huntr

Cross-site Scripting (XSS) - Stored in vanessa219/vditor

0

✓ Valid Reported on Jan 23rd 2022

Description

The Vanessa219/vditor is a markdown editor supported by browsers. If the user passes `javascript:alert(document.domain)` as the URL value when creating a link using the markdown syntax, there is no sanitizing process and the link is created as it is.

Proof of Concept

```
XSS PoC : [xss](javascript:alert(document.domain))

1. Open the https://ld246.com/guide/markdown
2. Enter the XSS PoC
3. Click the Link

Video : https://www.youtube.com/watch?v=5zzdiBivNSs
```

Impact

Through this vulnerability, an attacker is capable to execute malicious scripts.

CVE
CVE-2022-0350
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.1)

Visibility
Public

Status

Fixed

Found by

Pocas

@p0cas

amateur

Fixed by

V

@vanessa219

unranked

This report was seen 496 times.

We are processing your report and will contact the **vanessa219/vditor** team within 24 hours.
10 months ago

Pocas modified the report 10 months ago

V validated this vulnerability 10 months ago

Pocas has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Pocas 10 months ago Researcher

Hello. when will you publish for patch of this issue? Thanks.

V marked this as fixed in **3.8.13** with commit **e912e3** 8 months ago

V has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

Sign in to join this conversation