New issue

Jump to bottom

null dereference in gpac MP4Box gf_isom_vp_config_get #1768

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 gf_isom_vp_config_get,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:

```
=================================================================
==3138269==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7ffb91dc655f bp 0x7ffc1244f800 sp 0x7ffc1244f7e0 T0)
==3138269==The signal is caused by a READ memory access.
==3138269==Hint: address points to the zero page.
    #0 0x7ffb91dc655e in gf_isom_vp_config_get isomedia/avc_ext.c:2423
    #1 0x7ffb91ebb6d4 in gf_media_get_rfc_6381_codec_name media_tools/isom_tools.c:4119
    #2 0x5639a7f6f7e9 in DumpTrackInfo /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/filedump.c:3255
    #3 0x5639a7f7123c in DumpMovieInfo /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/filedump.c:3590
    #4 0x5639a7f5e8f5 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5904
    #5 0x5639a7f60653 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6335
    #6 0x7ffb919a90b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #7 0x5639a7f4c2ad in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x182ad)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/avc_ext.c:2423 in gf_isom_vp_config_get
==3138269==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
null_gf_isom_vp_config_get.zip

jeanlf closed this as completed in d527325 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