New issue

Jump to bottom

A global-buffer-overflow in error.c:46:18 #10

Open **seviezhou** opened this issue on Aug 4, 2020 · 0 comments

seviezhou commented on Aug 4, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), iffpp (latest master 0290be4)

Configure

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

Command line

./src/iffpp/.libs/lt-iffpp @@

Output

AddressSanitizer output

```
==2975==ERROR: AddressSanitizer: global-buffer-overflow on address 0x7ff1289d83a1 at pc 0x7ff1289d7710 bp 0x7ffc77e7d770 sp 0x7ffc77e7d768
READ of size 1 at 0x7ff1289d83a1 thread T0
    #0 0x7ff1289d770f in IFF_errorId /home/seviezhou/libiff/src/libiff/error.c:46:18
    #1 0x7ff1289d77cd in IFF_readError /home/seviezhou/libiff/src/libiff/error.c:52:5
    #2 0x7ff1289c7dc9 in IFF_readId /home/seviezhou/libiff/src/libiff/id.c:42:2
    #3 0x7ff1289c93c4 in IFF_readChunk /home/seviezhou/libiff/src/libiff/chunk.c:54:9
    #4 0x7ff1289cd295 in IFF_readGroup /home/seviezhou/libiff/src/libiff/group.c:80:21
    #5 0x7ff1289d0754 in IFF_readForm /home/seviezhou/libiff/src/libiff/form.c:45:23
    #6 0x7ff1289c9856 in IFF_readChunk /home/seviezhou/libiff/src/libiff/chunk.c:64:21
    #7 0x7ff1289d78f3 in IFF_readFd /home/seviezhou/libiff/src/libiff/iff.c:35:13
    #8 0x7ff1289d7b48 in IFF_read /home/seviezhou/libiff/src/libiff/iff.c:65:13
    #9 0x5167b3 in IFF_prettyPrint /home/seviezhou/libiff/src/iffpp/pp.c:33:10
    #10 0x516477 in main /home/seviezhou/libiff/src/iffpp/main.c:137:12
    #11 0x7ff127acb83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #12 0x41a478 in _start (/home/seviezhou/libiff/src/iffpp/.libs/lt-iffpp+0x41a478)

0x7ff1289d83a1 is located 63 bytes to the left of global variable '<string literal>' defined in 'chunk.c:58:49' (0x7ff1289d83e0) of size 10
  '<string literal>' is ascii string 'chunkSize'
0x7ff1289d83a1 is located 0 bytes to the right of global variable '<string literal>' defined in 'chunk.c:54:35' (0x7ff1289d83a0) of size 1
  '<string literal>' is ascii string ''
SUMMARY: AddressSanitizer: global-buffer-overflow /home/seviezhou/libiff/src/libiff/error.c:46:18 in IFF_errorId
Shadow bytes around the buggy address:
  0x0ffea5133020: 00 00 00 f9 f9 f9 f9 f9 03 f9 f9 f9 f9 f9 f9 f9
  0x0ffea5133030: 00 00 00 00 04 f9 f9 f9 f9 f9 f9 f9 00 00 00 07
  0x0ffea5133040: f9 f9 f9 f9 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ffea5133050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ffea5133060: 00 00 00 00 f9 f9 f9 f9 00 00 00 07 f9 f9 f9 f9
=>0x0ffea5133070: 00 00 00 00[01]f9 f9 f9 f9 f9 f9 f9 00 02 f9 f9
  0x0ffea5133080: f9 f9 f9 f9 05 f9 f9 f9 f9 f9 f9 f9 05 f9 f9 f9
  0x0ffea5133090: f9 f9 f9 f9 05 f9 f9 f9 f9 f9 f9 f9 05 f9 f9 f9
  0x0ffea51330a0: f9 f9 f9 f9 00 f9 f9 f9 f9 f9 f9 f9 02 f9 f9 f9
  0x0ffea51330b0: f9 f9 f9 f9 00 00 01 f9 f9 f9 f9 f9 04 f9 f9 f9
  0x0ffea51330c0: f9 f9 f9 f9 06 f9 f9 f9 f9 f9 f9 f9 00 00 00 00
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
==2975==ABORTING
```

POC

global-overflow-IFF_errorId-error-46.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant