New issue

Jump to bottom

A Segmentation fault in box_code_base.c:11579 #1586

Closed seviezhou opened this issue on Sep 4, 2020 · 0 comments

seviezhou commented on Sep 4, 2020

System info

Ubuntu x86_64, gcc (Ubuntu 5.5.0-12ubuntu1), MP4Box (latest master 5a884e)

Configure

CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" ./configure --static-mp4box

Command line

./bin/gcc/MP4Box -diso -out /dev/null @@

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==14934==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000010 (pc 0x556b734996bc bp 0x0c0c00001d9e sp 0x7fffb5212f80 T0)
    #0 0x556b734996bb in vwid_box_del isomedia/box_code_base.c:11579
    #1 0x556b721a79de in gf_isom_box_del isomedia/box_funcs.c:1668
    #2 0x556b721ab705 in gf_isom_box_parse_ex isomedia/box_funcs.c:295
    #3 0x556b721ac7a1 in gf_isom_parse_root_box isomedia/box_funcs.c:38
    #4 0x556b721e2f9c in gf_isom_parse_movie_boxes isomedia/isom_intern.c:259
    #5 0x556b721ede7e in gf_isom_parse_movie_boxes isomedia/isom_intern.c:247
    #6 0x556b721ede7e in gf_isom_open_file isomedia/isom_intern.c:740
    #7 0x556b71b167df in mp4boxMain /home/seviezhou/gpac/applications/mp4box/main.c:5333
    #8 0x7f5bcfaeeb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #9 0x556b71ae9be9 in _start (/home/seviezhou/gpac/bin/gcc/MP4Box+0x280be9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/box_code_base.c:11579 vwid_box_del
==14934==ABORTING
```

POC

SEGV-vwid_box_del-box_code_base-11579.zip

jeanlf closed this as completed in 362fc48 on Sep 7, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant