

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

## XSS vulnerability could result in RCE - CVE-2021-29996 #2548

Closed briskets opened this issue on Apr 4, 2021 · 1 comment · Fixed by #2765

briskets commented on Apr 4, 2021

### Description

Cross Site Scripting (XSS) vulnerability that could result in Remote Code Execution (RCE).

[CVE-2021-29996](#) was assigned for this issue.

### Steps to reproduce

1. Create a .md file that contains:

```
'''<style/onload=require('child_process').exec('calc')>
```

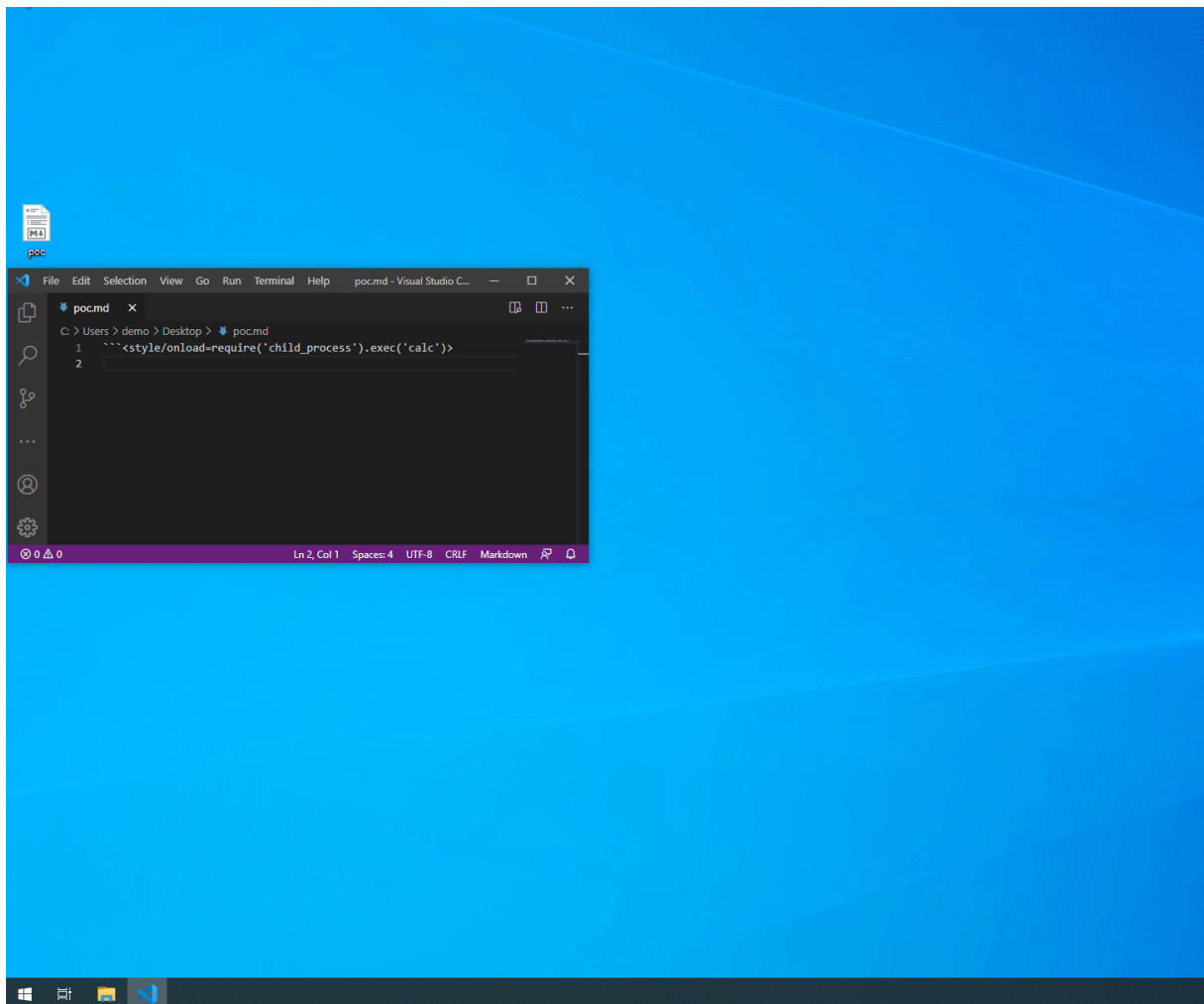
### Expected behavior:

Language input for the fenced code block should be sanitized before rendered.

### Actual behavior:

HTML stored as language input is not sanitized. Arbitrary javascript code is executed upon rendering. Processes outside of Mark Text could be executed due to nodeIntegration being enabled.

### Proof of Concept



### Versions


- Mark Text version: 0.16.3
- Operating system: Windows, Linux, MacOS

5 2


OS-WS commented on Jun 21, 2021

Hi, @briskets  
Was this issue ever addressed/ fixed?  
If so, in what commit?  
Thanks in advance!

 fxha added a commit that referenced this issue on Dec 14, 2021

 fxha fix XSS on language input and hyperlinks (#2548, #2601)

 e8653f3


 fxha mentioned this issue on Dec 14, 2021

fix XSS on language input and hyperlinks (#2548, #2601) #2765

 Merged

 fxha closed this as completed in #2765 on Dec 16, 2021

 fxha added a commit that referenced this issue on Dec 16, 2021

 fxha fix XSS on language input and hyperlinks (#2548, #2601) (#2765)

 0dd09cc

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 on language input and hyperlinks (#2548, #2601)  
marktext/marktext

2 participants

