Stored XSS on Admin Translations in pimcore/pimcore

0

Valid Reported on Aug 7th 2022

Description

Key/Name field in Admin Translation Settings is vulnerable to XSS.

Proof of Concept

1 - Go to Settings, Admin Translations.
2 - Click on Add, and put the XSS payload: "><iframe onload=confirm(1)> on Name then save
3 - XSS popup will be triggered.
Both Stable and Dev versions are vulnerable.

Video PoC

```
https://drive.google.com/drive/folders/15PhgJyEmIoyLJPgxz5Wb-Hy4HxN2E6_V?us
```

Impact

Steal Admin Cookies and gain unauthorized privileged access.

CVE
CVE-2022-2796
(Published)

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

Severity
Medium (6.7)

Registry
Other

Affected Version
11.x

Visibility
Public

Status
Fixed

Found by

Amine
@ahkecha
legend

Fixed by

Divesh Pahuja
@dvesh3
maintainer

This report was seen 776 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 4 months ago

We have contacted a member of the **pimcore** team and are waiting to hear back 4 months ago

We have sent a follow up to the **pimcore** team. We will try again in 7 days. 4 months ago

Divesh Pahuja validated this vulnerability 3 months ago

Amine has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the **pimcore** team. We will try again in 7 days. 3 months ago

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

Divesh Pahuja marked this as fixed in 10.5.4 with commit 2fd468 3 months ago

Divesh Pahuja has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation