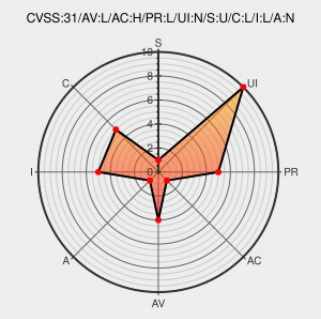
CVE-2022-36036

Published on: Not Yet Published

Last Modified on: 09/01/2022 08:50:00 PM UTC

CVE-2022-36036 - advisory for GHSA-rvgm-35jw-q628

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



Certain versions of Mdx-mermaid from Mdx-mermaid Project contain the following vulnerability:

mdx-mermaid provides plug and play access to Mermaid in MDX. There is a potential for an arbitrary javascript injection in versions less than 1.3.0 and 2.0.0-rc1. Modify any mermaid code blocks with arbitrary code and it will execute when the component is loaded by MDXjs. This vulnerability was patched in version(s) 1.3.0 and 2.0.0-rc2. There are currently no known workarounds.

CVE-2022-36036 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **sjwall** - **mdx-mermaid** version **< 1.3.0**

Affected Vendor/Software: **sjwall** - **mdx-mermaid** version **= 2.0.0-rc1**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Improper Control of Generation of Code ('Code Injection') in mdx-mermaid · Advisory · sjwall/mdx-mermaid · GitHub	github.com text/html	CONFIRM github.com/sjwall/mdx-mermaid/security/advisories/GHSA-rvgm-35jw-q628
Merge pull request from GHSA-rvgm-35jw-q628 · sjwall/mdx-mermaid@f2b9938 · GitHub	github.com text/html	MISC github.com/sjwall/mdx-mermaid/commit/f2b99386660fd13316823529c3f1314ebbcdfd2a

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	Mdx-mermaid Project	Mdx-mermaid	All	All	All	All
Application	Mdx-mermaid Project	Mdx-mermaid	2.0.0	rc1	All	All

cpe:2.3:a:mdx-mermaid_project:mdx-mermaid:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:mdx-mermaid_project:mdx-mermaid:2.0.0:rc1:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-36036 : mdx-mermaid provides plug and play access to Mermaid in MDX. There is a potential for an arbitrary… twitter.com/i/web/status/1…	2022-08-29 17:33:58
/r/netcve	CVE-2022-36036	2022-08-29 18:39:44

← Previous ID

Next ID→