

[New issue](#)[Jump to bottom](#)

Store Cross Site Scripting Vulnerability on "users_alerts" in rukovoditel 2.7.2 #4

🔒 Closed

r0ck3t1973 opened this issue on Dec 15, 2020 · 1 comment

r0ck3t1973 commented on Dec 15, 2020

[Owner](#)

/Describe the bug/

I download install rukovoditel 2.7.2

An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "users_alerts" feature.

To Reproduce

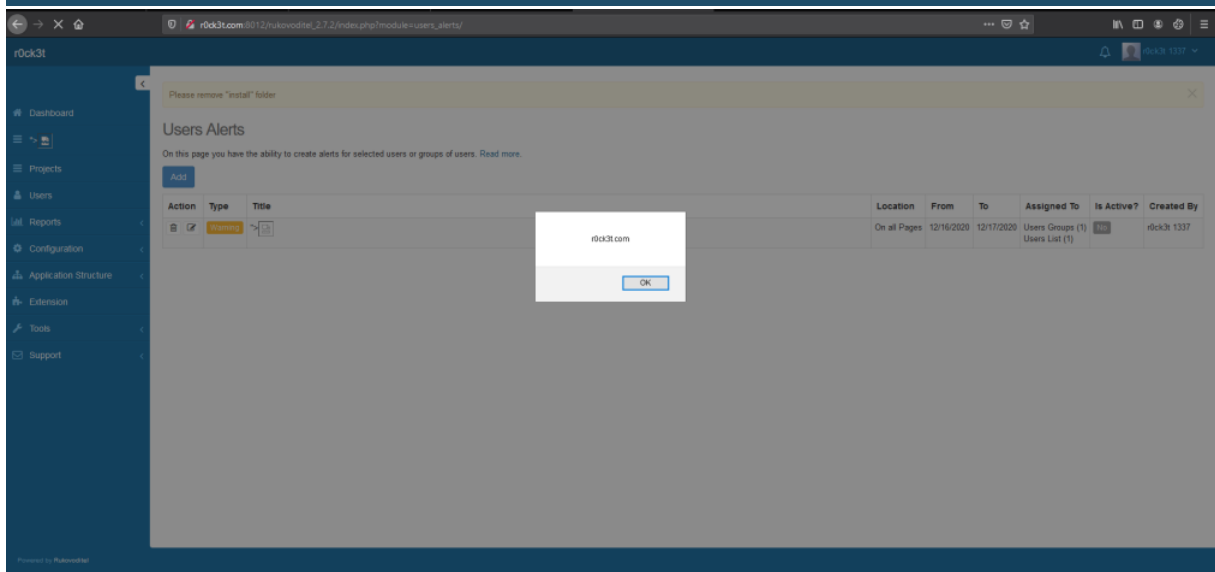
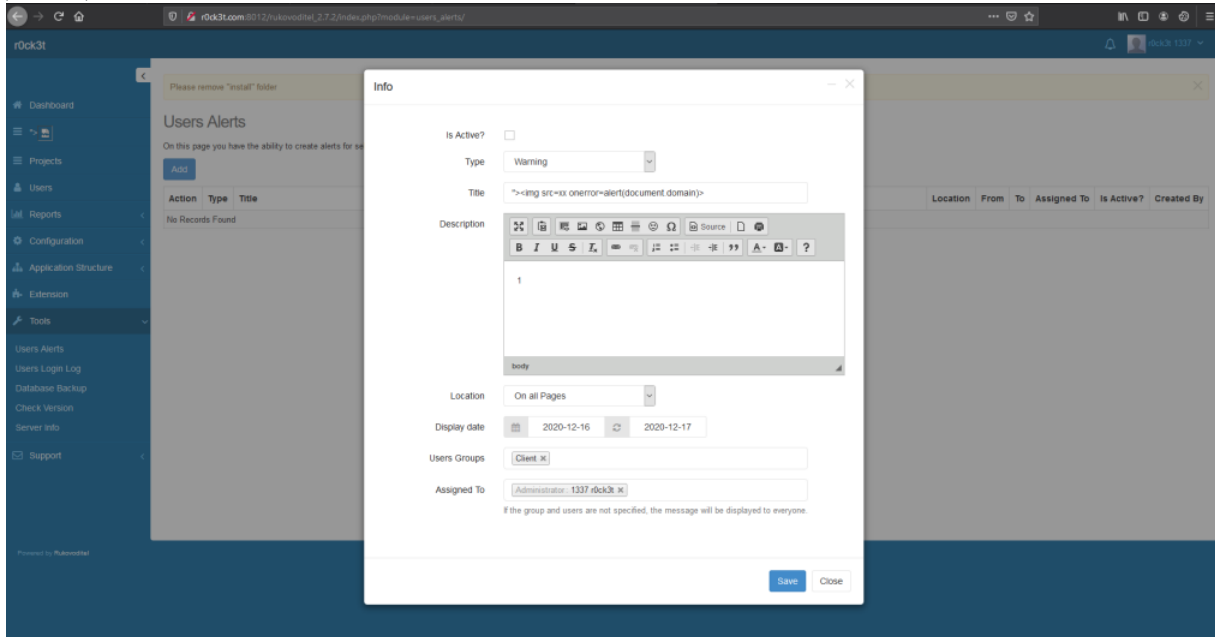
/Steps to reproduce the behavior/:

1. Login into the panel
2. Go to '/rukovoditel_2.7.2/index.php?module=users_alerts/'
3. Add new 'users_alerts'
4. Insert payload: ">
5. Save and BOOM!!!! Alert XSS Message

/Expected behavior/

The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page.

/Screenshots/



r0ck3t1973 commented on Jul 10, 2021

Owner

Author

[CVE-2020-35984](#)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

