New issue

Jump to bottom

Segmentation fault caused by null pointer dereference using mp4box in gf_isom_get_payt_count, hint_track.c:990 #1904

Closed 3 tasks done **5hadowblad3** opened this issue on Aug 31, 2021 · 0 comments

5hadowblad3 commented on Aug 31, 2021 • edited

- [x] I looked for a similar issue and couldn't find any.
- [x] I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
- [x] I give enough information for contributors to reproduce my issue (meaningful title, github labels, platform and compiler, command-line ...).

Hi, there.

There is a segmentation fault caused by null pointer dereference in gf_isom_get_payt_count, hint_track.c:990 in commit `d003a57` .

Here is my environment, compiler info and gpac version:

```
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.6 LTS
Release:        16.04
Codename:       xenial
gcc: 5.4.0

MP4Box - GPAC version 1.1.0-DEV-rev1191-g55d6dbc-master
(c) 2000-2021 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io
        MINI build (encoders, decoders, audio and video output disabled)

Please cite our work in your research:
        GPAC Filters: https://doi.org/10.1145/3339825.3394929
        GPAC: https://doi.org/10.1145/1291233.1291452

GPAC Configuration: --static-bin --enable-debug
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_SOCK_UN GPAC_MINIMAL_ODF GPAC_HAS_QJS GPAC_HAS_FREETYPE GPAC_HAS_JPEG GPAC_HAS_PNG  GPAC_DISABLE_3D
```

To reproduce, run

```
./MP4Box -info poc
```

POC:
poc.zip
(unzip first)

Here is the trace reported by gdb:

```
Stopped reason: SIGSEGV
gef➤  bt
#0  0x0000000000ab4f30 in gf_isom_get_payt_count (the_file=the_file@entry=0x248c220, trackNumber=trackNumber@entry=0x4) at /mnt/data/playground/gpac/src/isomedia/hint_track.c:990
#1  0x0000000000490533 in DumpTrackInfo (file=file@entry=0x248c220, trackID=0x6, trackID@entry=0x4, full_dump=full_dump@entry=GF_FALSE, is_track_num=is_track_num@entry=GF_TRUE,
dump_m4sys=dump_m4sys@entry=GF_TRUE) at /mnt/data/playground/gpac/applications/mp4box/filedump.c:3178
#2  0x0000000000491d78 in DumpMovieInfo (file=0x248c220, full_dump=GF_FALSE) at /mnt/data/playground/gpac/applications/mp4box/filedump.c:3789
#3  0x0000000000456587 in mp4boxMain (argc=<optimized out>, argv=<optimized out>) at /mnt/data/playground/gpac/applications/mp4box/main.c:6023
#4  0x0000000001f06976 in generic_start_main ()
#5  0x0000000001f06f65 in __libc_start_main ()
#6  0x000000000041c4e9 in _start ()
```

jeanlf closed this as completed in `ad18ece` on Sep 1, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant