huntr

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

1

✓ Valid Reported on Jan 26th 2022

Vuln : Stored XSS

Description

The pimcore/pimcore package is an open source platform that provides PIM, MDM, CDP, DAM, DXP/CMS & Digital Commerce services. stored xss vulnerability occurs when you change the value of name at "Setinngs" => "Website Settings" 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 "Setinngs" => "Website Settings"
3. Change the value of name to XSS PoC
4. Reflesh

Video : https://www.youtube.com/watch?v=k-aQ4RpJ1Po
```

Impact

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

CVE
CVE-2022-0509
(Published)

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

Severity
Medium (6.6)

Chat with us

Visibility

Public

Status

Fixed

Found by

Pocas

@p0cas

amateur

Fixed by

Divesh Pahuja

@dvesh3

maintainer

This report was seen 371 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

Pocas modified the report 10 months ago

Pocas modified the report 10 months ago

Pocas modified the report 10 months ago

We have sent a follow up to the **pimcore** team. We will try again in 7 days. 10 months ago

Pocas 10 months ago

Researcher

hey

We have sent a second follow up to the **pimcore** team. We will try again in

Chat with us

Divesh Pahuja validated this vulnerability 10 months ago

Divesh Pahuja validated this vulnerability 10 months ago

Pocas has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Divesh Pahuja marked this as fixed in 10.3.1 with commit 6ccb5c 10 months ago

Divesh Pahuja has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec