New issue

Jump to bottom

# heap-use-after-free in libsixel/src/dither.c:388 #157

Open a4865g opened this issue on Sep 14, 2021 · 0 comments

a4865g commented on Sep 14, 2021

Hi,I found a heap-use-after-free in the current master 6a5be8b
I build img2sixel with ASAN,this is ASAN report.

OS: Ubuntu 20.04.3 LTS x86_64
Kernel: 5.11.0-27-generic

POC: poc.zip

```
$ ./img2sixel -o ./a.sixel -8 -p 1 -C 10 -d fs -f auto -s auto -t auto -E ~/Downloads/poc
=================================================================
==3495149==ERROR: AddressSanitizer: heap-use-after-free on address 0x6080000000a0 at pc
0x7ffff74e92cd bp 0x7fffffff84d0 sp 0x7fffffff84c0
READ of size 4 at 0x6080000000a0 thread T0
    #0 0x7ffff74e92cc in sixel_dither_unref /home/wulearn/Desktop/libsixel/src/dither.c:388
    #1 0x7ffff7537374 in sixel_encoder_encode_frame
/home/wulearn/Desktop/libsixel/src/encoder.c:1079
    #2 0x7ffff753b0af in load_image_callback /home/wulearn/Desktop/libsixel/src/encoder.c:1679
    #3 0x7ffff7531302 in load_gif /home/wulearn/Desktop/libsixel/src/fromgif.c:671
    #4 0x7ffff752abc9 in load_with_builtin /home/wulearn/Desktop/libsixel/src/loader.c:908
    #5 0x7ffff752b5cb in sixel_helper_load_image_file
/home/wulearn/Desktop/libsixel/src/loader.c:1418
    #6 0x7ffff753b513 in sixel_encoder_encode /home/wulearn/Desktop/libsixel/src/encoder.c:1743
    #7 0x555555558a3b in main /home/wulearn/Desktop/libsixel/converters/img2sixel.c:457
    #8 0x7ffff72c60b2 in __libc_start_main (/usr/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #9 0x55555555638d in _start (/home/wulearn/Desktop/libsixel/converters/.libs/img2sixel+0x238d)

0x6080000000a0 is located 0 bytes inside of 94-byte region [0x6080000000a0,0x6080000000fe)
freed by thread T0 here:
    #0 0x7ffff76a27cf in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.5+0x10d7cf)
    #1 0x7ffff7549523 in sixel_allocator_free /home/wulearn/Desktop/libsixel/src/allocator.c:230
    #2 0x7ffff74e9226 in sixel_dither_destroy /home/wulearn/Desktop/libsixel/src/dither.c:368
    #3 0x7ffff74e92f1 in sixel_dither_unref /home/wulearn/Desktop/libsixel/src/dither.c:389
    #4 0x7ffff75352bf in sixel_encoder_prepare_palette
/home/wulearn/Desktop/libsixel/src/encoder.c:584
    #5 0x7ffff75369a4 in sixel_encoder_encode_frame
/home/wulearn/Desktop/libsixel/src/encoder.c:981
```

```
    #6 0x7ffff753b0af in load_image_callback /home/wulearn/Desktop/libsixel/src/encoder.c:1679
    #7 0x7ffff7531302 in load_gif /home/wulearn/Desktop/libsixel/src/fromgif.c:671
    #8 0x7ffff752abc9 in load_with_builtin /home/wulearn/Desktop/libsixel/src/loader.c:908
    #9 0x7ffff752b5cb in sixel_helper_load_image_file
/home/wulearn/Desktop/libsixel/src/loader.c:1418
    #10 0x7ffff753b513 in sixel_encoder_encode /home/wulearn/Desktop/libsixel/src/encoder.c:1743
    #11 0x555555558a3b in main /home/wulearn/Desktop/libsixel/converters/img2sixel.c:457
    #12 0x7ffff72c60b2 in __libc_start_main (/usr/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

previously allocated by thread T0 here:
    #0 0x7ffff76a2bc8 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x555555558c4e in rpl_malloc /home/wulearn/Desktop/libsixel/converters/malloc_stub.c:45
    #2 0x7ffff7549243 in sixel_allocator_malloc /home/wulearn/Desktop/libsixel/src/allocator.c:162
    #3 0x7ffff74e8a7a in sixel_dither_new /home/wulearn/Desktop/libsixel/src/dither.c:306
    #4 0x7ffff7535133 in sixel_encoder_prepare_palette
/home/wulearn/Desktop/libsixel/src/encoder.c:570
    #5 0x7ffff75369a4 in sixel_encoder_encode_frame
/home/wulearn/Desktop/libsixel/src/encoder.c:981
    #6 0x7ffff753b0af in load_image_callback /home/wulearn/Desktop/libsixel/src/encoder.c:1679
    #7 0x7ffff7531302 in load_gif /home/wulearn/Desktop/libsixel/src/fromgif.c:671
    #8 0x7ffff752abc9 in load_with_builtin /home/wulearn/Desktop/libsixel/src/loader.c:908
    #9 0x7ffff752b5cb in sixel_helper_load_image_file
/home/wulearn/Desktop/libsixel/src/loader.c:1418
    #10 0x7ffff753b513 in sixel_encoder_encode /home/wulearn/Desktop/libsixel/src/encoder.c:1743
    #11 0x555555558a3b in main /home/wulearn/Desktop/libsixel/converters/img2sixel.c:457
    #12 0x7ffff72c60b2 in __libc_start_main (/usr/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: heap-use-after-free /home/wulearn/Desktop/libsixel/src/dither.c:388 in
sixel_dither_unref
Shadow bytes around the buggy address:
  0x0c107fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c107fff8010: fa fa fa fa[fd]fd fd fd fd fd fd fd fd fd fd fd
  0x0c107fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8060: 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
  Shadow gap:              cc
==3495149==ABORTING
```

 **a4865g** mentioned this issue on Sep 14, 2021

**heap-use-after-free in libsixel/src/dither.c:379** libsixel/libsixel#27

Closed

### Assignees

No one assigned

### Labels

None yet

### Projects

None yet

### Milestone

No milestone

### Development

No branches or pull requests

### 1 participant