New issue

Jump to bottom

Cross-site scripting leads to Remote Code Execution #1716

Closed **soulfoodisgood** opened this issue on Feb 5, 2021 · 2 comments

Labels bug confirmed pinned priority:high security

Projects Zettlr 2.x

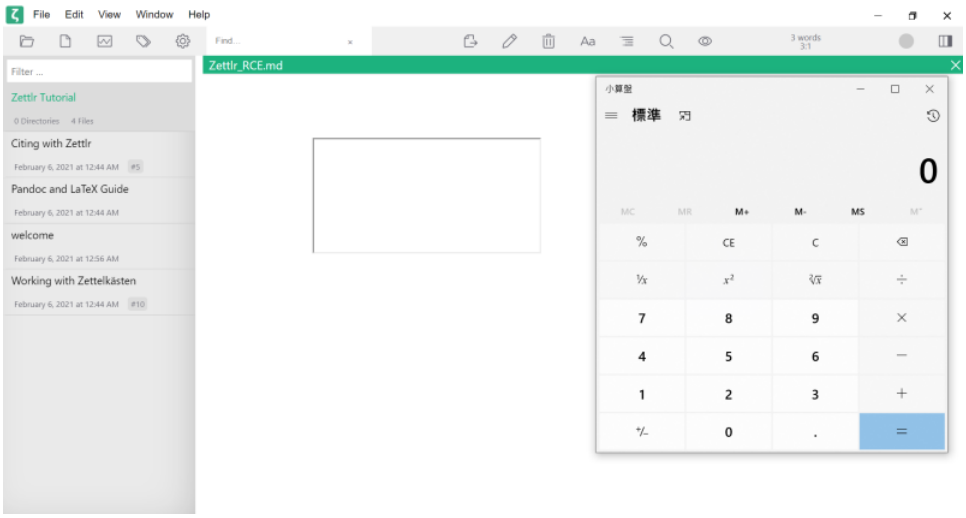
soulfoodisgood commented on Feb 5, 2021 • edited

Description

XSS leads to remote code execution

Reproducing

1. Download the crafted .md file (https://drive.google.com/file/d/1j9p1bL75ezWIIRbg0hb65-02jIt2u8OX/view?usp=sharing)
   Or make the md file by yourself. Foo.md content:
   ```
   <iframe src=x onload="require('electron').shell.openExternal('C:/Windows/System32/calc.exe')"></iframe>
   ```
2. Open the file with Zettlr 1.8.7Windows Version
3. Once the page refresh or you can click anywhere for refreshing, calculator pops up.



Expected behaviour

XSS payload shouldn't execute
Set nodeIntregration as false

Platform

- OS and version: Windows 10 x64
- Zettlr Version: 1.8.7

Additional information

boring-cyborg bot commented on Feb 5, 2021

Thanks so much for opening up your first issue here on the repository! 🎉 We would like to warmly welcome you to the community behind the app! 😊 We'll check in soon and have a look at your issue. In the meantime, you can check your issue and make sure it aligns with our contribution guidelines! Here's the comprehensive list:

Enhancements

An enhancement takes a feature and improves or alters its behaviour. Please make sure to argue how your proposition will aid non-technical text workers, and why it can't be emulated easily with other features or apps!

Feature requests

Feature requests introduce whole new features into the app. This requires a lot of work, so these might be turned down if the implementation costs supersede the benefits we expect to see from implementing it. Please do not be disappointed if that happens. It likely has nothing to do with your great request but simply with us and our missing resources!
You can of course always ask someone to implement this feature, because a PR with a working new feature has much higher chances of being merged! :)

Bug reports

Please note that one of the main reasons for why bug reports cannot be addressed is that there's not enough information for us to find and fix the bug you describe, so make sure you try to pinpoint the bug as close as possible.
The ideal bug report for us has two qualities:

1. The bug is always reproducible, at least within a certain context. 2. We know exactly what specifically goes wrong, and there is consensus on what should happen instead.

Please note that if you encounter behaviour that does not align with your expectations of what would happen, this might as well be simply intended behaviour and we need to simply *clarify* why the behaviour is the way it is. This is not to be considered a bug and such issues may be closed! Suggest an enhancement instead!
But now, have a great day and thank you again!

nathanlesage commented on Feb 8, 2021 Member

Absolutely true, Abricotine worked around this using a whitelist of pages. I have to implement something similar.

nathanlesage added bug confirmed **pinned** priority:high labels on Feb 8, 2021

nathanlesage added this to **To do** in **Zettlr 2.x** via automation on Feb 8, 2021

nathanlesage added the security label on Feb 8, 2021

nathanlesage closed this as completed in 53b544b on Apr 21, 2021

Zettlr 2.x automation moved this from **To do** to **Done** on Apr 21, 2021

Assignees
No one assigned

Labels
bug confirmed **pinned** priority:high security

Projects
Zettlr 2.x
Done

Milestone
No milestone

Development
No branches or pull requests

2 participants