huntr

Cross-site Scripting (XSS) - Stored in pimcore/pimcore

0

✓ Valid Reported on Jan 17th 2022

Description

stored xss vulnerability occurs when you change the value of Group at "Settings" => "Thumbnalis" => "Video Thumbnails" in the pimcore service.

Proof of Concept

```
XSS POC : "><img src=x onerror=alert(document.domain)>

1. Open the https://10.x-dev.pimcore.fun/admin/login?perspective=
2. After login, Go to "Settings" => "Thumbnalis" => "Video Thumbnails"
3. Change the value of Group to XSS PoC
4. Reflesh
```

Impact

Through this vulnerability, an attacker is capable to execute malicious scripts.

CVE
CVE-2022-0285
(Published)

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

Severity
Medium (6.6)

Visibility
Public

Status
Fixed

Found by

TroubleMaker

@inweol

noisy

Fixed by

Divesh Pahuja

@dvesh3

maintainer

This report was seen 350 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 10 months ago

We have contacted a member of the **pimcore** team and are waiting to hear back 10 months ago

Divesh Pahuja validated this vulnerability 10 months ago

TroubleMaker has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Divesh Pahuja marked this as fixed in 10.2.9 with commit b43222 10 months ago

Divesh Pahuja has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us