AddressSanitizer: heap-buffer-overflow in GetByte() at ngiflib.c:70 in NGIFLIB_NO_FILE mode #18

Closed **Marsman1996** opened this issue on Jun 29, 2021 · 0 comments

Marsman1996 commented on Jun 29, 2021 • edited

This Overflow problem is because in NGIFLIB_NO_FILE mode, `GetByte()` reads memory buffer without checking the boundary.

Test Environment

Ubuntu 16.04, 64bit
ngiflib(master `0245fd4`)

How to trigger

1. Compile the program with AddressSanitizer in NGIFLIB_NO_FILE mode `CC="clang -fsanitize=address -g" CFLAGS+=-DNGIFLIB_NO_FILE make`
2. run the compiled program `$ ./gif2tga --outbase /dev/null $POC`

POC file

https://github.com/Marsman1996/pocs/raw/master/ngiflib/poc-ngiflib-0245fd4-GetByte-overflow

Details

ASAN report

```
==8923==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x606000000058 at pc 0x00000051a564 bp 0x7fff7f5aeba0 sp 0x7fff7f5aeb98
READ of size 1 at 0x606000000058 thread T0
    #0 0x51a563 in GetByte /opt/disk/marsman/test/ngiflib/build_asan/ngiflib.c:70:10
    #1 0x51902b in LoadGif /opt/disk/marsman/test/ngiflib/build_asan/ngiflib.c:680:23
    #2 0x51696e in main /opt/disk/marsman/test/ngiflib/build_asan/gif2tga.c:95:10
    #3 0x7fa15acde83f in __libc_start_main /build/glibc-S7Ft5T/glibc-2.23/csu/../csu/libc-start.c:291
    #4 0x419fa8 in _start (/opt/disk/marsman/test/ngiflib/build_asan/gif2tga+0x419fa8)

0x606000000058 is located 0 bytes to the right of 56-byte region [0x606000000020,0x606000000058)
allocated by thread T0 here:
    #0 0x4de1d8 in __interceptor_malloc /home/mcgrady/wyh/llvm/llvm-6.0.0.src/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:88
    #1 0x5166c0 in main /opt/disk/marsman/test/ngiflib/build_asan/gif2tga.c:75:11
    #2 0x7fa15acde83f in __libc_start_main /build/glibc-S7Ft5T/glibc-2.23/csu/../csu/libc-start.c:291

SUMMARY: AddressSanitizer: heap-buffer-overflow /opt/disk/marsman/test/ngiflib/build_asan/ngiflib.c:70:10 in GetByte
Shadow bytes around the buggy address:
  0x0c0c7fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0c7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0c7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0c7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0c7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c0c7fff8000: fa fa fa fa 00 00 00 00 00 00 00[fa]fa fa fa fa
  0x0c0c7fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff8050: 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
==8923==ABORTING
```

Marsman1996 mentioned this issue on Jun 29, 2021

AddressSanitizer: heap-buffer-overflow in GetByteStr() at ngiflib.c:108 in NGIFLIB_NO_FILE mode #19

Closed

miniupnp closed this as completed in `19913ae` on Aug 11, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant