

New issue

[Jump to bottom](#)

V1.5.3: Unrestricted File Upload Vulnerability #325

✓ Closed b1ackc4t opened this issue on Mar 19 · 7 comments


Labels bug

b1ackc4t commented on Mar 19 • edited ▾

See PDF for details:
[typemill-1.5.3-backstage.UploadVul.pdf](#)



1

 b1ackc4t closed this as completed on Mar 20

 b1ackc4t reopened this on Mar 20

trendschau commented on Mar 22

Member

thank you for reporting, the upload-feature is for registered users only.
I will fix that asap and upload a hotfix version.

  trendschau added the bug label on Mar 25

trendschau commented on Mar 28

Member

just published the hotfix 1.5.3.1. I added a separate extension check and repeated the mimetype check when the file is uploaded to the temporary folder. If mimetype fails there, then the file is deleted immediately. Also updated the htaccess.

Vulnerability reported in #268 is still fixed.

The reason behind this security whole: Some environments did not support the mimetype extraction of a base64 string, so as a quick fix I made it conditionally and this opened up for this vulnerability. Now solved properly by checking the mimetype of the stored file which works in all environments.

Thank you for reporting again!



trendschau closed this as completed on Mar 28

MeteoLukas commented on Mar 30

Hi @trendschau

I'm new to Typemill, successfully installed Version 1.5.3.1 yesterday but found an issue with file upload. Folders and files have the appropriate permission and I can upload a picture with a FTP client to /media/... but not using the "image upload" button in the editor view. The image does not upload fully, meaning that the "loading" GIF below the uploaded image does not stop rotating waiting a few minutes. Similarly, for file upload, the file does not upload.

Since this might be related to this fix, I thought about leaving a comment here. Thanks for checking, I hope that it's not related to my infrastructure...

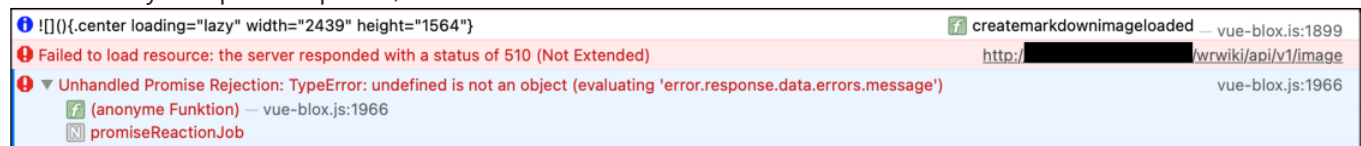
trendschau commented on Mar 30

Member

I cannot reproduce that error. Can you please open your developer tools in the browser, upload an image or file again and check the errors in the dev-tools? You should see something in the tabs "console" and/or "network".

MeteoLukas commented on Mar 30 • edited ▼

Thanks for your quick response, here the error:



Update: I installed Typemill on a different host and it works there. Might be a different configuration? they are both running PHP 8.0

trendschau commented on Mar 31

Member

Can you click on "network" and then inspect the call to api/v1/image? Just click on the call and then open the tab "response" and please post the content of the response, there should be a detailed error message. Before you do that, please go to the settings in the admin area, scroll down to developer settings and activate the checkbox for report errors so that all error details are visible.

MeteoLukas commented on Apr 6 • edited ▼

Thanks @trendschau for the hint. I found the error:

I got "Access denied by security policy" coming from the WAF (mod security). Allowing the image upload process, I'm now able to upload images.

In case this helps others: I'm using Hoststar and in the settings -> Hosting -> ModSecurity you can allow processes that recently failed...

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

