alagrede / znote-app Public

<> Code   Issues 11   Pull requests   Discussions   Actions   Projects   ···

New issue

Jump to bottom

Multiple Stored XSS #5

Closed   **soulfoodisgood** opened this issue on Feb 3, 2021 · 4 comments

Assignees

Labels   enhancement

Milestone   0.5.3

soulfoodisgood commented on Feb 3, 2021 • edited

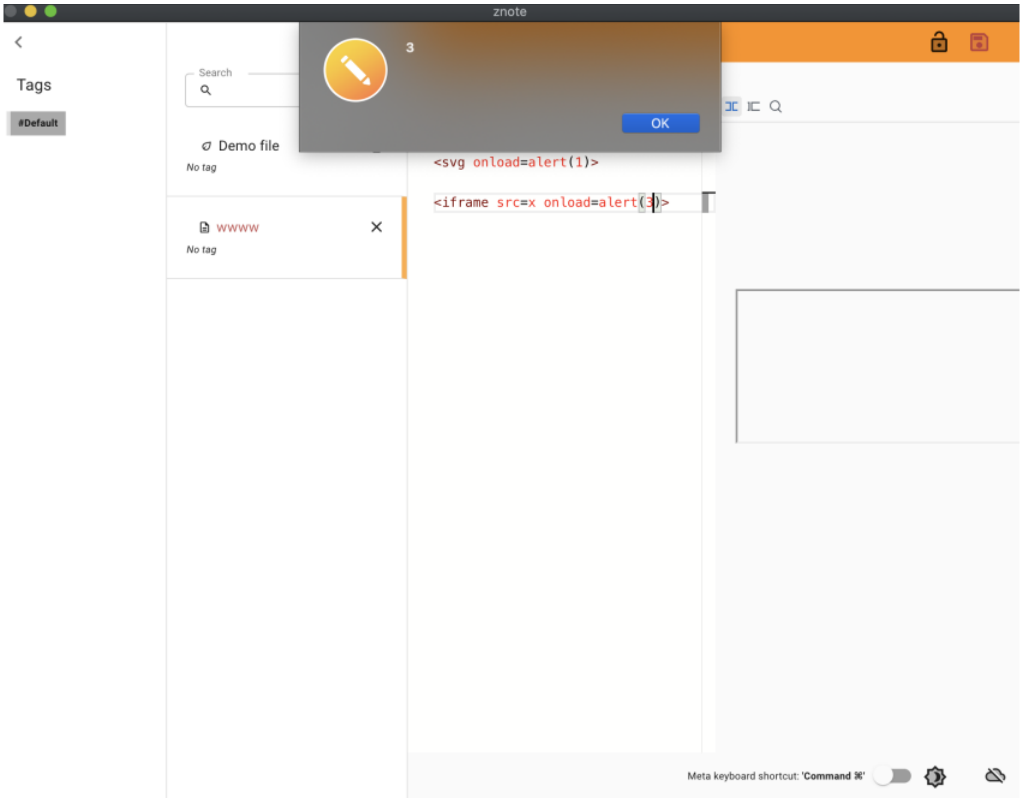
[Description]
Multiple XSS payloads are available for znote. It leads to attacker's javascript execution

[Reproduce]
You can try with copy paste the payloads below:
1.

```
<svg>
<svg onload=alert(1)>
```

2.

```
<iframe src=x onload=alert(1)>
```



```
<svg onload=alert(1)>

<iframe src=x onload=alert(3)>
```

alagrede commented on Feb 3, 2021   Owner

Hello **@soulfoodisgood**,
First of all, thank you for your report.
I'm trying to define the relevance of this issue.
Executing HTML/JS in the viewer it's originally a developer feature. It is the owner's responsibility to check the content of these notes.
I could probably prevent javascript execution without affecting HTML functionality and/or add a flag to manually allow javascript to run in files.
Thanks

alagrede added the enhancement label on Feb 3, 2021

soulfoodisgood commented on Feb 3, 2021 • edited   Author

Please check https://medium.com/bugbountywriteup/remote-code-execution-through-cross-site-scripting-in-electron-f3b891ad637
XSS is dangerous for electron apps because once `nodeIntegration` set as true or it can be bypassed to get "require" available, it leads to remote code execution .

👍 2

alagrede commented on Feb 4, 2021 Owner

Ok, for me. Thank you for drawing my attention to this point. I will provide a solution very soon.

👍 1

alagrede self-assigned this on Feb 4, 2021

alagrede added this to the **0.5.3** milestone on Feb 4, 2021

alagrede commented on Feb 4, 2021 Owner

Fix in 0.5.3. It's coming on Windows/Mac App stores.

🎉 1

alagrede closed this as completed on Feb 4, 2021

Assignees

alagrede

Labels

enhancement

Projects

None yet

Milestone

0.5.3

Development

No branches or pull requests

2 participants