snyk Vulnerability DB

Snyk Vulnerability Database › npm › gatsby-plugin-mdx

Search by package n

Deserialization of Untrusted Data

Affecting gatsby-plugin-mdx package, versions <2.14.1 >=3.0.0 <3.15.2

INTRODUCED: 18 FEB 2022 CVE-2022-25863 ? CWE-502 ? FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `gatsby-plugin-mdx` to version 2.14.1, 3.15.2 or higher.

Overview

gatsby-plugin-mdx is a MDX integration for Gatsby

Affected versions of this package are vulnerable to Deserialization of Untrusted Data when passing input through to the `gray-matter` package, due to its default configurations that are missing input sanitization. Exploiting this vulnerability is possible when passing input in both `webpack` (MDX files in src/pages or MDX file imported as a component in frontend / React code) and data mode (querying MDX nodes via GraphQL).

Workaround:

If an older version of `gatsby-plugin-mdx` must be used, input passed into the plugin should be sanitized ahead of processing.

Poc:

8.1

HIGH

Snyk CVSS

Exploit Maturity	**Proof of concept** ?
Attack Complexity	**Low** ?
Confidentiality	HIGH ?
Integrity	HIGH ?

See more

› **NVD** 9.8 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what

```
const mdxToJsx = require("gatsby-plugin-mdx/utils/mdx.js");
var payload = '---
jsn((require("child_process")).execSync("touch rce"))';
mdxToJsx(payload);
```

application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-JS-GATSBYPLUGINMDX-2405699
Published	6 Jun 2022
Disclosed	18 Feb 2022
Credit	Feng Xiao and Zhongfu Su

References

- GitHub Commit
- GitHub PR
- PoC

Report a new vulnerability

Found a mistake?

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon

Join the >> community

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.