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

0

Valid Reported on Mar 9th 2022

Description

pimcore datahub is vulnerable to Stored XSS in multiple places including:
(1) Field-Collections in Data Objects
(2) Objectbricks in Data Objects

Proof of Concept (for both 1 & 2)

Step 1: Go to https://10.x-dev.pimcore.fun/admin/ and login.
Step 2: Click Settings > Data Objects > Field-Collections / Objectbricks > Add
Step 3: Input aaa so as to capture legitimate POST request in Burp Suite
Step 4: Modify value of the "key" parameter in the body of POST request as below, which is URL encoded
"><img+src%3dx+onerror%3dalert(document.domain)>
Step 5: Forward the request
You will see the an alert box prompt whenever you access Field-Collections / Objectbricks

Impact

This vulnerability is capable for letting attacker potentially steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie.

CVE
CVE-2022-0911
(Published)

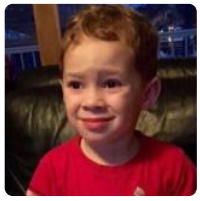
Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.8)

Visibility
Public

Status
Fixed

Found by



James Yeung
@scriptidiot
unranked

Fixed by

Divesh Pahuja
@dvesh3
maintainer

This report was seen 520 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 9 months ago

James Yeung modified the report 9 months ago

Divesh Pahuja validated this vulnerability 9 months ago

James Yeung has been awarded the disclosure bounty ✔

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. 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