New issue

Jump to bottom

null dereference in AV1_DuplicateConfig #1738

Closed 5n1p3r0010 opened this issue on Apr 8, 2021 · 0 comments

5n1p3r0010 commented on Apr 8, 2021

Hi,

There is a null dereference issue with gpac MP4Box,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
=================================================================
==2125572==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f0959a08b30 bp 0x7ffed8940580 sp 0x7ffed8940550 T0)
==2125572==The signal is caused by a READ memory access.
==2125572==Hint: address points to the zero page.
    #0 0x7f0959a08b2f in AV1_DuplicateConfig isomedia/avc_ext.c:1345
    #1 0x7f0959a08dbb in AV1_RewriteESDescriptorEx isomedia/avc_ext.c:1386
    #2 0x7f0959a08e33 in AV1_RewriteESDescriptor isomedia/avc_ext.c:1396
    #3 0x7f0959a25700 in video_sample_entry_box_read isomedia/box_code_base.c:4252
    #4 0x7f0959a66e6d in gf_isom_box_read isomedia/box_funcs.c:1801
    #5 0x7f0959a6570f in gf_isom_box_parse_ex isomedia/box_funcs.c:260
    #6 0x7f0959a66971 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1698
    #7 0x7f0959a298a2 in stsd_box_read isomedia/box_code_base.c:5340
    #8 0x7f0959a66e6d in gf_isom_box_read isomedia/box_funcs.c:1801
    #9 0x7f0959a6570f in gf_isom_box_parse_ex isomedia/box_funcs.c:260
    #10 0x7f0959a66971 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1698
    #11 0x7f0959a65c91 in gf_isom_box_array_read isomedia/box_funcs.c:381
    #12 0x7f0959a28787 in stbl_box_read isomedia/box_code_base.c:5003
    #13 0x7f0959a66e6d in gf_isom_box_read isomedia/box_funcs.c:1801
    #14 0x7f0959a6570f in gf_isom_box_parse_ex isomedia/box_funcs.c:260
    #15 0x7f0959a66971 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1698
    #16 0x7f0959a65c91 in gf_isom_box_array_read isomedia/box_funcs.c:381
    #17 0x7f0959a21d53 in minf_box_read isomedia/box_code_base.c:3494
    #18 0x7f0959a66e6d in gf_isom_box_read isomedia/box_funcs.c:1801
    #19 0x7f0959a6570f in gf_isom_box_parse_ex isomedia/box_funcs.c:260
    #20 0x7f0959a66971 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1698
    #21 0x7f0959a65c91 in gf_isom_box_array_read isomedia/box_funcs.c:381
    #22 0x7f0959a20680 in mdia_box_read isomedia/box_code_base.c:3049
    #23 0x7f0959a66e6d in gf_isom_box_read isomedia/box_funcs.c:1801
    #24 0x7f0959a6570f in gf_isom_box_parse_ex isomedia/box_funcs.c:260
    #25 0x7f0959a66971 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1698
    #26 0x7f0959a65c91 in gf_isom_box_array_read isomedia/box_funcs.c:381
    #27 0x7f0959a2f637 in trak_box_read isomedia/box_code_base.c:6691
    #28 0x7f0959a66e6d in gf_isom_box_read isomedia/box_funcs.c:1801
    #29 0x7f0959a6570f in gf_isom_box_parse_ex isomedia/box_funcs.c:260
    #30 0x7f0959a66971 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1698
    #31 0x7f0959a65c91 in gf_isom_box_array_read isomedia/box_funcs.c:381
    #32 0x7f0959a22988 in moov_box_read isomedia/box_code_base.c:3672
    #33 0x7f0959a66e6d in gf_isom_box_read isomedia/box_funcs.c:1801
    #34 0x7f0959a6570f in gf_isom_box_parse_ex isomedia/box_funcs.c:260
    #35 0x7f0959a64c08 in gf_isom_parse_root_box isomedia/box_funcs.c:38
    #36 0x7f0959a6f3d8 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:318
    #37 0x7f0959a70b2c in gf_isom_parse_movie_boxes isomedia/isom_intern.c:750
    #38 0x7f0959a70ebf in gf_isom_open_file isomedia/isom_intern.c:870
    #39 0x7f0959a73e9b in gf_isom_open isomedia/isom_read.c:520
    #40 0x559f115aee26 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5699
    #41 0x559f115b15e9 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6312
    #42 0x7f09595f00b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #43 0x559f1159d26d in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x1826d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/avc_ext.c:1345 in AV1_DuplicateConfig
==2125572==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
null_AV1_DuplicateConfig.zip

jeanlf closed this as completed in b2eab95 on Apr 9, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant