New issue   Jump to bottom

[security]memory leak in MP4Box afra_box_read #1782

⊘ 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 afra_box_read,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:

```
===============================================================
==3004994==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 32 byte(s) in 1 object(s) allocated from:
    #0 0x7fd19035bbc8 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7fd18f898dcb in gf_malloc utils/alloc.c:150
    #2 0x7fd18fb1140b in afra_box_read isomedia/box_code_adobe.c:429
    #3 0x7fd18faa3748 in gf_isom_box_read isomedia/box_funcs.c:1796
    #4 0x7fd18faa204b in gf_isom_box_parse_ex isomedia/box_funcs.c:261
    #5 0x7fd18faa14ec in gf_isom_parse_root_box isomedia/box_funcs.c:38
    #6 0x7fd18faabe04 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:318
    #7 0x7fd18faad708 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:777
    #8 0x7fd18faada9b in gf_isom_open_file isomedia/isom_intern.c:897
    #9 0x7fd18fab0a41 in gf_isom_open isomedia/isom_read.c:509
    #10 0x5576f4935e7e in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5720
    #11 0x5576f4938653 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6333
    #12 0x7fd18f6120b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: 32 byte(s) leaked in 1 allocation(s).
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
afra_box_read.zip

⊙ **jeanlf** closed this as completed in a51f951 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