New issue

Jump to bottom

A heap-buffer-overflow in sbr_qmf.c:614:27 #60

Closed seviezhou opened this issue on Aug 30, 2020 · 1 comment

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  174.805 secs, 5 ch, 48000 Hz

=================================================================
==39716==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x621000008900 at pc 0x0000005e19ba bp 0x7ffc780ef510 sp 0x7ffc780ef508
WRITE of size 4 at 0x621000008900 thread T0
    #0 0x5e19b9 in sbr_qmf_synthesis_64 /home/seviezhou/faad2/libfaad/sbr_qmf.c:614:27
    #1 0x59aeae in sbrDecodeSingleFrame /home/seviezhou/faad2/libfaad/sbr_dec.c:568:9
    #2 0x5c2f81 in reconstruct_single_channel /home/seviezhou/faad2/libfaad/specrec.c:1070:22
    #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 0x55593a in raw_data_block /home/seviezhou/faad2/libfaad/syntax.c:550:13
    #6 0x5389de in aac_frame_decode /home/seviezhou/faad2/libfaad/decoder.c:990:9
    #7 0x52f738 in decodeMP4file /home/seviezhou/faad2/frontend/main.c:916:25
    #8 0x52f738 in faad_main /home/seviezhou/faad2/frontend/main.c:1323
    #9 0x7f3373f6783f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #10 0x41a698 in _start (/home/seviezhou/faad2/frontend/faad+0x41a698)

0x621000008900 is located 0 bytes to the right of 4096-byte region [0x621000007900,0x621000008900)
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 0x55593a in raw_data_block /home/seviezhou/faad2/libfaad/syntax.c:550:13

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/faad2/libfaad/sbr_qmf.c:614:27 in sbr_qmf_synthesis_64
Shadow bytes around the buggy address:
  0x0c427fff90d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff90e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff90f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff9100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fff9110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c427fff9120:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff9130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff9140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff9150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff9160: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fff9170: 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
==39716==ABORTING
```

POC

heap-overflow-sbr_qmf_synthesis_64-sbr_qmf-614.zip

awesie added a commit to awesie/faad2 that referenced this issue on Oct 5, 2020

Restrict SBR frame length to 960 and 1024 samples. ... c78251b

fabiangreffrath commented on Oct 7, 2020 Collaborator

`c78251b`

fabiangreffrath closed this as completed on Oct 7, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants