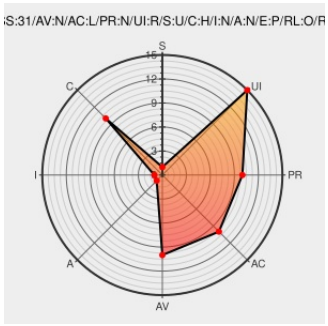
CVE-2020-7773

Published on: 11/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:54 PM UTC

CVE-2020-7773

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



Certain versions of Markdown-it-highlightjs from Markdown-it-highlightjs Project contain the following vulnerability:

This affects the package markdown-it-highlightjs before 3.3.1. It is possible insert malicious JavaScript as a value of lang in the markdown-it-highlightjs Inline code highlighting feature. const markdownItHighlightjs = require("markdown-it-highlightjs"); const md = require('markdown-it'); const reuslt_xss = md() .use(markdownItHighlightjs, { inline: true }) .render('console.log(42){.">js}'); console.log(reuslt_xss);

CVE-2020-7773 has been assigned by report@snyk.io to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link

markdown-it-highlightjs/index.js at v3.3.0 · valeriangalliat/markdown-it-highlightjs · GitHub	Broken Link github.com text/html	MISC github.com/valeriangalliat/markdown-it-highlightjs/blob/v3.3.0/index.js%23L52
Cross-site Scripting (XSS) in markdown-it-highlightjs | Snyk	Mitigation Third Party Advisory snyk.io text/html	CONFIRM N/A
fix: escape invalid lang characters (XSS) by ooooooo-q · Pull Request #14 · valeriangalliat/markdown-it-highlightjs · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM N/A

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Markdown-it-highlightjs Project	Markdown-it-highlightjs	All	All	All	All
Application	Markdown-it-highlightjs Project	Markdown-it-highlightjs	All	All	All	All

cpe:2.3:a:markdown-it-highlightjs_project:markdown-it-highlightjs:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:markdown-it-highlightjs_project:markdown-it-highlightjs:*:*:*:*:*:node.js:*:*:

Discovery Credit

ooooooo_q

← Previous ID

Next ID→