New issue

Jump to bottom

heap-buffer-overflow in dither_func_fs at tosixel.c:861 #114

Closed SuhwanSong opened this issue on Dec 13, 2019 · 1 comment

SuhwanSong commented on Dec 13, 2019

version : img2sixel 1.8.2

There is a heap-buffer-overflow in dither_func_fs at tosixel.c:861
please run following cmd to reproduce it.

```
img2sixel --high-color $PoC
```

poc
ASAN LOG

```
==39700==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fcc6219e808 at pc 0x7fcc6ad13008 bp 0x7ffe2a935b70 sp 0x7ffe2a935b68
READ of size 1 at 0x7fcc6219e808 thread T0
    #0 0x7fcc6ad13007 in dither_func_fs /home/tmp/libsixel/src/tosixel.c:861:9
    #1 0x7fcc6ad13007 in sixel_apply_15bpp_dither /home/tmp/libsixel/src/tosixel.c:1223
    #2 0x7fcc6ad13007 in sixel_encode_highcolor /home/tmp/libsixel/src/tosixel.c:1334
    #3 0x7fcc6ad13007 in sixel_encode /home/tmp/libsixel/src/tosixel.c:1485
    #4 0x7fcc6b0478a4 in sixel_encoder_output_without_macro /home/tmp/libsixel/src/encoder.c:820:14
    #5 0x7fcc6b0478a4 in sixel_encoder_encode_frame /home/tmp/libsixel/src/encoder.c:1050
    #6 0x7fcc6adfdd91 in sixel_helper_load_image_file /home/tmp/libsixel/src/loader.c:913:14
    #7 0x7fcc6b03fd4f in sixel_encoder_encode /home/tmp/libsixel/src/encoder.c:1737:14
    #8 0x51787f in main /home/tmp/libsixel/converters/img2sixel.c:457:22
    #9 0x7fcc693a2b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #10 0x41a379 in _start (/home/tmp/img2sixel+0x41a379)

0x7fcc6219e808 is located 0 bytes to the right of 573448-byte region [0x7fcc62112800,0x7fcc6219e808)
allocated by thread T0 here:
    #0 0x4da230 in __interceptor_malloc (/home/tmp/img2sixel+0x4da230)
    #1 0x7fcc6acfcc7f in sixel_encode_highcolor /home/tmp/libsixel/src/tosixel.c:1309:40
    #2 0x7fcc6acfcc7f in sixel_encode /home/tmp/libsixel/src/tosixel.c:1485
    #3 0x7fcc6b0478a4 in sixel_encoder_output_without_macro /home/tmp/libsixel/src/encoder.c:820:14
    #4 0x7fcc6b0478a4 in sixel_encoder_encode_frame /home/tmp/libsixel/src/encoder.c:1050
    #5 0x7fcc6adfdd91 in sixel_helper_load_image_file /home/tmp/libsixel/src/loader.c:913:14
    #6 0x7fcc6b03fd4f in sixel_encoder_encode /home/tmp/libsixel/src/encoder.c:1737:14
    #7 0x51787f in main /home/tmp/libsixel/converters/img2sixel.c:457:22
    #8 0x7fcc693a2b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/tmp/libsixel/src/tosixel.c:861:9 in dither_func_fs
Shadow bytes around the buggy address:
  0x0ffa0c42bcb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ffa0c42bcc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ffa0c42bcd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ffa0c42bce0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ffa0c42bcf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ffa0c42bd00: 00[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ffa0c42bd10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ffa0c42bd20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ffa0c42bd30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ffa0c42bd40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ffa0c42bd50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==39700==ABORTING
```

saitoha commented on Dec 16, 2019 Owner

`9d0a7ff` for #116 also fixed this problem.

saitoha closed this as completed on Dec 16, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants