huntr

Path Traversal in bookstackapp/bookstack

0

✓ Valid Reported on Oct 7th 2021

Description

A path traversal vulnerability in BookStacks export function allows for the exposure of sensitive files in local or local_secure Laravel filesystems.

Proof of Concept

1: Write the following in a new page:

```
<p id="bkmrk-"><img src="http://[BOOKSTACK_URL]/uploads/images/../../.htacc
```

2: Export in contained HTML to find the .htaccess file base64 encoded
3: If the STORAGE_IMAGE_TYPE in .env is set to local_secure, then it is possible to obtain the Laravel log file via the following payload:

```
<p id="bkmrk-"><img src="http://10.0.2.15/uploads/images/../../logs/laravel
```

Impact

This vulnerability is capable of exposure of sensitive log/configuration files present in the Laravel filesystems.

Occurrences

ImageService.php L414L442

CVE
CVE-2021-3874
(Published)

Vulnerability Type
CWE-22: Path Traversal

Severity
Medium (4.3)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

Fixed by

Dan Brown
@ssddanbrown
maintainer

This report was seen 479 times.

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

Dan Brown a year ago Maintainer

Chat with us

As mentioned on the other issue, Patch is in progress for this one but need to prepare to push the fix alongside a release and security announcement.

@admin If I mark this as valid, What is the scope of visibility for this report? I'd like to mark this as valid now but wouldn't really want this to become visible to anyone else outside of the original reporter, the main huntr team and myself.

haxatron a year ago Researcher

Hi there, thanks for reviewing my reports! So far, only the CWE of the report and the application will be listed on my profile but not the report itself. The whole report will only be disclosed after a fix is submitted. If you would like, @admin can confirm this statement.

Jamie Slome a year ago Admin

The report remains private until the fix is confirmed.

Dan Brown a year ago Maintainer

Thanks both! Will therefore mark this one valid now and will look to confirm the patch in the next day or so.

Dan Brown validated this vulnerability a year ago

haxatron has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Dan Brown marked this as fixed with commit 7224fb a year ago

Dan Brown has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

ImageService.php#L414L442 has been validated ✓

Sign in to join this conversation