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

0

Valid Reported on Jan 19th 2022

Description

Pimcore settings module is vulnerable to stored cross site scripting

Proof of Concept

1 . Login to dev demo account. https://10.x-dev.pimcore.fun/
2 . Goto settings -->data objects -->Add a new class --> add payload in icon field
3 . Click save and close and open that class alert will trigger
payload "><iMg SrC="x" oNeRRor="alert(document.domain);">

Impact

This vulnerability is capable of stolen the user cookie

CVE
CVE-2022-0348
(Published)

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

Severity
Medium (4.3)

Visibility
Public

Status
Fixed

Found by

Asura-N
@asura-n
noisy

noisy

Fixed by

JiaJia Ji

@kingjia90

maintainer

This report was seen 391 times.

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

Asura-N modified the report 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

Divesh Pahuja validated this vulnerability 10 months ago

Asura-N has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

JiaJia Ji marked this as fixed in **10.2** with commit **832c34** 10 months ago

JiaJia Ji has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

> Sign in to join this conversation