splitbrain / **dokuwiki** Public

Code · Issues 349 · Pull requests 78 · Actions · Projects 3 · ...

New issue

Jump to bottom

Possible XSS vulnerability #3651

Closed **enferas** opened this issue on Mar 30 · 3 comments

Labels	Bug **Category: Backend**
Projects	Release "Igor"

enferas commented on Mar 30

Hello,

I would like to report for possible XSS vulnerability.

The source in this file https://github.com/splitbrain/dokuwiki/blob/master/vendor/openpsa/universalfeedcreator/lib/Creator/HTMLCreator.php Line 157 in function _generateFilename.

While the sink in this https://github.com/splitbrain/dokuwiki/blob/master/feed.php line 103.

I tried to test the pathinfo function in PHP. And I found it is possible to bypass this function with this example.

```
<?php
$path_parts = pathinfo('/path/<img src="aaa.img" onerror=alert(document.cookie);>');

echo $path_parts['basename'], "\n"; // XSS
```

mprins commented on Mar 30 Contributor

This seems to be something in this 3rd party library and it's not clear if is it is a vulnerability in DokuWiki which has quite a bit of sanitising code.

In the meantime please report this to the authors of the `universalfeedcreator` package as listed in https://github.com/splitbrain/dokuwiki/blob/master/vendor/openpsa/universalfeedcreator/composer.json

enferas commented on Apr 4 Author

Thank you for the response.

After contacting the vendor the vulnerability is confirmed and the fixed is done in this push.
flack/UniversalFeedCreator@ `e4736a6`

I just would like to mention that the source was coming from the vendor while the sink was in feed.php file.

Klap-in added this to **Triage** in **Release "Igor"** via automation on May 3

Klap-in added **Category: Backend** Bug labels on May 3

splitbrain closed this as completed in `d323398` on May 12

Release "Igor" automation moved this from **Triage** to **Done** on May 12

enferas commented on Jun 13 Author

CVE-2022-28919 is assigned to this vulnerability.
Thank you.

Assignees

No one assigned

Labels

Bug **Category: Backend**

Projects

Release "Igor"
Done

Milestone

No milestone

Development

No branches or pull requests

3 participants