New issue

Jump to bottom

Segmentation fault using mp4box in ilst_box_read, box_code_apple.c:50 #1895

Closed ○ 3 tasks done **5hadowblad3** opened this issue on Aug 26, 2021 · 0 comments

5hadowblad3 commented on Aug 26, 2021

- ☑ I looked for a similar issue and couldn't find any.
- ☑ I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
- ☑ 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 ilst_box_read, box_code_apple.c:50 in commit `592ba26` .

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-rev1170-g592ba26-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 -hint poc
```

POC:
poc.zip
(unzip first)

Here is the trace reported by gdb:

```
Stopped reason: SIGSEGV
gef➤  bt
#0  0x0000000001963358 in ilst_box_read (s=0x248f740, bs=0x248c750) at /mnt/data/playground/gpac/src/isomedia/box_code_apple.c:50
#1  0x00000000008ff1fa in gf_isom_box_read (bs=0x248c750, a=0x248f740) at /mnt/data/playground/gpac/src/isomedia/box_funcs.c:1810
#2  gf_isom_box_parse_ex (outBox=outBox@entry=0x7fffffff9360, bs=bs@entry=0x248c750, is_root_box=is_root_box@entry=GF_TRUE, parent_type=0x0) at
/mnt/data/playground/gpac/src/isomedia/box_funcs.c:263
#3  0x0000000000900cf2 in gf_isom_parse_root_box (outBox=outBox@entry=0x7fffffff9360, bs=0x248c750, box_type=box_type@entry=0x0, bytesExpected=bytesExpected@entry=0x7fffffff93b0,
progressive_mode=progressive_mode@entry=GF_FALSE) at /mnt/data/playground/gpac/src/isomedia/box_funcs.c:38
#4  0x000000000093551f in gf_isom_parse_movie_boxes_internal (mov=mov@entry=0x248c220, boxType=boxType@entry=0x0, bytesMissing=bytesMissing@entry=0x7fffffff93b0,
progressive_mode=progressive_mode@entry=GF_FALSE) at /mnt/data/playground/gpac/src/isomedia/isom_intern.c:320
#5  0x000000000093e251 in gf_isom_parse_movie_boxes (progressive_mode=GF_FALSE, bytesMissing=0x7fffffff93b0, boxType=0x0, mov=0x248c220) at
/mnt/data/playground/gpac/src/isomedia/isom_intern.c:781
#6  gf_isom_open_file (fileName=0x7fffffffe159 "tmp", OpenMode=<optimized out>, tmp_dir=0x0) at /mnt/data/playground/gpac/src/isomedia/isom_intern.c:901
#7  0x0000000000454a80 in mp4boxMain (argc=<optimized out>, argv=<optimized out>) at /mnt/data/playground/gpac/applications/mp4box/main.c:5841
#8  0x0000000001f06bb6 in generic_start_main ()
#9  0x0000000001f071a5 in __libc_start_main ()
#10 0x000000000041c4e9 in _start ()
```

5hadowblad3 changed the title ~~Segmentation fault casued by null pointer dereference using mp4box in ilst_box_read, box_code_apple.c:50~~ **Segmentation fault using mp4box in ilst_box_read, box_code_apple.c:50** on Aug 26, 2021

jeanlf closed this as completed in `a69b567` on Aug 30, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant