New issue

Jump to bottom

null dereference in MP4Box gf_isom_cenc_get_default_info_internal #1735

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
=================================================================
==2601603==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x7f35e5cc871e bp 0x7ffd01f9fad0 sp 0x7ffd01f9fa60 T0)
==2601603==The signal is caused by a READ memory access.
==2601603==Hint: address points to the zero page.
    #0 0x7f35e5cc871d in gf_isom_cenc_get_default_info_internal isomedia/drm_sample.c:1689
    #1 0x7f35e5cda27e in gf_isom_get_sample_cenc_info_internal isomedia/isom_read.c:4862
    #2 0x7f35e5ca3c5d in senc_Parse isomedia/box_code_drm.c:1341
    #3 0x7f35e5d1e2d9 in MergeTrack isomedia/track.c:1110
    #4 0x7f35e5cc950e in MergeFragment isomedia/isom_intern.c:90
    #5 0x7f35e5ccb295 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:622
    #6 0x7f35e5ccb855 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:750
    #7 0x7f35e5ccbbe8 in gf_isom_open_file isomedia/isom_intern.c:870
    #8 0x7f35e5ccebc4 in gf_isom_open isomedia/isom_read.c:520
    #9 0x564eaf2e1d8a in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5699
    #10 0x564eaf2e454d in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6312
    #11 0x7f35e584b0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #12 0x564eaf2d020d in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x1820d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/drm_sample.c:1689 in gf_isom_cenc_get_default_info_internal
==2601603==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
null_gf_isom_cenc_get_default_info_internal.zip

jeanlf closed this as completed in 3b84ffc 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