saitoha / **libsixel** Public

<> Code ⊙ Issues 43 Pull requests 7 ▷ Actions Projects Wiki ···

New issue

Jump to bottom

heap-buffer-overflow in sixel_encoder_output_without_macro at encoder.c:814 #123

Closed **SuhwanSong** opened this issue on Dec 23, 2019 · 3 comments

SuhwanSong commented on Dec 23, 2019

version : img2sixel 1.8.4
OS : Ubuntu 18.04
configured with:
libcurl: yes
libpng: yes
libjpeg: yes
gdk-pixbuf2: no
GD: no

There is a heap-buffer-overflow in sixel_encoder_output_without_macro at encoder.c:814
please run following cmd to reproduce it.

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

poc
ASAN LOG

```
==26572==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f1b55fdd320 at pc 0x0000004d90f2 bp 0x7ffd65666ef0 sp 0x7ffd656666a0
READ of size 1526074725 at 0x7f1b55fdd320 thread T0
    #0 0x4d90f1 in __asan_memcpy (/home/tmp/img2sixel+0x4d90f1)
    #1 0x7f1c0acb8341 in sixel_encoder_output_without_macro /home/tmp/libsixel/src/encoder.c:814:5
    #2 0x7f1c0acb8341 in sixel_encoder_encode_frame /home/tmp/libsixel/src/encoder.c:1050
    #3 0x7f1c0ac8f026 in load_gif /home/tmp/libsixel/src/fromgif.c:649:22
    #4 0x7f1c0aa6c6fb in load_with_builtin /home/tmp/libsixel/src/loader.c:888:18
    #5 0x7f1c0aa6c6fb in sixel_helper_load_image_file /home/tmp/libsixel/src/loader.c:1392
    #6 0x7f1c0acb099f 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 0x7f1c09016b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #9 0x41a379 in _start (/home/tmp/img2sixel+0x41a379)

0x7f1b55fdd320 is located 0 bytes to the right of 36043552-byte region [0x7f1b53d7d800,0x7f1b55fdd320)
allocated by thread T0 here:
    #0 0x4da230 in __interceptor_malloc (/home/tmp/img2sixel+0x4da230)
    #1 0x7f1c0ac8ce95 in gif_init_frame /home/tmp/libsixel/src/fromgif.c:239:42
    #2 0x7f1c0ac8ce95 in load_gif /home/tmp/libsixel/src/fromgif.c:644
    #3 0x7f1c0aa6c6fb in load_with_builtin /home/tmp/libsixel/src/loader.c:888:18
    #4 0x7f1c0aa6c6fb in sixel_helper_load_image_file /home/tmp/libsixel/src/loader.c:1392
    #5 0x7f1c0acb099f 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 0x7f1c09016b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/tmp/img2sixel+0x4d90f1) in __asan_memcpy
Shadow bytes around the buggy address:
  0x0fe3eabf3a10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3eabf3a20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3eabf3a30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3eabf3a40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fe3eabf3a50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0fe3eabf3a60: 00 00 00 00[fa]fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3eabf3a70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3eabf3a80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3eabf3a90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3eabf3aa0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0fe3eabf3ab0: 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
==26572==ABORTING
```

👍 1

saitoha commented on Dec 24, 2019 Owner

This problem seems to be fixed on `fix-issue74-limit-memory-allocation-size` branch, with `0b1e0b3` .

saitoha commented on Jan 2, 2020 Owner

Fixed on v1.8.5. Thanks!

👍 1

saitoha closed this as completed on Jan 2, 2020

fgeek commented on Aug 12, 2021

CVE-2020-21677 has been assigned for this issue.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants