New issue

Jump to bottom

null dereference in MP4Box MergeTrack #1736

Closed 5n1p3r0010 opened this issue on Apr 8, 2021 · 0 comments

5n1p3r0010 commented on Apr 8, 2021

Hi,

There is a null dereference issue with gpac MP4Box,this can reproduce on the lattest commit.

Steps To Reproduce

build:

```
CC=gcc CXX=g++ CFLAGS="-fsanitize=address" CXXFLAGS="-fsanitize=address" LDFLAGS="-fsanitize=address" ./configure
make
```

run as:

```
MP4Box -hint <poc> -out /dev/null
```

shows the following log:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2662459==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f1e68d92dd9 bp 0x7ffe9fef18c0 sp 0x7ffe9fef16f0 T0)
==2662459==The signal is caused by a READ memory access.
==2662459==Hint: address points to the zero page.
    #0 0x7f1e68d92dd8 in MergeTrack isomedia/track.c:1038
    #1 0x7f1e68d3e50e in MergeFragment isomedia/isom_intern.c:90
    #2 0x7f1e68d40295 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:622
    #3 0x7f1e68d40855 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:750
    #4 0x7f1e68d40be8 in gf_isom_open_file isomedia/isom_intern.c:870
    #5 0x7f1e68d43bc4 in gf_isom_open isomedia/isom_read.c:520
    #6 0x560653ebbd8a in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5699
    #7 0x560653ebe54d in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6312
    #8 0x7f1e688c00b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #9 0x560653eaa20d in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x1820d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/track.c:1038 in MergeTrack
==2662459==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
null_MergeTrack.zip

jeanlf closed this as completed in `df8fffd` on Apr 8, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant