New issue

Jump to bottom

null dereference in MP4Box gf_odf_desc_copy #1756

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 gf_odf_desc_copy,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
=================================================================
==2865==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7ff7034c09ac bp 0x7ffc860743b0 sp 0x7ffc86074360 T0)
==2865==The signal is caused by a READ memory access.
==2865==Hint: address points to the zero page.
    #0 0x7ff7034c09ab in gf_odf_desc_copy odf/odf_codec.c:378
    #1 0x7ff70347f64c in Media_GetESD isomedia/media.c:411
    #2 0x7ff703455727 in gf_isom_get_decoder_config isomedia/isom_read.c:1319
    #3 0x7ff70345caa2 in gf_isom_guess_specification isomedia/isom_read.c:3905
    #4 0x55891de6c817 in HintFile /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:3312
    #5 0x55891de77e5b in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6193
    #6 0x55891de7863e in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6319
    #7 0x7ff702fce0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #8 0x55891de6426d in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x1826d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV odf/odf_codec.c:378 in gf_odf_desc_copy
==2865==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
null_gf_odf_desc_copy.zip

jeanlf closed this as completed in 328c6d6 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