New issue

Jump to bottom

[security]memory leak in MP4Box def_parent_box_new #1783

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 def_parent_box_new,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:

```
=================================================================
==3270106==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 40 byte(s) in 1 object(s) allocated from:
    #0 0x7fe319beebc8 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7fe31912bdcb in gf_malloc utils/alloc.c:150
    #2 0x7fe3192e9864 in def_parent_box_new isomedia/box_code_base.c:848
    #3 0x7fe31933611b in gf_isom_box_new_ex isomedia/box_funcs.c:1659
    #4 0x7fe319334f22 in gf_isom_box_parse_ex isomedia/box_funcs.c:237
    #5 0x7fe3193344ec in gf_isom_parse_root_box isomedia/box_funcs.c:38
    #6 0x7fe31933ee04 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:318
    #7 0x7fe319340708 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:777
    #8 0x7fe319343922 in gf_isom_open_progressive_ex isomedia/isom_read.c:467
    #9 0x7fe3193439d2 in gf_isom_open_progressive isomedia/isom_read.c:493
    #10 0x563842c0bee1 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5724
    #11 0x563842c0e653 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6333
    #12 0x7fe318ea50b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: 40 byte(s) leaked in 1 allocation(s).
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
def_parent_box_new.zip

jeanlf closed this as completed in `fe5155c` 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