New issue

Jump to bottom

A heap-buffer-overflow in mp4read.c:355:29 #57

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

```
********** Ahead Software MPEG-4 AAC Decoder V2.9.2 *****************

Build: Aug 30 2020
Copyright 2002-2004: Ahead Software AG
http://www.audiocoding.com
bug tracking: https://sourceforge.net/p/faac/bugs/
Floating point version

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License.

**************************************************************************

**** MP4 header ****
Brand:                  isom(version 512)
Compatible brands:      isomiso2mp41
*track media type: 'soun': OK
================================================================
==36828==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000010 at pc 0x00000051eaca bp 0x7ffe7db7e7f0 sp 0x7ffe7db7e7e8
WRITE of size 4 at 0x602000000010 thread T0
    #0 0x51eac9 in stszin /home/seviezhou/faad2/frontend/mp4read.c:355:29
    #1 0x517c4d in parse /home/seviezhou/faad2/frontend/mp4read.c:766:19
    #2 0x517ec2 in parse /home/seviezhou/faad2/frontend/mp4read.c:790:24
    #3 0x517ec2 in parse /home/seviezhou/faad2/frontend/mp4read.c:790:24
    #4 0x517ec2 in parse /home/seviezhou/faad2/frontend/mp4read.c:790:24
    #5 0x517ec2 in parse /home/seviezhou/faad2/frontend/mp4read.c:790:24
    #6 0x518cf8 in moovin /home/seviezhou/faad2/frontend/mp4read.c:867:15
    #7 0x517c4d in parse /home/seviezhou/faad2/frontend/mp4read.c:766:19
    #8 0x5169a5 in mp4read_open /home/seviezhou/faad2/frontend/mp4read.c:1005:16
    #9 0x52de44 in decodeMP4file /home/seviezhou/faad2/frontend/main.c:830:9
    #10 0x52de44 in faad_main /home/seviezhou/faad2/frontend/main.c:1323
    #11 0x7f92a07fc83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #12 0x41a698 in _start (/home/seviezhou/faad2/frontend/faad+0x41a698)

0x602000000011 is located 0 bytes to the right of 1-byte region [0x602000000010,0x602000000011)
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 0x51e387 in stszin /home/seviezhou/faad2/frontend/mp4read.c:348:28
    #2 0x517c4d in parse /home/seviezhou/faad2/frontend/mp4read.c:766:19
    #3 0x517ec2 in parse /home/seviezhou/faad2/frontend/mp4read.c:790:24
    #4 0x517ec2 in parse /home/seviezhou/faad2/frontend/mp4read.c:790:24
    #5 0x517ec2 in parse /home/seviezhou/faad2/frontend/mp4read.c:790:24
    #6 0x517ec2 in parse /home/seviezhou/faad2/frontend/mp4read.c:790:24
    #7 0x518cf8 in moovin /home/seviezhou/faad2/frontend/mp4read.c:867:15
    #8 0x517c4d in parse /home/seviezhou/faad2/frontend/mp4read.c:766:19
    #9 0x5169a5 in mp4read_open /home/seviezhou/faad2/frontend/mp4read.c:1005:16
    #10 0x52de44 in decodeMP4file /home/seviezhou/faad2/frontend/main.c:830:9
    #11 0x52de44 in faad_main /home/seviezhou/faad2/frontend/main.c:1323
    #12 0x7f92a07fc83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/faad2/frontend/mp4read.c:355:29 in stszin
Shadow bytes around the buggy address:
  0x0c047fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c047fff8000: fa fa[01]fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: 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
==36828==ABORTING
```

POC

heap-overflow-stszin-mp4read-355.zip

fabiangreffrath closed this as completed in `1b71a6b` on Aug 31, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant