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

1

Valid Reported on Jan 21st 2022

Description

Reflected cross site scripting vulnerability in pimpore/pimcore , it is in group field in Field collections and objectbricks in settings module.

Proof of Concept

1 .Login to demo account
2 . Go to settings module -->data objects -->object bricks or Field collection --> edit any one and add payload in group name
3 .Click Save xss will trigger

Impact

This vulnerability is capable of stolen the user cookie

CVE
CVE-2022-0510
(Published)

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

Severity
Medium (4.3)

Visibility
Public

Status
Fixed

Found by

Asura-N
@asura-n

@asura-n

noisy

Fixed by

Divesh Pahuja

@dvesh3

maintainer

This report was seen 427 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

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

Divesh Pahuja validated this vulnerability 10 months ago

Asura-N 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 **b5a9ad** 10 months ago

Divesh Pahuja has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation