Stored XSS due to no sanitization in the filename in causefx/organizr

0

✓ Valid   Reported on Apr 10th 2022

Description

The organizr application doesn't sanitize malicious javascript payload which leads to stored XSS and can also perform to the takeover admin account.

Proof of Concept

1.Login with Co-admin account and go to "Settings" -> "Image Manager" and upload any small size jpeg image and intercept the request on burp suite.
2.Then change the name of the uploaded image with the below XSS payload and forward the request:

```
<img src=1 onerror=alert(1337)>.jpeg
```

3.Then login with admin account and go to "Settings" -> "Image Manager" and open the uploaded image by Co-admin you will see that XSS will trigger.

PoC Video

```
https://drive.google.com/file/d/1X8-YyNkt8-MBLY2Btezn2Wel6HLjyhtu/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.

Chat with us

CVE

CVE-2022-1344
(Published)

Vulnerability Type

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

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 683 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

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

Chat with us

8 months ago

causefx 8 months ago Maintainer

Not sure how to get huntr.dev to assign CVE

SAMPRIT DAS 8 months ago Researcher

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

SAMPRIT DAS 8 months ago Researcher

maintainer no problem you just validate the report @admin will assign CVE for all those report

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

Chat with us

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

Jamie Slome 7 months ago Admin

Sorted 👍

Sign in to join this conversation