null dereference issue with MP4Box #1706

Closed 5n1p3r0010 opened this issue on Mar 12, 2021 · 0 comments

5n1p3r0010 commented on Mar 12, 2021

Hi,

There is a null dereference issue with MP4Box,this can reproduce on the lattest commit aka `ee87237` .

Steps to reproduce

build with asan:

```
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:

```
[iso file] Unknown box type 0000 in parent trak
[iso file] Unknown box type C5sds in parent mp4s
[iso file] Unknown box type tra87 in parent moov
[iso file] Box "UNKN" is larger than container box
[iso file] Box "moov" size 12336 (start 44) invalid (read 13329)
[iso file] Unknown top-level box type 00d00
Track ID 808464432 disabled - skipping hint
AddressSanitizer:DEADLYSIGNAL
=================================================================
==33096==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000028 (pc 0x7fbefe8b0094 bp 0x7ffc3da91b80 sp 0x7ffc3da91ac0 T0)
==33096==The signal is caused by a READ memory access.
==33096==Hint: address points to the zero page.
    #0 0x7fbefe8b0093 in gf_isom_set_extraction_slc (/home/r00t/fuzz/target/gpac/bin/gcc/libgpac.so.10+0x242093)
    #1 0x7fbefe990add in gf_hinter_track_new (/home/r00t/fuzz/target/gpac/bin/gcc/libgpac.so.10+0x322add)
    #2 0x55babb63b9f1 in HintFile (/home/r00t/fuzz/target/gpac/bin/gcc/MP4Box+0x239f1)
    #3 0x55babb63f5e2 in mp4boxMain (/home/r00t/fuzz/target/gpac/bin/gcc/MP4Box+0x275e2)
    #4 0x7fbefe4a30b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #5 0x55babb63026d in _start (/home/r00t/fuzz/target/gpac/bin/gcc/MP4Box+0x1826d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/home/r00t/fuzz/target/gpac/bin/gcc/libgpac.so.10+0x242093) in gf_isom_set_extraction_slc
==33096==ABORTING
```

Reporter

5n1p3r0010 from Topsec Alpha Lab

null.zip

jeanlf closed this as completed in `ebfa346` on Mar 12, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant