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

0

Valid Reported on Jan 17th 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 add media query at "Settings" => "Thumbnails" => "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" => "Thumbnails" => "Video Thumbnails"
3. Click the Any Video
4. Click the Add Media Segment Button
5. Enter the XSS POC and Click the OK
6. Add Transformations!!
7. Reflesh

Video : https://youtu.be/OZQqIugDyBE
```

Impact

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

CVE
CVE-2022-0262
(Published)

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

Severity

Severity
Medium (6.6)

Visibility
Public
Status
Fixed

Found by

Pocas
@p0cas
amateur

Fixed by

Bernhard Rusch
@brusch
maintainer

This report was seen 368 times.

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

Pocas modified the report 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 in **10.2.7** with commit **6f36e8** 10 months ago

Bernhard Rusch has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation

Chat with us