

[New issue](#)[Jump to bottom](#)

# fix(gatsby-plugin-mdx): don't allow JS frontmatter by default

## #35830

[Merged](#) pieh merged 1 commit into [master](#) from [fix/mdx-js-frontmatter-vuln](#) on Jun 2

Conversation 5 Commits 1 Checks 1 Files changed 29



pieh commented on Jun 2 • edited

Contributor

## Description

Currently `gatsby-plugin-mdx` by default supports the "JS engine" for frontmatter. The example syntax for it is:

```
---js
{
  foo: require(`fs`).readFileSync('something', 'utf-8')
}
---
```

Your regular MDX body

This was never intended default behavior because in some cases it can open up an attack vector for remote code execution (on the build server). As long as sourced content is secure and actually owned by same party as site owner, this doesn't cause problems, but we should be explicit with this, so we disable it by default with option to re-enable it (if someone actually relied on this unintended "feature")

In new default mode (JS frontmatter engine disabled), we will show warning if there is any content that use JS frontmatter that this will not be processed/executed:

```
success Building HTML renderer - 163.243s
success Execute page configs - 0.102s
success Caching Webpack compilations - 0.002s
warn You have frontmatter declared with "---js" or "---javascript" that is not parsed by
default to mitigate a security risk (see
https://github.com/gatsbyjs/gatsby/security/advisories/GHSA-mj46-r4gr-5x83). If you require
this feature it can be enabled by setting "JSFrontmatterEngine: true" in the plugin option
of gatsby-plugin-mdx.
success run queries in workers - 1.975s - 6/6 3.04/s
```

Because this is security risk we will continuously show warning as reminder that it might not be safe to use it (it's not guaranteed it's not safe - context matter a lot):

```
success load gatsby config - 0.394s
warn JS frontmatter engine is enabled in gatsby-plugin-mdx (via JSFrontmatterEngine: true in plugin options). This can cause a security risk, see
https://github.com/gatsbyjs/gatsby/security/advisories/GHSA-mj46-r4gr-5x83. If you are not relying on this feature we strongly suggest disabling it via
the "JSFrontmatterEngine: false" plugin option. If you rely on this feature make sure to properly secure or sanitize your content source.
success load plugins - 15.598s
```

## Documentation

Small stub added to README.md about new plugin option referencing not yet published advisory with some details - this could likely be made nicer, but for the sake of getting fix out, this will have to do for now.

  **fix(gatsby-plugin-mdx): don't allow JS frontmatter by default** ... ✖ f214eb0


  **gatsbot** bot added the **status: triage needed** label on Jun 2

  **pieh** added **topic: remark/mdx** and removed **status: triage needed** labels on Jun 2

  **mlgualtieri** self-requested a review 6 months ago

**mlgualtieri** approved these changes on Jun 2

[View changes](#)

 **pieh** merged commit **b3690fb** into **master** on Jun 2  
32 of 36 checks passed

[View details](#)

  **pieh** deleted the **fix/mdx-js-frontmatter-vuln** branch 6 months ago

  **pieh** added this to **To cherry-pick in V3 Release Hotfixes** via automation on Jun 2

  **pieh** added this to **To cherry-pick in Release candidate** via automation on Jun 2

  **pieh** added this to **To cherry-pick in V4 Release hotfixes** via automation on Jun 2

  **gatsbybot** mentioned this pull request on Jun 2

**fix(gatsby-plugin-mdx): don't allow JS frontmatter by default (#35830)** #35832

 Merged

 pieh added a commit that referenced this pull request on Jun 2

 fix(gatsby-plugin-mdx): don't allow JS frontmatter by default (#35830) ...  1c491d4

 pieh added a commit that referenced this pull request on Jun 2

 fix(gatsby-plugin-mdx): don't allow JS frontmatter by default (#35830) ...  444bfd4

