New issue

Jump to bottom

Segmentation fault using mp4box in gf_odf_size_descriptor, desc_private.c:380 #1889

Closed 3 tasks done **5hadowblad3** opened this issue on Aug 24, 2021 · 2 comments

5hadowblad3 commented on Aug 24, 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 in gf_odf_desc_copy, odf_codec.c:381 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  0x0000000001a016e8 in gf_odf_size_descriptor (desc=0x3e8024746a0, outSize=outSize@entry=0x7fffffff6994) at /mnt/data/playground/gpac/src/odf/desc_private.c:380
#1  0x0000000000aeaaee in gf_odf_size_dcd (dcd=0x7fffffff6ae0, outSize=0x7fffffff69c4) at /mnt/data/playground/gpac/src/odf/odf_code.c:1211
#2  0x0000000001a01b15 in gf_odf_size_descriptor (desc=desc@entry=0x7fffffff6ae0, outSize=outSize@entry=0x7fffffff69c4) at /mnt/data/playground/gpac/src/odf/desc_private.c:386
#3  0x0000000000aeade9 in gf_odf_write_dcd (bs=0x249a960, dcd=0x7fffffff6ae0) at /mnt/data/playground/gpac/src/odf/odf_code.c:1235
#4  0x0000000001a020bd in gf_odf_write_descriptor (bs=bs@entry=0x249a960, desc=desc@entry=0x7fffffff6ae0) at /mnt/data/playground/gpac/src/odf/desc_private.c:487
#5  0x0000000000af1357 in gf_odf_desc_write_bs (desc=desc@entry=0x7fffffff6ae0, bs=bs@entry=0x249a960) at /mnt/data/playground/gpac/src/odf/odf_codec.c:325
#6  0x0000000000af14b7 in gf_odf_desc_write (desc=desc@entry=0x7fffffff6ae0, outEncDesc=outEncDesc@entry=0x7fffffff6a30, outSize=outSize@entry=0x7fffffff6a2c) at
/mnt/data/playground/gpac/src/odf/odf_codec.c:343
#7  0x0000000000af17f6 in gf_odf_desc_copy (inDesc=inDesc@entry=0x7fffffff6ae0, outDesc=outDesc@entry=0x2497550) at /mnt/data/playground/gpac/src/odf/odf_codec.c:387
#8  0x00000000009d2a3f in gf_isom_set_extraction_slc (the_file=the_file@entry=0x248c220, trackNumber=trackNumber@entry=0x6, StreamDescriptionIndex=StreamDescriptionIndex@entry=0x1,
slConfig=slConfig@entry=0x7fffffff6ae0) at /mnt/data/playground/gpac/src/isomedia/isom_write.c:5468
#9  0x0000000000ce75ff in gf_hinter_finalize (file=file@entry=0x248c220, IOD_Profile=<optimized out>, bandwidth=bandwidth@entry=0x8bdf) at
/mnt/data/playground/gpac/src/media_tools/isom_hinter.c:1245
#10 0x000000000043c218 in HintFile (file=0x248c220, MTUSize=MTUSize@entry=0x59e, max_ptime=0x0, rtp_rate=0x0, base_flags=<optimized out>, copy_data=GF_FALSE, interleave=GF_FALSE,
regular_iod=GF_FALSE, single_group=GF_FALSE, hint_no_offset=GF_FALSE) at /mnt/data/playground/gpac/applications/mp4box/main.c:3550
#11 0x000000000044bd42 in mp4boxMain (argc=<optimized out>, argv=<optimized out>) at /mnt/data/playground/gpac/applications/mp4box/main.c:6329
#12 0x0000000001f06bb6 in generic_start_main ()
#13 0x0000000001f071a5 in __libc_start_main ()
#14 0x000000000041c4e9 in _start ()
```

aureliendavid commented on Aug 24, 2021 • edited Contributor

EDIT: I posted in the wrong issue

jeanlf commented on Aug 30, 2021 Contributor

cf fixes for #1885

jeanlf closed this as completed on Aug 30, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants