New issue

Jump to bottom

A heap-buffer-overflow in lt_predict.c:108:36 #62

Closed seviezhou opened this issue on Sep 4, 2020 · 0 comments

seviezhou commented on Sep 4, 2020

System info

Ubuntu x86_64, clang 6.0, faad (latest master f71b5e)

Configure

CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" ./configure --enable-shared=no

Command line

./frontend/faad -w -b 5 @@

AddressSanitizer output

```
=================================================================
==13979==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x620000003006 at pc 0x0000005e1605 bp 0x7ffc00e45c30 sp 0x7ffc00e45c28
READ of size 2 at 0x620000003006 thread T0
    #0 0x5e1604 in lt_prediction /home/seviezhou/faad2/libfaad/lt_predict.c:108:36
    #1 0x5be727 in reconstruct_single_channel /home/seviezhou/faad2/libfaad/specrec.c:995:9
    #2 0x55308e in single_lfe_channel_element /home/seviezhou/faad2/libfaad/syntax.c:643:14
    #3 0x55308e in decode_sce_lfe /home/seviezhou/faad2/libfaad/syntax.c:357
    #4 0x551d9a in raw_data_block /home/seviezhou/faad2/libfaad/syntax.c:550:13
    #5 0x534e1e in aac_frame_decode /home/seviezhou/faad2/libfaad/decoder.c:990:9
    #6 0x52bbeb in decodeMP4file /home/seviezhou/faad2/frontend/main.c:916:25
    #7 0x52bbeb in faad_main /home/seviezhou/faad2/frontend/main.c:1323
    #8 0x7f3ce6cebb96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #9 0x41a669 in _start (/home/seviezhou/faad2/frontend/faad+0x41a669)

0x620000003006 is located 122 bytes to the left of 3840-byte region [0x620000003080,0x620000003f80)
allocated by thread T0 here:
    #0 0x4da520 in __interceptor_malloc (/home/seviezhou/faad2/frontend/faad+0x4da520)
    #1 0x5bdc3e in allocate_single_channel /home/seviezhou/faad2/libfaad/specrec.c:714:53
    #2 0x5bdc3e in reconstruct_single_channel /home/seviezhou/faad2/libfaad/specrec.c:934
    #3 0x55308e in single_lfe_channel_element /home/seviezhou/faad2/libfaad/syntax.c:643:14
    #4 0x55308e in decode_sce_lfe /home/seviezhou/faad2/libfaad/syntax.c:357
    #5 0x551d9a in raw_data_block /home/seviezhou/faad2/libfaad/syntax.c:550:13

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/faad2/libfaad/lt_predict.c:108:36 in lt_prediction
Shadow bytes around the buggy address:
  0x0c407fff85b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff85c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff85d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff85e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff85f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c407fff8600:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c407fff8610: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff8620: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff8630: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff8640: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff8650: 00 00 00 00 00 00 00 00 00 00 00 00 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
==13979==ABORTING
```

POC

heap-overflow-lt_prediction-lt_predict-108.zip

fabiangreffrath closed this as completed in e19a5e4 on Oct 6, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant