Stored XSS in "Tab Image" and "Group Image" in causefx/organizr

0

✓ Valid Reported on May 24th 2022

Description

The organizr application allows malicious javascript payload in the "Tab Image" and "Group Image" for which its leads to stored XSS.

Proof of Concept 1

1.Login to the co-admin account and go to "Settings" -> "Tab Editor".
2.Now click on "Tabs" -> "Add New Tab" and filled all the details.
3.Then in "Tab Image" insert the payload `"><img src=x onerror=alert(document.cookie)>` and click on Add Tab

Proof of Concept 2

1.Login to the co-admin account and go to "Settings" -> "User Management" -> "Manage Groups".
2.Now click on "Add New Group" and filled all the details.
3.Then in "Group Image" insert the payload `"><img src=x onerror=alert(document.location)>` and click on Add Group

Video PoC

```
https://drive.google.com/file/d/1P6-Zq5D55EegVjfeLNtwG-7bU0_6mexn/view?usp=
```

Impact

This allows attackers to execute malicious scripts in the user's browser and it
session hijacking, sensitive data exposure, and worse.

CVE

CVE-2022-1909

(Published)

Vulnerability Type

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

Severity

Critical (9)

Registry

Other

Affected Version

2.1.1810

Visibility

Public

Status

Fixed

Found by

SAMPRIT DAS

@sampritdas8

pro

Fixed by

causefx

@causefx

unranked

This report was seen 617 times.

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

SAMPRIT DAS modified the report 6 months ago

We have contacted a member of the **causefx/organizr** team and are waiting
6 months ago

Chat with us

causefx validated this vulnerability 6 months ago

SAMPRIT DAS has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

causefx marked this as fixed in **2.1.2200** with commit **d5245c** 6 months ago

causefx has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

SAMPRIT DAS 6 months ago Researcher

@admin as the fix has been deployed can you assign CVE for this report?

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

part of 418sec

company

about

team

Chat with us