GIFLIB Bugs

A library and utilities for processing GIFs
Brought to you by: abadger1999, esr

#151 A heap-buffer-overflow in gif2rgb.c:294:45

Milestone: v1.0_(example) **Status:** open **Owner:** nobody **Labels:** bug (1)
Priority: 1
Updated: 2020-08-02 **Created:** 2020-08-02 **Creator:** zhouan **Private:** No

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), gif2rgb (5.14, github mirror)

Configure

CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" ./configure

Command line

./util/gif2rgb @@

AddressSanitizer output

```
=================================================================
==64686==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x604000000080 at pc 0x00
READ of size 1 at 0x604000000080 thread T0
    #0 0x5158ed in DumpScreen2RGB /home/seviezhou/giflib/util/gif2rgb.c:294:45
    #1 0x5158ed in GIF2RGB /home/seviezhou/giflib/util/gif2rgb.c:474
    #2 0x5158ed in main /home/seviezhou/giflib/util/gif2rgb.c:525
    #3 0x7fcb3aeb5b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-s
    #4 0x41a259 in _start (/home/seviezhou/giflib/util/gif2rgb+0x41a259)

0x604000000080 is located 0 bytes to the right of 48-byte region [0x604000000050,0x60400000
allocated by thread T0 here:
    #0 0x4da338 in calloc (/home/seviezhou/giflib/util/gif2rgb+0x4da338)
    #1 0x5342f8 in GifMakeMapObject /home/seviezhou/giflib/lib/gifalloc.c:55:38

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/giflib/util/gif2rgb.c:294:4
Shadow bytes around the buggy address:
  0x0c087fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c087fff8000: fa fa fd fd fd fd fd fd fa fa 00 00 00 00 00 00
=>0x0c087fff8010:[fa]fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
  0x0c087fff8020: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
  0x0c087fff8030: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
  0x0c087fff8040: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
  0x0c087fff8050: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
  0x0c087fff8060: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 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
==64686==ABORTING
```

1 Attachments

heap-buffer-overflow-DumpScreen2RGB-gif2rgb-294.zip

Discussion

Log in to post a comment.

SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

Team

SourceForge Headquarters
225 Broadway Suite 1600
San Diego, CA 92101
+1 (858) 454-5900

Resources

Support

Site Documentation

Site Status

Terms Privacy Opt Out Advertise