New issue

Jump to bottom

null dereference in MP4Box trak_box_size #1757

Closed **5n1p3r0010** opened this issue on Apr 22, 2021 · 0 comments

5n1p3r0010 commented on Apr 22, 2021

Hi,

There is a null dereference issue in gpac MP4Box trak_box_size,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 --enable-debug
make
```

run as:

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

shows the following log:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2912==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000058 (pc 0x7f0b5bc03250 bp 0x7fffbdc68da0 sp 0x7fffbdc68d70 T0)
==2912==The signal is caused by a READ memory access.
==2912==Hint: address points to the zero page.
    #0 0x7f0b5bc0324f in trak_box_size isomedia/box_code_base.c:6748
    #1 0x7f0b5bc3ad55 in gf_isom_box_size_listing isomedia/box_funcs.c:1901
    #2 0x7f0b5bc3ada6 in gf_isom_box_size isomedia/box_funcs.c:1913
    #3 0x7f0b5bc5a338 in WriteInterleaved isomedia/isom_store.c:1898
    #4 0x7f0b5bc5c1ec in WriteToFile isomedia/isom_store.c:2471
    #5 0x7f0b5bc47de8 in gf_isom_write isomedia/isom_read.c:600
    #6 0x7f0b5bc47ee9 in gf_isom_close isomedia/isom_read.c:624
    #7 0x558adcb08381 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6265
    #8 0x558adcb0863e in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6319
    #9 0x7f0b5b7c20b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #10 0x558adcaf426d in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x1826d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/box_code_base.c:6748 in trak_box_size
==2912==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
null_trak_box_size.zip

jeanlf closed this as completed in b8f8b20 on Apr 23, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant