A heap-buffer-overflow in captoinfo.c:321:12

From: Anshunkang Zhou
Subject: A heap-buffer-overflow in captoinfo.c:321:12
Date: Tue, 4 Aug 2020 21:26:04 +0800

Dear Developers,
I found a heap-buffer-overflow in captoinfo.c:321:12, detailed system information and build configuration is as follows, the poc is in the mail attachment.

## System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), ncurses (latest master label v6_2_20200801)

## Configure

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

## Command line

./progs/tic -o /tmp @@

## AddressSanitizer output

```
=================================================================
==18977==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x621000002500 at pc 0x000000570883 bp 0x7ffd25a79bd0 sp 0x7ffd25a79bc8
READ of size 1 at 0x621000002500 thread T0
    #0 0x570882 in _nc_captoinfo /home/seviezhou/ncurses/ncurses/../ncurses/./tinfo/captoinfo.c:321:12
    #1 0x588e16 in _nc_parse_entry /home/seviezhou/ncurses/ncurses/../ncurses/./tinfo/parse_entry.c:548:13
    #2 0x57c076 in _nc_read_entry_source /home/seviezhou/ncurses/ncurses/../ncurses/./tinfo/comp_parse.c:226:6
    #3 0x517a0d in main /home/seviezhou/ncurses/progs/../progs/tic.c:963:5
    #4 0x7f424829183f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #5 0x41a9f8 in _start (/home/seviezhou/ncurses/progs/tic+0x41a9f8)

0x621000002500 is located 0 bytes to the right of 4096-byte region [0x621000001500,0x621000002500)
allocated by thread T0 here:
    #0 0x4dec08 in __interceptor_malloc /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:88
    #1 0x580f32 in _nc_get_token /home/seviezhou/ncurses/ncurses/../ncurses/./tinfo/comp_scan.c:448:16
    #2 0x586031 in _nc_parse_entry /home/seviezhou/ncurses/ncurses/../ncurses/./tinfo/parse_entry.c:265:18
    #3 0x57c076 in _nc_read_entry_source /home/seviezhou/ncurses/ncurses/../ncurses/./tinfo/comp_parse.c:226:6
    #4 0x517a0d in main /home/seviezhou/ncurses/progs/../progs/tic.c:963:5
    #5 0x7f424829183f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/ncurses/ncurses/../ncurses/./tinfo/captoinfo.c:321:12 in _nc_captoinfo
Shadow bytes around the buggy address:
  0x0c427fff8450: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff8460: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff8470: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff8480: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff8490: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c427fff84a0:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff84b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff84c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff84d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff84e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff84f0: 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
==18977==ABORTING
```

heap-overflow-_nc_captoinfo-captoinfo-321.zip
Description: Zip archive

reply via email to
Anshunkang Zhou

[Prev in Thread] **Current Thread** [Next in Thread]

- **A heap-buffer-overflow in captoinfo.c:321:12**, *Anshunkang Zhou* <=
    - **Re: A heap-buffer-overflow in captoinfo.c:321:12**, *Thomas Dickey*, 2020/08/04
        - **Re: A heap-buffer-overflow in captoinfo.c:321:12**, *Anshunkang Zhou*, 2020/08/04

- Prev by Date: **ANN: ncurses-6.2-20200801**
- Next by Date: **A memory leak in**
- Previous by thread: **ANN: ncurses-6.2-20200801**
- Next by thread: **Re: A heap-buffer-overflow in captoinfo.c:321:12**
- Index(es):
    - **Date**
    - **Thread**