New issue

Jump to bottom

Possible Cross site scripting (XSS) #850

Closed **Rishivarkumar** opened this issue on Dec 18, 2019 · 1 comment · Fixed by #858

Assignees

Milestone 4.2.2

Rishivarkumar commented on Dec 18, 2019 • edited

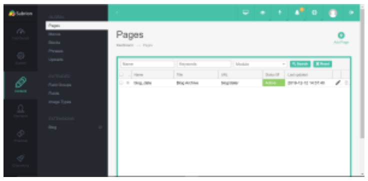
SCOPE:
Package: Subrion CMS
Version: 4.2.1
ISSUE: XSS

Vulnerability Description: The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. As a result, an attacker can inject and execute arbitrary HTML and script code in user's browser in context of a vulnerable website.

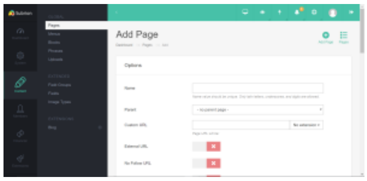
Vulnerability Classification:
CWE: 79
CVSS3Basescore: 6.1
CVSS: 3.5 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:H

Steps To Reproduce:

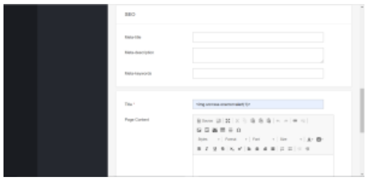
- Login
- Click on contents->Pages->Add page



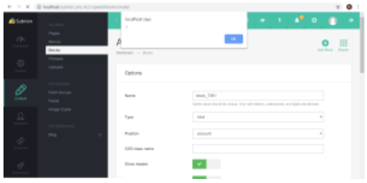
- Fill the details



In title give the payload



- Now click on blocks while adding a new block XSS is being triggered.



Reference: https://cwe.mitre.org/data/definitions/79.html
Mitigations:

- Perform sanitization of input data before inserting it into the page content.
- Escaping user input.
- Validating user input.

4unkur added a commit that referenced this issue on Feb 26, 2020

Resolves #850 2357f4b

4unkur self-assigned this on Feb 26, 2020

4unkur commented on Feb 26, 2020 Member

@Rishivarkumar
Thank you for your report. The patch will be released soon

4unkur added a commit that referenced this issue on Feb 27, 2020

`#850 additional escaping in menu ul` 8c5e2fa

4unkur linked a pull request on Feb 27, 2020 that will close this issue

Resolves #850 #858 Merged

vbezruchkin closed this as completed in #858 on Feb 27, 2020

vbezruchkin pushed a commit that referenced this issue on Feb 27, 2020

`Resolves #850` 06950c2

vbezruchkin pushed a commit that referenced this issue on Feb 27, 2020

`#850 additional escaping in menu ul` 0e9180d

4unkur added this to the **4.2.2** milestone on Feb 28, 2020

Assignees

4unkur

Labels

None yet

Projects

None yet

Milestone

4.2.2

Development

Successfully merging a pull request may close this issue.

Resolves #850
intelliants/subrion

2 participants