

New issue

[Jump to bottom](#)

Segmentation fault caused by double free using mp4box in iloc_entry_del, box_code_meta.c:242 #1890

Closed 3 tasks done Shadowblad3 opened this issue on Aug 25, 2021 · 0 comments

Shadowblad3 commented on Aug 25, 2021 • edited

- ☒ 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_free`, `alloc.c:165` in commit [592ba26](#) caused by double free issue.

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 0x000000001f31acf in free ()
#1 0x00000000053de4d in gf_free (ptr=<optimized out>) at /mnt/data/playground/gpac/src/utis/alloc.c:165
#2 0x0000000019f3d5d in iloc_entry_del (location=0x3dd8780) at /mnt/data/playground/gpac/src/isomedia/box_code_meta.c:242
#3 iloc_box_del (s=0x248f080) at /mnt/data/playground/gpac/src/isomedia/box_code_meta.c:256
#4 0x0000000008fa22f in gf_isom_box_del (a=0x248f080) at /mnt/data/playground/gpac/src/isomedia/box_funcs.c:1794
#5 0x00000000090b5c in gf_isom_box_parse_ex (outBox=outBox@entry=0x7fffff9360, 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
#6 0x00000000090bcf2 in gf_isom_parse_root_box (outBox=outBox@entry=0x7fffff9360, bs=0x248c750, box_type=box_type@entry=0x0, bytesExpected=bytesExpected@entry=0x7fffff93b0, progressive_mode=progressive_mode@entry=GF_FALSE) at /mnt/data/playground/gpac/src/isomedia/box_funcs.c:38
#7 0x0000000009351f in gf_isom_parse_movie_boxes_internal (mov=mov@entry=0x248c220, boxType=boxType@entry=0x0, bytesMissing=bytesMissing@entry=0x7fffff93b0, progressive_mode=progressive_mode@entry=GF_FALSE) at /mnt/data/playground/gpac/src/isomedia/isom_intern.c:320
#8 0x00000000093e251 in gf_isom_parse_movie_boxes (progressive_mode=GF_FALSE, bytesMissing=0x7fffff93b0, boxType=0x0, mov=0x248c220) at /mnt/data/playground/gpac/src/isomedia/isom_intern.c:781
#9 gf_isom_open_file (fileName=0x7fffffe159 "tmp", OpenMode=<optimized out>, tmp_dir=0x0) at /mnt/data/playground/gpac/src/isomedia/isom_intern.c:901
#10 0x00000000045a80 in mp4boxMain (argc=<optimized out>, argv=<optimized out>) at /mnt/data/playground/gpac/applications/mp4box/main.c:5841
#11 0x000000001f06bb6 in generic_start_main ()
#12 0x000000001f071a5 in __libc_start_main ()
#13 0x00000000041c4e9 in _start ()
```

It seems that the pointer has been free previously in `configfile.c`

```
455 /* same value, don't update */
456 if (!strcmp(key->value, keyValue)) return GF_OK;
457
458 if (key->value) gf_free(key->value);
459 key->value = gf_strdup(keyValue);
460 if (has_changed)
461     iniFile->hasChanged = GF_TRUE;
462 return GF_OK;
463 }
```

Shadowblad3 mentioned this issue on Aug 25, 2021



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

Closed

3 tasks

Shadowblad3 changed the title ~~Segmentation fault caused by double free using mp4box in gf_free, alloc.c:165~~ Segmentation fault caused by double free using mp4box in `iloc_entry_del`, `box_code_meta.c:242` on Aug 25, 2021

 **jeanlf** closed this as completed in [b83c9f2](#) on Aug 30, 2021

  **jeanlf** mentioned this issue on Aug 30, 2021

Segmentation fault caused by use after free using mp4box in gf_list_count, list.c:642 #1896

 Closed

 3 tasks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

