New issue

Jump to bottom

# [security]memory leak in MP4Box gf_isom_oinf_read_entry #1785

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

**5n1p3r0010** commented on May 8, 2021

Hi,

There is a memory leak issue in gpac MP4Box gf_isom_oinf_read_entry,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:

```
=================================================================
==3514810==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 804 byte(s) in 1 object(s) allocated from:
    #0 0x7f8fe09cabc8 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f8fdff07dcb in gf_malloc utils/alloc.c:150
    #2 0x7f8fe00bad7a in gf_isom_oinf_read_entry isomedia/avc_ext.c:3371
    #3 0x7f8fe01767f5 in oinf_box_read isomedia/iff.c:821
    #4 0x7f8fe0112748 in gf_isom_box_read isomedia/box_funcs.c:1796
    #5 0x7f8fe011104b in gf_isom_box_parse_ex isomedia/box_funcs.c:261
    #6 0x7f8fe01104ec in gf_isom_parse_root_box isomedia/box_funcs.c:38
    #7 0x7f8fe011ae04 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:318
    #8 0x7f8fe011c708 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:777
    #9 0x7f8fe011ca9b in gf_isom_open_file isomedia/isom_intern.c:897
    #10 0x7f8fe011fa41 in gf_isom_open isomedia/isom_read.c:509
    #11 0x55d2ad597e7e in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5720
    #12 0x55d2ad59a653 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6333
    #13 0x7f8fdfc810b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: 804 byte(s) leaked in 1 allocation(s).
```

**Reporter:**

5n1p3r0010 from Topsec Alpha Lab
gf_isom_oinf_read_entry.zip

**jeanlf** closed this as completed in `0a85029` on May 10, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant