Stored XSS through code blocks with mustache expressions

Moderate **NGPixel** published **GHSA-6xx4-m8gx-826r** on Mar 13, 2021

Package

No package listed

Affected versions	Patched versions
< 2.5.190	2.5.190

Description

Impact

Wiki.js 2.5.189 and earlier is vulnerable to stored cross-site scripting through mustache expressions in code blocks. This vulnerability exists due to mustache expressions being parsed by Vue during content injection even though it is contained within a `<pre>` element.

By creating a crafted wiki page, a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the page is viewed by other users. The following example, when inserted into a markdown page, triggers javascript execution:

```
{{
  window.alert("Wiki.JS Stored XSS") }}
```

Patches

Commit `5ffa189` fixes this vulnerability by adding the v-pre directive to all `<pre>` tags during the render.

Thanks to Mina M. Edwar for reporting this vulnerability.

Severity

Moderate

CVE ID

CVE-2021-21383

Weaknesses

No CWEs