huntr

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

0

✓ Valid Reported on Mar 8th 2022

Description

pimcore datahub is vulnerable to Stored XSS in the Unique Indetifier of the function of "Add a new configuration" in Datahub. Whenever an admin user access data hub, a stored XSS will be triggered.

Proof of Concept

Step 1: Go to https://demo.pimcore.fun/admin/ and login.
Step 2: Click Datahub
Step 3: Click Add Configuration
Step 4: Input aaa so as to capture legitimate request in Burp Suite
Step 5: Modify value of the name parameter in the GET request as below, which is URL encoded
"><img+src%3dx+onerror%3dalert(1)%3b>
Step 6: Forward the request
You will see the an alert box prompt wheenver you access Datahub

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.

Occurrences

ConfigController.php L46-L65

There is no any input sanitzation from client (e.g. html characters escape)

CVE
CVE-2022-0955
(Published)

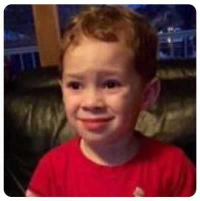
Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by



James Yeung
@scriptidiot
unranked

Fixed by

Divesh Pahuja
@dvesh3
maintainer

This report was seen 535 times.

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

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

Divesh Pahuja 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

James Yeung 9 months ago Researcher

May I know if CVE ID could be assigned in this case? Thanks!

James Yeung 9 months ago Researcher

Forgot to tag @admin

Jamie Slome 9 months ago Admin

We have not automatically assigned a CVE here as we only do this for the top 40% of popular packages/repositories on GitHub.

However, if requested manually, we can if the maintainer is happy to publish a CVE.

@maintainer - are you happy for us to assign and publish a CVE?

We have sent a fix follow up to the **pimcore/data-hub** team. We will try again in 7 days.
8 months ago

Divesh Pahuja 8 months ago Maintainer

@admin yes, go ahead!

Jamie Slome 8 months ago Admin

Sorted! ♥ Let me know once you are ready to publish this report and I will make the CVE live in the MITRE/NVD database.

Divesh Pahuja marked this as fixed in **1.2.4** with commit **15d5b5** 8 months ago

Divesh Pahuja has been awarded the fix bounty ✓

Chat with us

This vulnerability will not receive a CVE ✗

ConfigController.php#L46-L65 has been validated ✓

James Yeung 8 months ago

Researcher

@admin, may I know if its normal for waiting days to have update on https://nvd.nist.gov/vuln/detail/CVE-2022-0955

Since I found other CVEs will get an update after 2-3 days only. Thanks!

Jamie Slome 8 months ago

Admin

@scriptidiot - thanks for the nudge here. This is only because the CVE was assigned manually. Publishing the CVE for you now - it should be live in 1 hour.

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

part of 418sec

company

about

team

Chat with us

Chat with us