Stored XSS viva .svg file upload in causefx/organizr

0

✓ Valid Reported on Apr 10th 2022

Description

The application allows .svg files to upload which leads to stored XSS

Proof of Concept

1.Download the payload from this link:-
https://drive.google.com/file/d/1c1BP5bxXBxtwLfRJTrEPgMWK1yVFDF2R/view?usp=sharing
2.Login to the application with Co-admin account and go to "Settings" -> "Image Manager" and upload the downloaded "XSS.svg" payload.
3.Then login with admin account and go to "Settings" -> "Image Manager" and select the "XSS.svg" and open it on a new tab or open the uploaded location you will see that XSS will trigger and this can lead to the admin account takeover.

PoC video:

```
https://drive.google.com/file/d/1jdjUHuQPG0xVR3pImcg3vT4cuxhIEuBi/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-2022-1345
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

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 936 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 ✗

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

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

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 👍

Chat with us

Sign in to join this conversation