Multiple Stored XSS in causefx/organizr

1

Valid Reported on Apr 10th 2022

Description

The organizr application allows malicious javascript payload in multiple-input fields like "Categories", "Bookmark Tabs" and "Bookmark Categories" for which attacker can takeover the admin account.

Proof of Concept

1.Login to the co-admin account and go to go to "Settings" -> "Tab Editor".
2.Now in "Categories", "Bookmark Tabs" and "Bookmark Categories" Add options insert the below payloads:

```
<img src=x onerror=alert(document.cookie)>

<img src=x onerror=alert(document.domain)>

<img src=x onerror=alert(document.location)>
```

3.Then login with the admin account and go to "Settings" -> "Tab Editor" and visit the "Categories", "Bookmark Tabs" and "Bookmark Categories" and you will see XSS will trigger in all those fields.

PoC Video

https://drive.google.com/file/d/1n9FvXxzzmvtZc4VsdzOHl0oPxSnSDpMy/view?usp=

Impact

This allows attackers to execute malicious scripts in the user's browser and it can lead to

session hijacking, sensitive data exposure, and worse.

CVE
CVE-2022-1346
(Published)

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

Severity
Critical (9)

Registry
Other

Affected Version
1.90

Visibility
Public

Status
Fixed

Found by

SAMPRIT DAS
@sampritdas8
pro

Fixed by

causefx
@causefx
unranked

This report was seen 656 times.

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

SAMPRIT DAS modified the report 8 months ago

We have contacted a member of the **causefx/organizr** team and are waiting to hear back
8 months ago

causefx modified the report 8 months ago

causefx validated this vulnerability 8 months ago

SAMPRIT DAS has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

causefx marked this as fixed in **2.1.1810** with commit **a09d83** 8 months ago

causefx has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

SAMPRIT DAS 8 months ago — Researcher

CVSS score should be: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H admin please change it

causefx 7 months ago — Maintainer

My mistake, please change the severity as said by researcher and award the bounty

causefx 7 months ago — Maintainer

forgot to tag @admin sorry about that.

SAMPRIT DAS 7 months ago — Researcher

Also admin please change the Affected Version: 1.0.1 to 1.90

Jamie Slome 7 months ago — Admin

Sorted 👍

SAMPRIT DAS 7 months ago Researcher

@admin Can you assign CVE to this report as the @maintainer agree

causefx 7 months ago Maintainer

@admin you can assign CVE for this report

Jamie Slome 7 months ago Admin

Sorted 👍

Sign in to join this conversation