

New issue

[Jump to bottom](#)

Stored Cross Site Scripting Vulnerability on "Users Alerts" in rukovoditel 3.2.1 #7

✓ Closed anhdq201 opened this issue on Oct 9 · 1 comment

anhdq201 commented on Oct 9

Owner

Version: 3.2.1

Description

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

Proof of Concept

Step 1: Go to `/index.php?module=users_alerts/users_alerts`, click "Add" and insert payload `` in Title field.

rukovoditel | Users Alerts

localhost:13338/index.php?module=users_alerts/

Incognito

rukovoditel.demo

localhost:13338 says
cookie_test=please_accept_for_session;
sid=nomms0shdbbh9rcr934gre6grh5; user_skin=blue

administrator test

Dashboard

test

Projects

test 2

Users

__script_alert(1)/script_

__script_alert(1)/script_

Reports

Configuration

Application Structure

Extension

Tools

Documentation

Users Alerts

On this page you have the ability to create alerts for selected users or groups of users. [Read more.](#)

Add

Action	Type	Title	Location	From	To	Assigned To	Is Active?	Created By
	Success		On all Pages				Yes	administrator test
	Warning	test	On all Pages				Yes	administrator test

Impact

If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user.



anhdq201 closed this as completed on Oct 9



anhdq201 reopened this on Oct 23

anhdq201 commented 24 days ago

Owner

Author

[CVE-2022-43167](#)



anhdq201 closed this as completed 24 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

