saitoha / libsixel Public

Code Issues 41 Pull requests 7 Actions Projects Wiki ···

New issue Jump to bottom

[BUG] a reachable assert in stbi__create_png_image_raw #163

Open kdsjZh opened this issue on Mar 19 · 0 comments

kdsjZh commented on Mar 19 • edited

Describe the bug
There is a reachable assert bug found in stbi__create_png_image_raw, can be triggered via img2sixel+ ASan

To Reproduce
compile the program with CFLAGS="-fsanitize=address" CC=clang
then run `./img2sixel $POC`
output:

```
img2sixel: ./stb_image.h:4374: int stbi__create_png_image_raw(stbi__png *, stbi_uc *,
stbi__uint32, int, stbi__uint32, stbi__uint32, int, int): Assertion `img_width_bytes <= x' failed.
Aborted
```

system
ubuntu 16.04,
clang 12.0.1
libsixel latest commit `6a5be8b`

Credit
Han Zheng
NCNIPC of China
Hexhive

POC
poc.zip

Assignees

No one assigned

Labels

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant