New issue

Jump to bottom

System abort caused by double free using mp4box, gf_list_del, list.c:614 #1891

Closed 3 tasks done **5hadowblad3** opened this issue on Aug 25, 2021 · 1 comment

5hadowblad3 commented on Aug 25, 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 system abort in gf_free, alloc.c:165 in commit `592ba26` caused by double free issue, it is similar to issue #1890 but the scenario is different.

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: SIGABRT
gef➤  bt
#0  0x0000000001f15d08 in raise ()
#1  0x0000000001f15f3a in abort ()
#2  0x0000000001f24ed6 in __libc_message ()
#3  0x0000000001f2da76 in _int_free ()
#4  0x0000000001f31af7 in free ()
#5  0x000000000053de4d in gf_free (ptr=<optimized out>) at /mnt/data/playground/gpac/src/utils/alloc.c:165
#6  0x00000000004f8c14 in gf_list_del (ptr=0x482f2f0) at /mnt/data/playground/gpac/src/utils/list.c:614
#7  0x000000000019f4315 in iloc_entry_del (location=0x480b370) at /mnt/data/playground/gpac/src/isomedia/box_code_meta.c:244
#8  iloc_box_del (s=0x248f080) at /mnt/data/playground/gpac/src/isomedia/box_code_meta.c:256
#9  0x00000000008fa22f in gf_isom_box_del (a=0x248f080) at /mnt/data/playground/gpac/src/isomedia/box_funcs.c:1794
#10 0x0000000000900b5c in 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:303
#11 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
#12 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
#13 0x0000000000093e251 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
#14 gf_isom_open_file (fileName=0x7fffffffe159 "tmp", OpenMode=<optimized out>, tmp_dir=0x0) at /mnt/data/playground/gpac/src/isomedia/isom_intern.c:901
#15 0x00000000000454a80 in mp4boxMain (argc=<optimized out>, argv=<optimized out>) at /mnt/data/playground/gpac/applications/mp4box/main.c:5841
#16 0x0000000001f06bb6 in generic_start_main ()
#17 0x0000000001f071a5 in __libc_start_main ()
#18 0x0000000000041c4e9 in _start ()
```

5hadowblad3 changed the title ~~System abort caused by double free using mp4box~~ System abort caused by double free using mp4box, gf_list_del, list.c:614 on Aug 25, 2021

jeanlf commented on Aug 30, 2021 Contributor

cf fixes for #1890

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

2 participants