



Published in System Weakness



Tuhin Bose

Follow

Mar 18, 2021 · 1 min read · Listen



CVE-2021-26215

Exploit Title: SeedDMS 5.1.x is affected by cross-site request forgery (CSRF) in out.EditDocument.php

Date: 15/03/21

Exploit Author: Tuhin Bose

Vendor Homepage: <https://www.seeddms.org/>

Version: 5.1.x

CVE : CVE-2021-26215

SeedDMS 5.1.x is affected by cross-site request forgery (CSRF) in out.EditDocument.php that allows an attacker to edit victim's documents. To exploit this vulnerability, an attacker has to host the html code in his server and send the link to victim.

Steps to reproduce:

1. Go to <https://localhost/out/out.MyDocuments.php>
2. Click on Edit on any document.
3. Enter some random(valid) name, comment, keyword, categories and others.
4. Click on save and capture the request using Burpsuite.
5. Right click on the request and click on "Engagement tools" "Generate CSRF poc"
6. Copy the html code and save it as csrf.html on your server.
7. Edit the csrf.html file and change the name, comment, keyword, categories and others what you want to change.
8. Open the html file and click on "submit".

You'll see that the details will be changed.

Cybersecurity

Bug hunting

Cve

Vulnerability

Infosec



116



1

Enjoy the read? Reward the writer. ^{Beta}

Your tip will go to Tuhin Bose through a third-party platform of their choice, letting them know you appreciate their story.

Give a tip

Get an email whenever Tuhin Bose publishes.

By signing up, you will create a Medium account if you don't already have one. Review our [Privacy Policy](#) for more information about our privacy practices.



Subscribe