New issue

Jump to bottom

null dereference in MP4Box DumpTrackInfo #1767

Closed **5n1p3r0010** opened this issue on Apr 29, 2021 · 0 comments

5n1p3r0010 commented on Apr 29, 2021

Hi,

There is a null dereference issue in gpac MP4Box DumpTrackInfo,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 -info <poc>
```

shows the following log:

```
=================================================================
==3138257==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x55ffcb90f3d9 bp 0x7fffae555b10 sp 0x7fffae52f160 T0)
==3138257==The signal is caused by a READ memory access.
==3138257==Hint: address points to the zero page.
    #0 0x55ffcb90f3d8 in DumpTrackInfo /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/filedump.c:2877
    #1 0x55ffcb91323c in DumpMovieInfo /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/filedump.c:3590
    #2 0x55ffcb9008f5 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5904
    #3 0x55ffcb902653 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6335
    #4 0x7f17fb5c50b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #5 0x55ffcb8ee2ad in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x182ad)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/filedump.c:2877 in DumpTrackInfo
==3138257==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
null_DumpTrackInfo.zip

jeanlf closed this as completed in `289ffce` on Apr 30, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant