Cyber Division Follow
Aug 2, 2021 · 1 min read · Listen

CVE-2021–35343

VIT Bhopal University

# Exploit Title: SeedDMS v5.1.x<5.1.23 and v6.0.x<6.0.16 is affected by cross-site request forgery (CSRF) in /op/op.Ajax.php
# Date: 02/08/21
# Exploit Author: Tuhin Bose, Division of Cyber Security and Digital Forensics, VIT Bhopal University
# Vendor Homepage: https://www.seeddms.org/
# Version: 5.1.x<5.1.23 and 6.0.x<6.0.16
# CVE : CVE-2021–35343
Description:
Cross-Site Request Forgery (CSRF) vulnerability in the /op/op.Ajax.php in SeedDMS v5.1.x<5.1.23 and v6.0.x<6.0.16 allows a remote attacker to edit document name without victim's knowledge, by enticing an authenticated user to visit an attacker's web page.
Steps to reproduce:
1. Login from Browser A and go to http://localhost/out/out.ViewDocument.php?documentid=<ID>
2. Edit the document name and capture the request using burpsuite.
3. Right click on the request and click on "Engagement tools" → "Generate CSRF poc"
4. Copy the html code and save it as csrf.html on your server.
5. Edit the csrf.html file and change the name with any name that you want to change.
6. Now login from Browser B.
7. Open the html file and click on "submit".
You'll see that the document name will be changed.

Cybersecurity Cve Bug Bounty Infosec Vit Bhopal University