gpac / **gpac** Public

Code Issues 13 Pull requests 2 Wiki Security Insights

New issue

Jump to bottom

A Segmentation fault in filedump.c:1627 #1566

Closed **seviezhou** opened this issue on Aug 6, 2020 · 0 comments

seviezhou commented on Aug 6, 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 -sdp -ttxt -2 -dump-chap-ogg -dump-cover -drtp -bt -out /dev/null @@

Output

```
Scene loaded - dumping root scene
Exporting MPEG-4 AAC Audio - SampleRate 44100 2 channels 16 bits per sample
Segmentation fault (core dumped)
```

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==31981==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f1269c005a1 bp 0x000000000000 sp 0x7fffad3ba678 T0)
    #0 0x7f1269c005a0  (/lib/x86_64-linux-gnu/libc.so.6+0x18e5a0)
    #1 0x7f1269af1204 in fputs (/lib/x86_64-linux-gnu/libc.so.6+0x7f204)
    #2 0x55eb9834073a in dump_isom_sdp /home/seviezhou/gpac/applications/mp4box/filedump.c:1627
    #3 0x55eb98311eb3 in mp4boxMain /home/seviezhou/gpac/applications/mp4box/main.c:5533
    #4 0x7f1269a93b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #5 0x55eb982eff09 in _start (/home/seviezhou/gpac/bin/gcc/MP4Box+0x27ff09)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ??:0 ??
==31981==ABORTING
```

POC

SEGV-dump_isom_sdp-filedump-1627.zip

jeanlf closed this as completed in ce01bd1 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