huntr

stored xss due to unsantized anchor url in alvarotrigo/fullpage.js

1



✓ Valid) Reported on Apr 11th 2022

BUG

stored xss due to unsantized anchor url

SUMMURY

using fullpage.js you can create a anchor tag. But when put href in anchor then it does not sanitize the url which allow to break context of anchor element and can add our new element. I see main javascript or other javascript library like jquery are properly sanitized the url before puting in anchor tag.

STEP TO RERPDOUCE

i uses bellow code to test

```
<script type="text/javascript" src="https://cdnjs.cloudflare.com/ajax/libs/
<script type="text/javascript">
     var myFullpage = new fullpage('#fullpage', {
         anchors: ['xss1"><img src=x onerror=alert(1)>'],
         navigation: true
    });
</script>
</body>
</html>
```

4

Here see i put xss1"> in anchors array. During anchor tag creation fullpage.js does not encoded this url. So, this payload will close the existing anchor tag and create a new element . So, using this payload we can execute any javascript code .

My suggestion is before putting in anchor href ,you must encode the url using encodeURI() https://www.w3schools.com/JSREF/jsref_encodeuri.asp https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/encodeURI

i checked other library and they are properly encoded the url so that it does not break the existing element context

main-javascript

 \triangleleft

jquery

```
<!DOCTYPE html>
   <html>
   <head>
       <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.1/jc</pre>
   </head>
   <body>
           <script>
         $(document).ready(function() {
           $('#btn').click(function() {
               var link = \$("\langle a \rangle");
               link.attr("href", '#dasda"><img src=x onerror=alert(1)>');
               link.attr("title", "Google.com");
               link.text("Google");
               $(".box").html(link);
           });
            $('#btn').click();
       });
       </script>
       <div class="box" id="box"></div>
           <input type="button" id="btn" style="display:none" value="Cr</p>
   </body>
   </html>
```

 \triangleleft

Impact

stored xss.

CVE CVE-2022-1330 (Published)

Chat with us

Vulnerability Type

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

Severity

Critical (9.4)

Registry

Npm

Affected Version

3.1.2

Visibility

Public

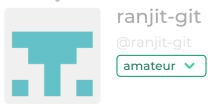
Status

Fixed

Found by



Fixed by



This report was seen 919 times

We are processing your report and will contact the alvarotrigo/fullpage.js team within 24 hours.
7 months ago

ranjit-git modified the report 7 months ago

ranjit-git submitted a patch 7 months ago

We have contacted a member of the alvarotrigo/fullpage.js team and are waiting to hear back 7 months ago

Chat with us

Maintainer

Awesome, 1	thanks	for	that!
I'll merge it	soon!		

Álvaro validated this vulnerability 7 months ago

ranjit-git has been awarded the disclosure bounty 🗸

The fix bounty is now up for grabs

Álvaro marked this as fixed in 4.0.4 with commit e7a5db 7 months ago

ranjit-git has been awarded the fix bounty 🗸

This vulnerability will not receive a CVE x

Álvaro 7 months ago Maintainer

Merged!

Sign in to join this conversation

2022 @ 418sec

huntr part of 418sec

home company

acktivity abou

eaderboard tea

Chat with us

FAQ

contact us

terms

privacy policy