

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

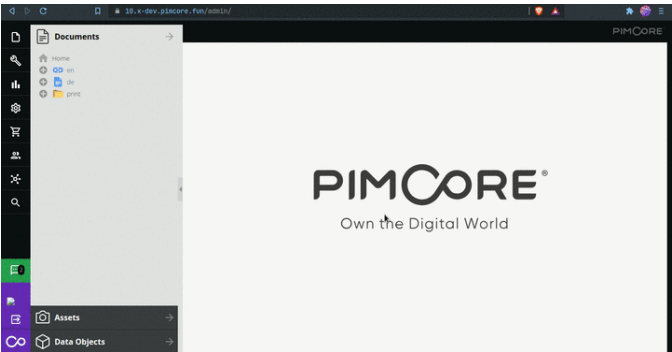
Valid Reported on Aug 27th 2021

0

Description

pimcore is a Open Source Data & Experience Management Platform (PIM, MDM, CDP, DAM, DXP/CMS & Digital Commerce) this package is vulnerable for Stored XSS custom meta data

Proof of Concept



Impact

This vulnerability is capable of Stored XSS

Occurrences

EmbeddedMetaDataTrait.php L41

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

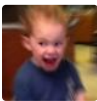
Severity
Medium (5.5)

Affected Version
*

Visibility
Public

Status
Fixed

Found by



Abdul muhaimin

@b1nslashsh

unranked

Fixed by



Bernhard Rusch

@brusch

maintainer

This report was seen 528 times.

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

Bernhard Rusch validated this vulnerability a year ago

Abdul muhaimin has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bernhard Rusch marked this as fixed with commit 79a575 a year ago

Bernhard Rusch has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

Sign in to join this conversation

2022 © 418sec

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)