New issue

Jump to bottom

XSS via Link Target #1102

Closed farisv opened this issue on Apr 14, 2021 · 1 comment · Fixed by #1104

farisv commented on Apr 14, 2021 • edited ▾ Contributor

The `react-draft-wysiwyg` library is not filtering the `javascript:` prefix in the Link Target. XSS can be triggered when someone clicks the malicious link on the draft. This vulnerability can be exploited in a scenario where the draft is shared among different users (such as in a blog/content dashboard).

Steps to reproduce

1. On https://jpuri.github.io/react-draft-wysiwyg/#/demo, insert a link.
2. Set `javascript:alert(document.domain)` as Link Target.
3. Hover the link and click the icon to open the link.
4. You can see the JavaScript is executed under the context of `jpuri.github.io` .

Expectation

If the link starts with `javascript:` , don't open it. You can try another rich text editor such as https://ckeditor.com/ckeditor-5/demo/ for reference.

The XSS itself is triggered because of this line (`window.open(url, 'blank')`). The `url` should be validated before it reaches that line.

farisv mentioned this issue on Apr 14, 2021

Fix XSS in Link Target #1104

Merged

jpuri closed this as completed in #1104 on Apr 17, 2021

paweb commented on Aug 11, 2021

@farisv @jpuri Could this safe URL check be made at earlier stage? Why it is even allowed to create a link with XSS code? My suggestion would be to show an error message beside the link target input field when a user is trying to add `javascript:..` code into it. And also `Add` button could be disabled until the URL is safe.

Or if you think it's not an good idea, I'd love to hear your arguments. :)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix XSS in Link Target
farisv/react-draft-wysiwyg

2 participants