

## Announcement/XSS attack

[Browse history interactively](#)

[VisualWikitext](#)

**Revision as of 12:06, 26 April 2022** ([view source](#))

[Margit Link-Rodrigue](#) ([talk](#) | [contribs](#))

[m](#) ((username removed) (log details removed))

[← Older edit](#)

**Revision as of 12:57, 15 June 2022** ([view source](#))

[Margit Link-Rodrigue](#) ([talk](#) | [contribs](#))

No edit summary

[Tag](#): 2017 source edit

[Newer edit →](#)

**Line 1:**

```
{ {Featurepage|featured=true|featuredesc=Patch Release 4.1.3
contains an important "'security fix"' for a "reflected XSS" attack. <span class="bi bi-exclamation-circle-fill" style="color:orange"
></span>|featurestart=04/25/2022}}
```

==Event==

XSS attack vector in "mwstake/mediawiki-component-commonuserinterface."

**Line 1:**

```
{ {Featurepage|featured=true|featuredesc=Patch Release 4.1.3
contains an important "'security fix"' for a "reflected XSS" attack.
|featurestart=04/25/2022}}
```

==Event==

XSS attack vector in "mwstake/mediawiki-component-commonuserinterface."

---

## Revision as of 12:57, 15 June 2022

---

### Event

XSS attack vector in *mwstake/mediawiki-component-commonuserinterface*.

---

## Evaluation of the vulnerability in BlueSpice

The value from 'title' parameter get's unsanitized to the output (e.g. in 'list-group-item').

[Patch release 4.1.3](#) contains an important security-fix for this attack.

The [corresponding CVE entry](#) is still pending and will be published soon. It is highly recommended that all users update their installation of BlueSpice 4 as soon as possible.