


New issue

Jump to bottom

A Segmentation fault in box_dump.c:3641 #1574

 Closed seviezhou opened this issue on Aug 12, 2020 · 0 comments

seviezhou commented on Aug 12, 2020

System info

Ubuntu x86_64, gcc (Ubuntu 5.5.0-12ubuntu1), MP4Box (latest master [2aa266](#))

Configure

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

Command line

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

AddressSanitizer output

```
ASAN:SIGSEGV
=====
==77583==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000038 (pc 0x555d67a9030a bp 0x61600000cf80 sp 0x7ffc245f5240 T0)
#0 0x555d67a90309 in 1lst_item_box_dump isomedia/box_dump.c:3641
#1 0x555d67ac2749 in gf_isom_box_dump isomedia/box_funcs.c:1923
#2 0x555d67a6caba in gf_isom_dump isomedia/box_dump.c:135
#3 0x555d67449ce9 in dump_isom_xml /home/seviezhou/gpac/applications/mp4box/filedump.c:1670
#4 0x555d6741afa4 in mp4boxMain /home/seviezhou/gpac/applications/mp4box/main.c:5548
#5 0x7fe303b6bb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#6 0x555d673f8f09 in _start (/home/seviezhou/gpac/bin/gcc/MP4Box+0x27ff09)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/box_dump.c:3641 1lst_item_box_dump
==77583==ABORTING
```

POC

[SEGV-1lst_item_box_dump-box_dump-3641.zip](#)

 jeanlf closed this as completed in [fc4d8f5](#) on Sep 1, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

