huntr

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

0

✓ Valid Reported on Feb 7th 2022

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 Abbreviation, Longname, Converter Service at "Settings" => "Data Objects" => "Quantity Value" 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" => "Data Objects" => "Quantity Value"
3. Change the value of Abbreviation, Longname, Converter service to XSS PoC
4. Reflesh

Video : https://www.youtube.com/watch?v=c8waBKF5VAQ
```

Impact

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

CVE
CVE-2022-0705
(Published)

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

Severity

Medium (4.2)

Visibility

Public

Status

Fixed

Found by

Pocas

@p0cas

amateur ✓

Fixed by

Divesh Pahuja

@dvesh3

maintainer

This report was seen 424 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

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

Pocas 9 months ago

Researcher

hey

We have sent a second follow up to the **pimcore** team. We will try again in 10 days. 9 months ago

Divesh Pahuja modified the report 9 months ago

Divesh Pahuja validated this vulnerability 9 months ago

Pocas has been awarded the disclosure bounty ✓

Chat with us

The fix bounty is now up for grabs

We have sent a fix follow up to the **pimcore** team. We will try again in 7 days. 9 months ago

We have sent a second fix follow up to the **pimcore** team. We will try again in 10 days. 9 months ago

Pocas 9 months ago Researcher

Hello :) when wiil you patch ?

Pocas 9 months ago Researcher

update?

Divesh Pahuja 9 months ago Maintainer

Hi @Pocas we are working on generic approach to fix XSS issues. The PR https://github.com/pimcore/pimcore/pull/11447 is already there and soon it will be merged. thanks!

Pocas 9 months ago Researcher

Thanks maintainer!

We have sent a third and final fix follow up to the **pimcore** team. This report is now considered stale. 8 months ago

Divesh Pahuja marked this as fixed in **10.4.0** with commit **6e0922** 8 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

Chat with us