New issue

Jump to bottom

null dereference issue in MP4Box abst_box_size #1753

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 abst_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
=================================================================
==429109==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f8c2ee47675 bp 0x7ffc1a1c5fa0 sp 0x7ffc1a1c5718 T0)
==429109==The signal is caused by a READ memory access.
==429109==Hint: address points to the zero page.
    #0 0x7f8c2ee47674  (/lib/x86_64-linux-gnu/libc.so.6+0x18b674)
    #1 0x7f8c2f8e28fb  (/lib/x86_64-linux-gnu/libasan.so.5+0x678fb)
    #2 0x7f8c2f1c82fb in abst_box_size isomedia/box_code_adobe.c:316
    #3 0x7f8c2f15bd55 in gf_isom_box_size_listing isomedia/box_funcs.c:1901
    #4 0x7f8c2f15bda6 in gf_isom_box_size isomedia/box_funcs.c:1913
    #5 0x7f8c2f17b338 in WriteInterleaved isomedia/isom_store.c:1898
    #6 0x7f8c2f17d1ec in WriteToFile isomedia/isom_store.c:2471
    #7 0x7f8c2f168de8 in gf_isom_write isomedia/isom_read.c:600
    #8 0x7f8c2f168ee9 in gf_isom_close isomedia/isom_read.c:624
    #9 0x557be3ad5381 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6265
    #10 0x557be3ad563e in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6319
    #11 0x7f8c2ece30b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #12 0x557be3ac126d in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x1826d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0x18b674)
==429109==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
null_abst_box_size.zip

jeanlf closed this as completed in e74be59 on Apr 22, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant