New issue

Jump to bottom

A stack-buffer-overflow in mp4read.c:141:9 #56

Closed seviezhou opened this issue on Aug 16, 2020 · 0 comments

seviezhou commented on Aug 16, 2020

System info

Ubuntu x86_64, clang 6.0, faad (latest master eb19fa)

Configure

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

Command line

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

AddressSanitizer output

```
=================================================================
==66437==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7fff84ab6078 at pc 0x0000004462d7 bp 0x7fff84ab5ee0 sp 0x7fff84ab5690
READ of size 41 at 0x7fff84ab6078 thread T0
    #0 0x4462d6 in printf_common(void*, char const*, __va_list_tag*) (/home/seviezhou/faad2/frontend/faad+0x4462d6)
    #1 0x446f1b in __interceptor_vfprintf (/home/seviezhou/faad2/frontend/faad+0x446f1b)
    #2 0x446fe6 in fprintf (/home/seviezhou/faad2/frontend/faad+0x446fe6)
    #3 0x5150d3 in ftypin /home/seviezhou/faad2/frontend/mp4read.c:141:9
    #4 0x5143fd in parse /home/seviezhou/faad2/frontend/mp4read.c:765:19
    #5 0x5130f8 in mp4read_open /home/seviezhou/faad2/frontend/mp4read.c:999:9
    #6 0x52a3a7 in decodeMP4file /home/seviezhou/faad2/frontend/main.c:830:9
    #7 0x52a3a7 in faad_main /home/seviezhou/faad2/frontend/main.c:1323
    #8 0x7f9c8fbc2b96 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)

Address 0x7fff84ab6078 is located in stack of thread T0 at offset 88 in frame
    #0 0x514aef in ftypin /home/seviezhou/faad2/frontend/mp4read.c:126

  This frame has 2 object(s):
    [32, 36) 'u32.i' (line 104)
    [48, 88) 'buf' (line 128) <== Memory access at offset 88 overflows this variable
HINT: this may be a false positive if your program uses some custom stack unwind mechanism or swapcontext
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow (/home/seviezhou/faad2/frontend/faad+0x4462d6) in printf_common(void*, char const*, __va_list_tag*)
Shadow bytes around the buggy address:
  0x10007094ebb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007094ebc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007094ebd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007094ebe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007094ebf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x10007094ec00: 00 00 00 00 f1 f1 f1 f1 f8 f2 00 00 00 00 00[f3]
  0x10007094ec10: f3 f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007094ec20: 00 00 00 00 00 00 00 00 f1 f1 f1 f1 f8 f2 f8 f2
  0x10007094ec30: f8 f3 f3 f3 00 00 00 00 00 00 00 00 00 00 00 00
  0x10007094ec40: 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1
  0x10007094ec50: f8 f2 f2 f2 04 f3 f3 f3 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
==66437==ABORTING
```

POC

stack-overflow-ftypin-mp4read-141.zip

fabiangreffrath closed this as completed in 1073aee on Aug 17, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant