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

0

Valid Reported on Feb 7th 2022

Description

Cross site scripting vulnerability in pimcore,pimcore field, it is fixed in this commit 832c34 , but still it is executing xss .Icon field in events and news

Proof of Concept

1 . Login to the demo account https://10.x-dev.pimcore.fun/admin/
Go to settings -->data objects --> classes --> Events icon field --> add payload and click save
Go to data objects tab which is located at the bottom, go to events folder and extend alert will trigger .
payload = "><iMg SrC="x" oNeRRor="alert(1);">

Impact

This vulnerability is capable of stolen the user cookie

CVE
CVE-2022-0704
(Published)

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

Severity
Medium (4)

Visibility
Public

Status
Fixed

Found by
Asura-N

Asura-N

@asura-n

noisy

Fixed by

Divesh Pahuja

@dvesh3

maintainer

This report was seen 420 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

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

We have sent a second follow up to the **pimcore** team. We will try again in 10 days. 9 months ago

Divesh Pahuja modified the report 9 months ago

Divesh Pahuja validated this vulnerability 9 months ago

Asura-N 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. 9 months ago

We have sent a second fix follow up to the **pimcore** team. We will try again in 10 days. 9 months ago

We have sent a third and final fix follow up to the **pimcore** team. This repor
stale. 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