New issue

Jump to bottom

Segmentation fault casued by null pointer dereference using mp4box in mpgviddmx_process, reframe_mpgvid.c:643 #1905

Closed 3 tasks done **5hadowblad3** opened this issue on Sep 1, 2021 · 0 comments

5hadowblad3 commented on Sep 1, 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 caused by null pointer dereference in mpgviddmx_process, reframe_mpgvid.c:643 in commit `d003a57` . It seems to be an incomplete fix of issue #1887 and causes another problem.

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-rev1191-g55d6dbc-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 -info poc
```

POC:
poc.zip
(unzip first)

Here is the trace reported by gdb:

```
Stopped reason: SIGSEGV
gef➤  bt
#0  0x0000000000141a950 in memcpy (__len=0xffffffffffffffff, __src=0x24ada59, __dest=0x24a5770) at /usr/include/x86_64-linux-gnu/bits/string3.h:53
#1  mpgviddmx_process (filter=0x24a0bd0) at /mnt/data/playground/gpac/src/filters/reframe_mpgvid.c:643
#2  0x0000000000fe3e78 in gf_filter_process_task (task=0x2492f30) at /mnt/data/playground/gpac/src/filter_core/filter.c:2441
#3  0x0000000000f7ab69 in gf_fs_thread_proc (sess_thread=sess_thread@entry=0x248c2b0) at /mnt/data/playground/gpac/src/filter_core/filter_session.c:1640
#4  0x0000000000f927b8 in gf_fs_run (fsess=fsess@entry=0x248c220) at /mnt/data/playground/gpac/src/filter_core/filter_session.c:1877
#5  0x0000000000c17c8b in gf_media_import (importer=importer@entry=0x7fffffff5bf0) at /mnt/data/playground/gpac/src/media_tools/media_import.c:1178
#6  0x0000000000497345 in convert_file_info (inName=0x7fffffffe15b "tmp", trackID=0x0) at /mnt/data/playground/gpac/applications/mp4box/fileimport.c:128
#7  0x0000000000456aaa in mp4boxMain (argc=<optimized out>, argv=<optimized out>) at /mnt/data/playground/gpac/applications/mp4box/main.c:5925
#8  0x0000000001f06976 in generic_start_main ()
#9  0x0000000001f06f65 in __libc_start_main ()
#10 0x0000000000041c4e9 in _start ()
```

Here is the trace reported by ASAN:

```
==29762==ERROR: AddressSanitizer: negative-size-param: (size=-1)
     #0 0x7fdaf42ff813  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79813)
     #1 0x7fdaf2897f1c in memcpy /usr/include/x86_64-linux-gnu/bits/string_fortified.h:34
     #2 0x7fdaf2897f1c in mpgviddmx_process /playground/gpac/src/filters/reframe_mpgvid.c:643
     #3 0x7fdaf254efa0 in gf_filter_process_task /playground/gpac/src/filter_core/filter.c:2441
     #4 0x7fdaf250f0e2 in gf_fs_thread_proc /playground/gpac/src/filter_core/filter_session.c:1640
     #5 0x7fdaf2519fb0 in gf_fs_run /playground/gpac/src/filter_core/filter_session.c:1877
     #6 0x7fdaf1ff21f5 in gf_media_import /playground/gpac/src/media_tools/media_import.c:1178
     #7 0x55ce40c3484f in convert_file_info /playground/gpac/applications/mp4box/fileimport.c:128
     #8 0x55ce40c07635 in mp4boxMain /playground/gpac/applications/mp4box/main.c:5925
     #9 0x7fdaef9a6bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
     #10 0x55ce40be83f9 in _start (/playground/gpac/build-a/bin/gcc/MP4Box+0x873f9)

 0x622000007489 is located 0 bytes to the right of 5001-byte region [0x622000006100,0x622000007489)
 allocated by thread T0 here:
     #0 0x7fdaf4364b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
     #1 0x7fdaf26a0289 in filein_initialize /playground/gpac/src/filters/in_file.c:193
     #2 0x7fdaf253b0f0 in gf_filter_new_finalize /playground/gpac/src/filter_core/filter.c:425
     #3 0x7fdaf253f294 in gf_filter_new /playground/gpac/src/filter_core/filter.c:382
     #4 0x7fdaf2519310 in gf_fs_load_source_dest_internal /playground/gpac/src/filter_core/filter_session.c:2833
     #5 0x7fdaf2524a82 in gf_fs_load_source /playground/gpac/src/filter_core/filter_session.c:2873
     #6 0x7fdaf1ff21a6 in gf_media_import /playground/gpac/src/media_tools/media_import.c:1165
     #7 0x55ce40c3484f in convert_file_info /playground/gpac/applications/mp4box/fileimport.c:128
     #8 0x55ce40c07635 in mp4boxMain /playground/gpac/applications/mp4box/main.c:5925
     #9 0x7fdaef9a6bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)

 SUMMARY: AddressSanitizer: negative-size-param (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79813)
 ==29762==ABORTING
```

jeanlf closed this as completed in `5f2c2a1` on Sep 1, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant