New issue

Jump to bottom

heap-buffer-overflow in sixel_encode_highcolor at tosixel.c:1361 #116

Closed **SuhwanSong** opened this issue on Dec 15, 2019 · 1 comment

SuhwanSong commented on Dec 15, 2019

img2sixel 1.8.3

There is a heap-buffer-overflow in sixel_encode_highcolor at tosixel.c:1361
please run following cmd to reproduce it.

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

poc
ASAN LOG

```
==28051==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6220000018fd at pc 0x7f6182c3fea8 bp 0x7ffde16993d0 sp 0x7ffde16993c8
READ of size 1 at 0x6220000018fd thread T0
    #0 0x7f6182c3fea7 in sixel_encode_highcolor /home/tmp/libsixel/src/tosixel.c:1361:25
    #1 0x7f6182c3fea7 in sixel_encode /home/tmp/libsixel/src/tosixel.c:1509
    #2 0x7f6182f6e5a4 in sixel_encoder_output_without_macro /home/tmp/libsixel/src/encoder.c:820:14
    #3 0x7f6182f6e5a4 in sixel_encoder_encode_frame /home/tmp/libsixel/src/encoder.c:1050
    #4 0x7f6182d2aa21 in sixel_helper_load_image_file /home/tmp/libsixel/src/loader.c:919:14
    #5 0x7f6182f66a4f in sixel_encoder_encode /home/tmp/libsixel/src/encoder.c:1737:14
    #6 0x51787f in main /home/tmp/libsixel/converters/img2sixel.c:457:22
    #7 0x7f61812cdb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #8 0x41a379 in _start (/home/tmp/img2sixel+0x41a379)

0x6220000018fd is located 3 bytes to the left of 5328-byte region [0x622000001900,0x622000002dd0)
allocated by thread T0 here:
    #0 0x4da230 in __interceptor_malloc (/home/tmp/img2sixel+0x4da230)
    #1 0x7f6182f6e0ee in sixel_encoder_output_without_macro /home/tmp/libsixel/src/encoder.c:784:26
    #2 0x7f6182f6e0ee in sixel_encoder_encode_frame /home/tmp/libsixel/src/encoder.c:1050
    #3 0x7f6182d2aa21 in sixel_helper_load_image_file /home/tmp/libsixel/src/loader.c:919:14
    #4 0x7f6182f66a4f in sixel_encoder_encode /home/tmp/libsixel/src/encoder.c:1737:14
    #5 0x51787f in main /home/tmp/libsixel/converters/img2sixel.c:457:22
    #6 0x7f61812cdb96 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:1361:25 in sixel_encode_highcolor
Shadow bytes around the buggy address:
  0x0c447fff82c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff82d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff82e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff82f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff8300: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c447fff8310: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa[fa]
  0x0c447fff8320: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c447fff8330: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c447fff8340: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c447fff8350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c447fff8360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==28051==ABORTING
```

saitoha added a commit that referenced this issue on Dec 16, 2019

`Fix access violation problem on high color mode (#116), Thanks to Suh…` ··· `9d0a7ff`

saitoha mentioned this issue on Dec 16, 2019

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

saitoha commented on Dec 18, 2019 Owner

Fixed on v1.8.4, Thanks!

saitoha closed this as completed on Dec 18, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants