New issue

Jump to bottom

double-free in sixel_chunk_destroy /root/libsixel/src/chunk.c:107:9 #144

Closed **chibataiki** opened this issue on Dec 30, 2020 · 2 comments

chibataiki commented on Dec 30, 2020 • edited

version:
img2sixel 1.8.6

OS: Ubuntu 20.04.1 LTS x86_64
Kernel: 5.4.0-54-generic

compiler: gcc version 9.3.0

configured with:
libcurl: no
libpng: yes
libjpeg: no
gdk-pixbuf2: no
GD: no

compiled with :

```
(CFLAGS="-g -fsanitize=address" ./configure && make)
```

run

```
./img2sixel   poc
```

poc_double_free.zip

```
=================================================================
==872176==ERROR: AddressSanitizer: attempting double-free on 0x62d000000400 in thread T0:
    #0 0x49489d in free (/root/libsixel/converters/.libs/img2sixel+0x49489d)
    #1 0x7fb24078593d in sixel_chunk_destroy /root/libsixel/src/chunk.c:107:9
    #2 0x7fb240799ddf in sixel_helper_load_image_file /root/libsixel/src/loader.c:1432:5
    #3 0x7fb2407f4e36 in sixel_encoder_encode /root/libsixel/src/encoder.c:1743:14
    #4 0x4c5c88 in main /root/libsixel/converters/img2sixel.c:457:22
    #5 0x7fb2403400b2 in __libc_start_main /build/glibc-ZN95T4/glibc-2.31/csu/../csu/libc-start.c:308:16
    #6 0x41c3dd in _start (/root/libsixel/converters/.libs/img2sixel+0x41c3dd)

0x62d000000400 is located 0 bytes inside of 32768-byte region [0x62d000000400,0x62d000008400)
freed by thread T0 here:
    #0 0x49489d in free (/root/libsixel/converters/.libs/img2sixel+0x49489d)
    #1 0x7fb2407defe9 in load_png /root/libsixel/src/loader.c:633:5
    #2 0x7fb240799a85 in load_with_builtin /root/libsixel/src/loader.c:889:18
    #3 0x7fb240799a85 in sixel_helper_load_image_file /root/libsixel/src/loader.c:1418:18
    #4 0x7fb2407f4e36 in sixel_encoder_encode /root/libsixel/src/encoder.c:1743:14
    #5 0x4c5c88 in main /root/libsixel/converters/img2sixel.c:457:22
    #6 0x7fb2403400b2 in __libc_start_main /build/glibc-ZN95T4/glibc-2.31/csu/../csu/libc-start.c:308:16

previously allocated by thread T0 here:
    #0 0x494b1d in malloc (/root/libsixel/converters/.libs/img2sixel+0x494b1d)
    #1 0x7fb24080df0c in sixel_allocator_malloc /root/libsixel/src/allocator.c:162:12
    #2 0x7fb240797a57 in sixel_helper_load_image_file /root/libsixel/src/loader.c:1375:14
    #3 0x7fb2407f4e36 in sixel_encoder_encode /root/libsixel/src/encoder.c:1743:14
    #4 0x4c5c88 in main /root/libsixel/converters/img2sixel.c:457:22
    #5 0x7fb2403400b2 in __libc_start_main /build/glibc-ZN95T4/glibc-2.31/csu/../csu/libc-start.c:308:16

SUMMARY: AddressSanitizer: double-free (/root/libsixel/converters/.libs/img2sixel+0x49489d) in free
==872176==ABORTING
```

chibataiki changed the title ~~AddressSanitizer: double-free in in sixel_chunk_destroy /root/libsixel/src/chunk.c:107:9~~ double-free in in sixel_chunk_destroy /root/libsixel/src/chunk.c:107:9 on Jan 3, 2021

chibataiki changed the title ~~double-free in in sixel_chunk_destroy /root/libsixel/src/chunk.c:107:9~~ double-free in sixel_chunk_destroy /root/libsixel/src/chunk.c:107:9 on Jan 18, 2021

chibataiki closed this as completed on Jan 18, 2021

carnil commented on Mar 11

@chibataiki you did open and close this issue (but without a reason). Did the issue turned out to be a non-issue? If so I believe the CVE entry which got assigned for this issue, CVE-2020-36123 should be rejected.

chibataiki commented on Jun 6 Author

@carnil Yes ,the issue was mistaken, the cve id can be rejected.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants