New issue

Jump to bottom

A heap-buffer-overflow in sbr_qmf.c:96:77 #59

Closed seviezhou opened this issue on Aug 30, 2020 · 0 comments

seviezhou commented on Aug 30, 2020

System info

Ubuntu x86_64, clang 6.0, faad (latest master 1073ae)

Configure

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

Command line

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

AddressSanitizer output

```
NULL    349.611 secs, 7 ch, 24000 Hz

=================================================================
==73167==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x620000004f80 at pc 0x0000005df054 bp 0x7fffad795310 sp 0x7fffad795308
READ of size 4 at 0x620000004f80 thread T0
    #0 0x5df053 in sbr_qmf_analysis_32 /home/seviezhou/faad2/libfaad/sbr_qmf.c:96:77
    #1 0x598dc5 in sbr_process_channel /home/seviezhou/faad2/libfaad/sbr_dec.c
    #2 0x59addc in sbrDecodeSingleFrame /home/seviezhou/faad2/libfaad/sbr_dec.c:562:17
    #3 0x5c2f81 in reconstruct_single_channel /home/seviezhou/faad2/libfaad/specrec.c:1070:22
    #4 0x556c2e in single_lfe_channel_element /home/seviezhou/faad2/libfaad/syntax.c:643:14
    #5 0x556c2e in decode_sce_lfe /home/seviezhou/faad2/libfaad/syntax.c:357
    #6 0x555c2b in raw_data_block /home/seviezhou/faad2/libfaad/syntax.c:565:13
    #7 0x5389de in aac_frame_decode /home/seviezhou/faad2/libfaad/decoder.c:990:9
    #8 0x52f738 in decodeMP4file /home/seviezhou/faad2/frontend/main.c:916:25
    #9 0x52f738 in faad_main /home/seviezhou/faad2/frontend/main.c:1323
    #10 0x7f2790ec683f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #11 0x41a698 in _start (/home/seviezhou/faad2/frontend/faad+0x41a698)

0x620000004f80 is located 0 bytes to the right of 3840-byte region [0x620000004080,0x620000004f80)
allocated by thread T0 here:
    #0 0x4de8a8 in __interceptor_malloc /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:88
    #1 0x5c1a0b in allocate_single_channel /home/seviezhou/faad2/libfaad/specrec.c:736:48
    #2 0x5c1a0b in reconstruct_single_channel /home/seviezhou/faad2/libfaad/specrec.c:934
    #3 0x556c2e in single_lfe_channel_element /home/seviezhou/faad2/libfaad/syntax.c:643:14
    #4 0x556c2e in decode_sce_lfe /home/seviezhou/faad2/libfaad/syntax.c:357
    #5 0x555c2b in raw_data_block /home/seviezhou/faad2/libfaad/syntax.c:565:13

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/faad2/libfaad/sbr_qmf.c:96:77 in sbr_qmf_analysis_32
Shadow bytes around the buggy address:
  0x0c407fff89a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff89b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff89c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff89d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c407fff89e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c407fff89f0:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c407fff8a00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c407fff8a10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c407fff8a20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c407fff8a30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c407fff8a40: 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
==73167==ABORTING
```

POC

sbr_qmf_analysis_32-sbr_qmf-96.zip

fabiangreffrath closed this as completed in c78251b 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