New issue

Jump to bottom

Segmentation fault caused by double free using mp4box in av1dmx_finalize, reframe_av1.c:1075 #1893

Closed 3 tasks done **5hadowblad3** opened this issue on Aug 25, 2021 · 2 comments

5hadowblad3 commented on Aug 25, 2021

- [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 in av1dmx_finalize, reframe_av1.c:1075 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: 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  0x00000000013e3d4d in av1dmx_finalize (filter=<optimized out>) at /mnt/data/playground/gpac/src/filters/reframe_av1.c:1075
#7  0x0000000000f9949c in gf_fs_del (fsess=fsess@entry=0x248c220) at /mnt/data/playground/gpac/src/filter_core/filter_session.c:646
#8  0x0000000000c1a86a in gf_media_import (importer=importer@entry=0x7fffffff5bf0) at /mnt/data/playground/gpac/src/media_tools/media_import.c:1242
#9  0x0000000000497345 in convert_file_info (inName=0x7fffffffe159 "tmp", trackID=0x0) at /mnt/data/playground/gpac/applications/mp4box/fileimport.c:128
#10 0x000000000456aaa in mp4boxMain (argc=<optimized out>, argv=<optimized out>) at /mnt/data/playground/gpac/applications/mp4box/main.c:5925
#11 0x0000000001f06bb6 in generic_start_main ()
#12 0x0000000001f071a5 in __libc_start_main ()
#13 0x000000000041c4e9 in _start ()
```

jeanlf closed this as completed in `7bb1b4a` on Aug 30, 2021

5hadowblad3 commented on Aug 31, 2021 Author

This one is not fixed completely. I can still trigger this issue using the commit `d003a57` .

Here is the POC input:
poc.zip
(unzip first)

With command:

```
MP4Box -info POC
```

jeanlf added a commit that referenced this issue on Sep 1, 2021

`further fixes for #1893` `b28f50f`

jeanlf commented on Sep 1, 2021 Contributor

indeed, now fixed thanks for cross-checking!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants