Reflected XSS In User/Roles Function in pimcore/pimcore

0

✓ Valid Reported on Sep 14th 2022

Description

URL: https://demo.pimcore.fun/admin/
In Setting select User/Roles and select User. After created user, move to Workspace tab and inject payload XSS at Documents, Assets and Data Objects. XSS payload will be trigger. Besides, Workspace in Roles Also having the same situation. Can you create Role and move to Workspace tab and inject payload to Documents, Assets, Data Objectes.

Proof of Concept

```
//
payload =  "><img src=x onerror=alert(2)>
```

Image PoC: ![PoC_Image](https://drive.google.com/file/d/1oUR2JXF8jQ1YMpuKNNqKe8TAJaCuZwL8/view?usp=sharing "poc")

Impact

If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user. Amongst other things, the attacker can:
Perform any action within the application that the user can perform. View any information that the user is able to view. Modify any information that the user is able to modify. Initiate interactions with other application users, including malicious attacks, that will appear to originate from the initial victim user.

CVE
CVE-2022-3255
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Reflected

CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
Medium (6.8)

Registry
Other

Affected Version
v10.5.5

Visibility
Public

Status
Fixed

Found by

tunght
@ht11761
amateur ✓

This report was seen 2,385 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 2 months ago

tunght modified the report 2 months ago

We have contacted a member of the **pimcore** team and are waiting to hear back 2 months ago

A **pimcore/pimcore** maintainer has acknowledged this report 2 months ago

JiaJia Ji modified the Severity from High (8.8) to Medium (6.8) 2 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

JiaJia Ji validated this vulnerability 2 months ago

tunght has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Chat with us

The researcher's credibility has increased: +7

The researcher's credibility has increased: +7

JiaJia Ji marked this as fixed in 10.5.7 with commit 1e916e 2 months ago

The fix bounty has been dropped ×

This vulnerability will not receive a CVE ×

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us