New issue

Jump to bottom

Cross Site Scripting vulnerability #137

Open **notaisy** opened this issue on May 17, 2021 · 1 comment

notaisy commented on May 17, 2021

Hi, I'd like to report a security vulnerability in lastest release :

Description: Cross-site scripting (XSS) vulnerability(also execute constructed malicious code)
Date: 2021.05.17
Version: v1.26.2~v1.34.0
Tested on: Windows10 & Mac

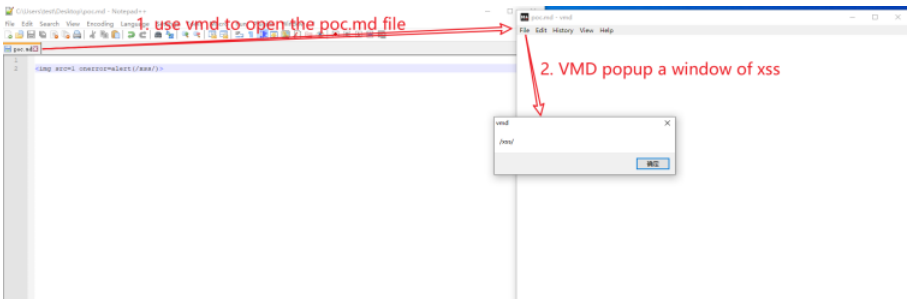
POC

The program does not properly handle the content of the code, causing the program to have a cross-site scripting vulnerability, which can also execute constructed malicious code

1. creat poc.md file with the following content: `<img src=1 onerror=alert(/xss/)>`
2. use vmd.exe to open the poc.md ,the poc code is executed
3. pop up calc.exe

XSS

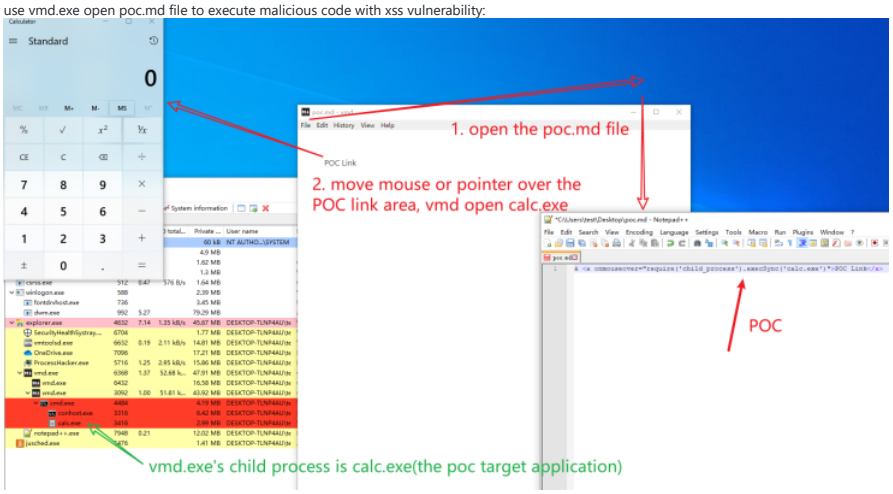
the file content code : `<img src=1 onerror=alert(/xss/)>`



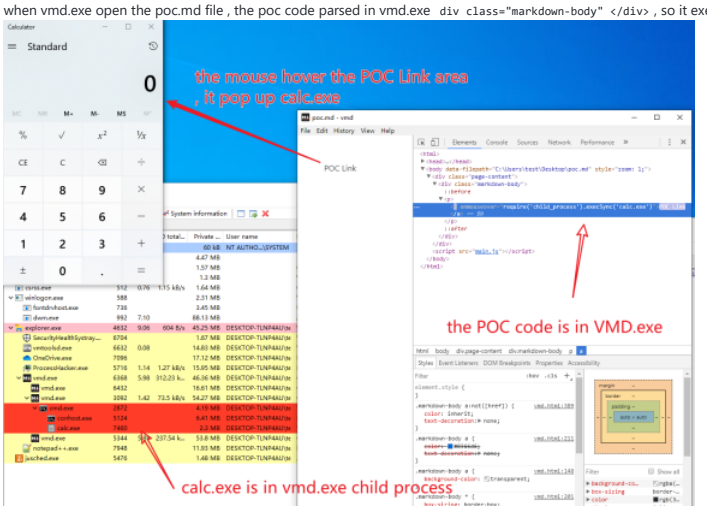
Execute malicious code

the file content code : `<a onmouseover="require('child_process').execSync('calc.exe')">POC Link</a>`

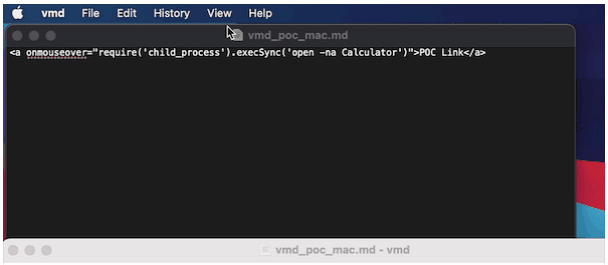
use vmd.exe open poc.md file to execute malicious code with xss vulnerability:



when vmd.exe open the poc.md file , the poc code parsed in vmd.exe `<div class="markdown-body"></div>` , so it executed:



Use the Poc `<a onmouseover="require('child_process').execSync('open -na Calculator')">POC Link</a>` on Mac:



POC Link

How to fix

1. Use an appropriate escaping/encoding technique depending on where user input is to be used: HTML escape, JavaScript escape, CSS escape, URL escape, etc.
2. VMD should sanitize the content in order to avoid XSS.

nu11secur1ty commented on Jul 2, 2021 • edited

Hello, notaisy, and the other friends of this project.
Yeah, buddy, I've decided to investigate this case, and yeah, there is have a big problem, only for a stupid example, if someone malicious guy sends `md` file with malicious content, and for example, the user is a real user ;) and don't know what actually is going on, the game is over for him.

debug and proof of concept:

https://streamable.com/oykc86
https://streamable.com/ngx2xm
https://streamable.com/j7e13y

BR

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants