cacalabs / **libcaca** Public

Code | **Issues** 24 | Pull requests 5 | Actions | Projects | Wiki | ···

New issue

Jump to bottom

[BUG] Divide by zero in img2txt #65

○ Open **kdsjZh** opened this issue on Feb 24 · 3 comments

kdsjZh commented on Feb 24 • edited ▾

version: latest commit `f42aa68`

driver: `src/img2txt`

Environment: ubuntu 22.04, clang-12

step to reproduce:

```
export CFLAGS="-fsanitize=address -g"
export CC=clang
./bootstrap
./configure
make -j8
./src/img2txt ./divide_by_0.seed
```

Sanitizer output:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==25214==ERROR: AddressSanitizer: FPE on unknown address 0x0000004d0433 (pc 0x0000004d0433 bp
0x7fff1cb39010 sp 0x7fff1cb38ee0 T0)
    #0 0x4d0433 in main /benchmarks/libcaca/src/img2txt.c:183:42
    #1 0x7fa2270f9d8f  (/lib/x86_64-linux-gnu/libc.so.6+0x2dd8f)
    #2 0x7fa2270f9e3f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2de3f)
    #3 0x421944 in _start (/benchmarks/libcaca/src/img2txt+0x421944)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /benchmarks/libcaca/src/img2txt.c:183:42 in main
==25214==ABORTING
```

#POC

divide_by_0.zip

##Credit
Han Zheng
NCNIPC of China
Hexhive

pterjan commented on Feb 25 Contributor

Thank you, reading the code it could happen when given a valid image of width 0 (probably the case here), but also with any image if passing -y 0.

jmoellers commented on Mar 14

How's this going to be fixed?
I added a check for `i->w` and/or `i->h` being 0, issuing an error message (`"image size is 0"`) and setting `lines` and `cols` to 0 (`caca_set_canvas_size` can handle this).
Obviously `caca_export_canvas_to_memory` then chokes on this but this is handled already. I only then also changed the `format` in the error message to `format?format:"ansi"` .

kirotawa commented on Mar 15

CVE-2022-0856 was assigned to this issue - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0856

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants

4 participants