huntr

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

0

✓ Valid Reported on Jan 22nd 2022

Description

The Vanessa219/vditor is a markdown editor supported by browsers. When a user creates a link using the markdown syntax, the server does not URL-encode the double-quotes, so the user can escape the href attribute and trigger XSS using the on* attribute.

Proof of Concept

```
XSS PoC : [xss](https://google.com/"//onmousemove="alert(document.domain))
> I can insert an onerror. But I can't log in without a Chinese phone numbe

1. Open the https://ld246.com/guide/markdown
2. Enter the XSS PoC (Strangely, it doesn't insert at once, so I have to tr
3. When the user hovers the mouse over the link, XSS is triggered via a mou

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

Impact

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

CVE
CVE-2022-0341
(Published)

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

Severity
Medium (6.6)

Chat with us

Visibility

Public

Status

Fixed

Found by

Pocas

@p0cas

amateur ✓

Fixed by

V

@vanessa219

unranked ✓

This report was seen 490 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

We have contacted a member of the **vanessa219/vditor** team and are waiting to hear back 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

V marked this as fixed in **3.8.12** with commit **219f8a** 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