huntr

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

0

✓ Valid Reported on Dec 24th 2021

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 rule name in the admin dev page.

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 "Online Shop" => "Pricing Rules"
3. Change the name of the rule to XSS POC
4. Refresh

Video : https://www.youtube.com/watch?v=7sTclCmH1rY
```

Impact

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

CVE
CVE-2022-0257
(Published)

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

Severity
Medium (6.1)

Chat with us

Visibility
Public

Public

Status

Fixed

Found by

Pocas

@p0cas

amateur ✓

Fixed by

Bernhard Rusch

@brusch

maintainer

This report was seen 381 times.

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

Pocas modified the report a year ago

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

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

Pocas a year ago Researcher

When will the maintainer check this?

Pocas modified the report a year ago

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

Pocas a year ago Researcher

Hey

Chat with us

We have sent a third and final follow up to the **pimcore** team. This report is now considered stale. 10 months ago

Bernhard Rusch validated this vulnerability 10 months ago

Pocas has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bernhard Rusch marked this as fixed with commit dfaf78 10 months ago

Bernhard Rusch has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation