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

0

Valid Reported on Dec 22nd 2021

Description

Stored cross site scripting vulnerability in report class field on custom report feature.

Proof of Concept

1 . Login to dev account https://10.x-dev.pimcore.fun/admin/
2 . Go to marketing --> custom reports --> Report class :field in left navigation menu
3 . Add payload "><iMg SrC="x" oNeRRor="alert(1);"> in report class field and click save and reload
4 . go to custom reports alert will trigger
payload "><iMg SrC="x" oNeRRor="alert(1);">

Impact

This vulnerability is capable of stolen the user cookie

Occurrences

CustomReportController.php L298

CVE
CVE-2022-0256
(Published)

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

Severity
Medium (5.3)

Visibility
Public

Status
Fixed

Found by

Asura-N

@asura-n

noisy

Fixed by

Bernhard Rusch

@brusch

maintainer

This report was seen 357 times.

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

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

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

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

We have sent a third and final follow up to the **pimcore** team. This report is now considered stale. 10 months ago

Bernhard Rusch validated this vulnerability 10 months ago

Asura-N has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bernhard Rusch marked this as fixed with commit **dff1cb** 10 months ago

Bernhard Rusch has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

CustomReportController.php#L298 has been validated ✔

Sign in to join this conversation