 This was referenced on Jun 2

**fix(gatsby-plugin-mdx): don't allow JS frontmatter by default (#35830) #35833**

 Merged

**fix(gatsby-plugin-mdx): don't allow JS frontmatter by default (#35830) #35834**

 Merged

 pieh added a commit that referenced this pull request on Jun 2

 fix(gatsby-plugin-mdx): don't allow JS frontmatter by default (#35830) ...  417e4e8

  pieh moved this from To cherry-pick to Backport PR opened in Release candidate on Jun 2

  pieh moved this from To cherry-pick to Backport PR opened in V4 Release hotfixes on Jun 2

  pieh moved this from To cherry-pick to Backport PR opened in V3 Release Hotfixes on Jun 2

  pieh moved this from Backport PR opened to Backported in Release candidate on Jun 2

 pieh added a commit that referenced this pull request on Jun 2

 fix(gatsby-plugin-mdx): don't allow JS frontmatter by default (#35830) ( ...  b982eb7

 pieh added a commit that referenced this pull request on Jun 2

 fix(gatsby-plugin-mdx): don't allow JS frontmatter by default (#35830) ( ...  ff94ed5

 **pieh** added a commit that referenced this pull request on Jun 2



fix(gatsby-plugin-mdx): don't allow JS frontmatter by default ([#35830](#)) ( ...

✓ e916cf8

**mosesoak** commented on Jun 2

@**pieh** @**mlgualtieri** Thanks for this addition. Wanted to let you know that the link to the security issue is a Github 404.

[GHSA-mj46-r4gr-5x83](#)

It appears 3 times in this PR.

**mlgualtieri** commented on Jun 2

Contributor

Thanks @**mosesoak**! It was not an oversight, but we were waiting on GitHub to assign a CVE to the issue before publishing the advisory. But, it doesn't appear that this will happen today so I went ahead and published the advisory. The link should work for you now.

  **pieh** moved this from **Backport PR opened** to **Published in V3 Release Hotfixes** on Jun 3

  **pieh** moved this from **Backport PR opened** to **Published in V4 Release hotfixes** on Jun 3

**karlhorky** commented on Jun 4

Contributor

@**pieh** after upgrading from `gatsby-plugin-mdx@3.15.1` to `gatsby-plugin-mdx@3.15.2`, we're seeing our Frontmatter code show up in the content of the page 🤖

 `http://localhost:3000`

ed

`pageTitle: 'Dashboard' navTitle: 'Dashboard'`

# Learning Platform

This appears regardless of whether we have the `JSFrontmatterEngine` set to `true` or unconfigured...

**karlhorky** commented on Jun 4 • edited ▼

Contributor

**Edit:** this only works for `gatsby develop`, see below for a solution for `gatsby build`

It seems like commenting out line 187 with `options` prevents this from happening:

[gatsby/packages/gatsby-plugin-mdx/loaders/mdx-loader.js](#)

Lines 180 to 196 in 7dfd52d

```
180     let code = content
181     // after running mdx, the code *always* has a default export, so this
182     // check needs to happen first.
183     if (!hasDefaultExport(content, options) && !!defaultLayout) {
184       debug(`inserting default layout`, defaultLayout)
185       const { content: contentWithoutFrontmatter, matter } = grayMatter(
186         content,
187         options
188       )
189
190       code = `${matter ? matter : ``}
```

Also, it seems like the options being passed to `gray-matter` on this line don't match the valid `gray-matter` options at all... They are Gatsby config options.

**Edit:** Apparently commenting out the above line only works in `gatsby develop`.

A solution for `gatsby build` (SSG) requires:

1. Commenting out passing all options to `gray-matter` in the `mdx-loader.js`, `utils/mdx.js`, `utils/gen-mdx.js` files (using `patch-package`)
2. And then ALSO enabling the `JSFrontmatterEngine` option

Super strange, wonder what's causing this Frontmatter to show up in the content.

