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

CVE-2021–36543

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.UnlockDocument.php
Date: 02/08/21
Exploit Author:
(i) Tuhin Bose, Division of Cyber Security and Digital Forensics, VIT Bhopal University
(ii) Fardeen Ahmed, Division of Cyber Security and Digital Forensics, VIT Bhopal University
(iii) Sumon Nath, Division of Cyber Security and Digital Forensics, VIT Bhopal University
(iv) Saket Upadhay, Division of Cyber Security and Digital Forensics, VIT Bhopal University
(v) Shishir Kumar Shandilya, Division of Cyber Security and Digital Forensics, VIT Bhopal University
(vi) Manas Kumar Mishra, 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.UnlockDocument.php in SeedDMS v5.1.x<5.1.23 and v6.0.x<6.0.16 allows a remote attacker to unlock any document without victim's knowledge, by enticing an authenticated user to visit an attacker's web page.
Steps to reproduce:
1. Login with the admin account.
2. Visit this URL: http://localhost/op/op.UnlockDocument.php?documentid=<ID>
You'll see that the document will be unlocked.

Cve Bug Bounty Cybersecurity Infosec Vit Bhopal University