

Cross-Site Scripting Through Link Attachments

Low ssddanbrown published GHSA-7p2j-4h6p-cq3h on Oct 31, 2020

Package	
BookStack	
Affected versions	Patched versions
< v0.30.4	v0.30.4

Description

Impact

A user with permissions to edit a page could add an attached link which would execute untrusted JavaScript code when clicked by a viewer of the page.

Patches

The issue was addressed in BookStack v0.30.4.

Dangerous content may remain in the database after this update. If you think this could have been exploited you can search your database for potential cases with the following SQL command:

```
select a.name as attachment_name, p.name as page_name, p.id as page_id from attachments a left join pages p on (a.uploaded_to=p.id) where a.path like '%javascript:%';
```

Workarounds

Page edit permissions could be limited to only those that are trusted until you can upgrade although this will not address existing exploitation of this vulnerability.

References

- BookStack Beta v0.30.4
- BookStack Blog Post

Attribution

- Thanks to Yassine ABOUKIR (<https://twitter.com/yassineaboukir/>) for the discovery and reporting of this vulnerability.

For more information

If you have any questions or comments about this advisory:

- Open an issue in [the BookStack GitHub repository](#).
- Ask on the [BookStack Discord chat](#).
- Follow the [BookStack Security Advice](#) to contact someone privately.

Severity

Low


CVE ID

CVE-2020-26210

Weaknesses

No CWEs

Credits

 yassineaboukir