

New issue

Jump to bottom

A Segmentation fault in output.c:49:16 #58

Closed seviezhou opened this issue on Aug 30, 2020 · 0 comments · Fixed by #66

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 190.264 secs, 6 ch, 44100 Hz

AddressSanitizer:DEADLYSIGNAL
=====
==3662==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x000000546b64 bp 0x629000000200 sp 0x7ffed5a32ff0 T0)
==3662==The signal is caused by a READ memory access.
==3662==Hint: address points to the zero page.
#0 0x546b63 in get_sample /home/seviezhou/faad2/libfaad/output.c:49:16
#1 0x546b63 in to_PCM_double /home/seviezhou/faad2/libfaad/output.c:390
#2 0x546b63 in output_to_PCM /home/seviezhou/faad2/libfaad/output.c:427
#3 0x53b8df in aac_frame_decode /home/seviezhou/faad2/libfaad/decoder.c:1176:21
#4 0x52f738 in decodeMP4file /home/seviezhou/faad2/frontend/main.c:916:25
#5 0x52f738 in faad_main /home/seviezhou/faad2/frontend/main.c:1323
#6 0x7fb2de93483f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
#7 0x41a698 in _start (/home/seviezhou/faad2/frontend/faad+0x41a698)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/faad2/libfaad/output.c:49:16 in get_sample
==3662==ABORTING
```

POC

[SEGV-get_sample-output-49.zip](#)

 fabiangreiff mentioned this issue on Oct 8, 2020

Fix NULL dereferences and hangs. #65

Merged

 awesie added a commit to awesie/faad2 that referenced this issue on Oct 9, 2020

 Check for error after each channel decode. ...

7778bb8

 awesie added a commit to awesie/faad2 that referenced this issue on Oct 9, 2020

 Check for error after each channel decode. ...

b588401

 awesie mentioned this issue on Oct 9, 2020

Fix additional crashes. #66

Merged

 fabiangreiff closed this as completed in #66 on Oct 9, 2020

Assignees

No one assigned

Labels

None yet

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **Fix additional crashes.**
awesie/faad2

1 participant

