins project** - **Jenkins Markdown Formatter Plugin** version **<= 0.1.0**

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
Open Source Vulnerability Database | WhiteSource	www.whitesourcesoftware.com text/html	MISC www.whitesourcesoftware.com/vulnerability-database/CVE-2021-21660

oss-security - Multiple vulnerabilities in Jenkins plugins	www.openwall.com text/html	MLIST [oss-security] 20210525 Multiple vulnerabilities in Jenkins plugins
Jenkins Security Advisory 2021-05-25	www.jenkins.io text/html	CONFIRM www.jenkins.io/security/advisory/2021-05-25/#SECURITY-2198

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jenkins	Markdown Formatter	All	All	All	All

cpe:2.3:a:jenkins:markdown_formatter:*:*:*:*:*:jenkins:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-21660 : Jenkins Markdown Formatter Plugin 0.1.0 and earlier does not sanitize crafted link target URLs, re… twitter.com/i/web/status/1…	2021-05-25 15:48:47
@LinInfoSec	Jenkins - CVE-2021-21660: jenkins.io/security/advis…	2021-05-25 18:30:32
/r/netcve	CVE-2021-21660	2021-05-25 16:41:37

← Previous ID

Next ID→