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

0

Valid Reported on Feb 27th 2022

Description

pimcore is vulnerable to Stored XSS at **Key** field in the **Navigation & Properties** tab of a Document page.

Payload

```
"><img src=x onerror=alert(1);>
```

Step to reproduce

1.Go to `https://demo.pimcore.fun/admin/` and login.
2.Click on any document (**Home, de**,...) in the **Documents**
3.Go to **Navigation & Properties** tab, in the **Key** column, input payload `"><img src=x onerror=alert(1);>` into the **Key** field of any record.
You will see the XSS popup triggers.

Impact

This vulnerability has the potential to steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie.

Occurrences

JS properties.js L39-L227 JS properties.js L14-L36 JS properties.js L241-L273

CVE
CVE-2022-0831
(Published)

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

CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
Medium (4.6)

Visibility
Public

Status
Fixed

Found by

KhanhCM
@khanhchauminh
pro

Fixed by

JiaJia Ji
@kingjia90
maintainer

This report was seen 557 times.

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

We have contacted a member of the **pimcore** team and are waiting to hear back 9 months ago

Divesh Pahuja modified the report 9 months ago

JiaJia Ji validated this vulnerability 9 months ago

KhanhCM has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

JiaJia Ji marked this as fixed in **10.3.3** with commit **e786fd** 9 months ago

JiaJia Ji has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

properties.js#L241-L273 has been validated ✔

properties.js#L14-L36 has been validated ✔

properties.js#L39-L227 has been validated ✔

> Sign in to join this conversation