@pieh have any idea what's happening here? Or do you think that I should open a new issue?



8 hidden items

[Load more...](#)

[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1 Rutam21/gatsby#246

 Open

 This was referenced on Jun 6

[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1 Xtuden-com/gatsby#2062

 Open

[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1 nidhi42/gatsby#985

 Open

[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1 Rutam21/gatsby#247

 Open

[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1 0xSebin/gatsby#541

 Open

[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1 chawdamrunal/gatsby#1094

 Open

  kaocher82 mentioned this pull request on Jun 6

[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1 Xtuden-com/gatsby#2063

 Open

 This was referenced on Jun 6

[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1 nidhi42/gatsby#986

 Open

[Snyk] Security upgrade gatsby-plugin-mdx from 1.2.52 to 2.14.1 0xSebin/gatsby#542























 Open

[Snyk] Security upgrade gatsby-plugin-mdx from 1.4.0 to 2.14.1 chawdamrunal/gatsby#1096

 Open

[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1 0xSebin/gatsby#543

 Open

-   **MaxMood96** mentioned this pull request on Jun 7
- [Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** MaxMood96/gatsby#448
-  [Open](#)
-   **0xSebin** mentioned this pull request on Jun 7
- [Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** 0xSebin/gatsby#544
-  [Open](#)
-   **chawdamrunal** mentioned this pull request on Jun 7
- [Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** chawdamrunal/gatsby#1097
-  [Open](#)
-   **kaocher82** mentioned this pull request on Jun 7
- [Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** Xtuden-com/gatsby#2065
-  [Open](#)
-  This was referenced on Jun 7
- [Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** MaxMood96/gatsby#449
-  [Open](#)
- [Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** Xtuden-com/gatsby#2066
-  [Open](#)
- [Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** 0xSebin/gatsby#545
-  [Open](#)
-   **tyhopp** mentioned this pull request on Jun 7
- fix(gatsby-plugin-mdx): Do not leak frontmatter into page** #35859
-  [Merged](#)
-   **kaocher82** mentioned this pull request on Jun 7
- [Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** Xtuden-com/gatsby#2067
-  [Open](#)

  **marvinjude** moved this from **Backported** to **Archived** in **Release candidate** on Jun 7

  **kaocher82** mentioned this pull request on Jun 7

**[Snyk] Security upgrade gatsby-plugin-mdx from 1.2.34 to 2.14.1** Xtuden-com/gatsby#2068

 **Open**

  **0xSebin** mentioned this pull request on Jun 7

**[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** 0xSebin/gatsby#548

 **Open**

  **snyk-bot** mentioned this pull request on Jun 7

**[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** 0xSebin/gatsby#550

 **Open**

**karlhorky** commented on Jun 9

**Contributor**

Ok @pieh I created a new issue over here: [#35901](#) - just need to get around to creating a reproduction...

  **karlhorky** mentioned this pull request on Jun 9

**[gatsby-plugin-mdx] Frontmatter shows up in page content** #35901

 **Closed**

 2 tasks

  **tyhopp** removed this from **Archived** in **Release candidate** on Jun 16

  **kaocher82** mentioned this pull request on Jun 22

**[Snyk] Fix for 6 vulnerabilities** Xtuden-com/gatsby#2270

 **Open**

  **MaxMood96** mentioned this pull request on Aug 16

**[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** MaxMood96/gatsby#557




 Open

  **samq-ws** mentioned this pull request 22 days ago

**[Snyk] Security upgrade gatsby-plugin-mdx from 1.10.1 to 2.14.1** samq-research/gatsby#62

 Open

#### Reviewers

 **mlgualtieri**



#### Assignees

No one assigned

#### Labels

topic: remark/mdx

#### Projects

 **V4 Release hotfixes**  
Published

1 closed project ▼

#### Milestone

No milestone

#### Development

Successfully merging this pull request may close these issues.

None yet

4 participants

