[Security]memory leak with MP4Box #1737

Closed 5n1p3r0010 opened this issue on Apr 8, 2021 · 0 comments

5n1p3r0010 commented on Apr 8, 2021

Hi,

There is a memory leak issue with gpac MP4Box,this can reproduce on the lattest commit.

Steps To Reproduce

build:

```
CC=gcc CXX=g++ CFLAGS="-fsanitize=address" CXXFLAGS="-fsanitize=address" LDFLAGS="-fsanitize=address" ./configure --enable-debug
make
```

run as:

```
MP4Box -hint <poc> -out /dev/null
```

shows the following log:

```
=================================================================
==2125589==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 112 byte(s) in 1 object(s) allocated from:
    #0 0x7f8622e8abc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f8622464d02 in gf_malloc utils/alloc.c:150
    #2 0x7f86226d64e6 in gf_odf_new_esd odf/odf_code.c:126
    #3 0x7f86226cfe4d in gf_odf_create_descriptor odf/desc_private.c:42
    #4 0x7f86226d0bee in gf_odf_parse_descriptor odf/descriptors.c:88
    #5 0x7f86226db3ef in gf_odf_desc_read odf/odf_codec.c:301
    #6 0x7f86226db647 in gf_odf_desc_copy odf/odf_codec.c:389
    #7 0x7f862269a405 in Media_GetESD isomedia/media.c:411
    #8 0x7f86226baeba in GetESD isomedia/track.c:87
    #9 0x7f8622670961 in gf_isom_get_esd isomedia/isom_read.c:1298
    #10 0x7f862279ef3b in gf_hinter_track_new media_tools/isom_hinter.c:294
    #11 0x5563ffefecd3 in HintFile /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:3402
    #12 0x5563fff09e18 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6186
    #13 0x5563fff0a5e9 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6312
    #14 0x7f86221eb0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

Indirect leak of 64 byte(s) in 1 object(s) allocated from:
    #0 0x7f8622e8abc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f8622464d02 in gf_malloc utils/alloc.c:150
    #2 0x7f86226dd551 in gf_odf_new_slc odf/slc.c:34
    #3 0x7f86226cfe6b in gf_odf_create_descriptor odf/desc_private.c:47
    #4 0x7f86226d0bee in gf_odf_parse_descriptor odf/descriptors.c:88
    #5 0x7f86226d69a7 in gf_odf_read_esd odf/odf_code.c:275
    #6 0x7f86226d0260 in gf_odf_read_descriptor odf/desc_private.c:282
    #7 0x7f86226d0c98 in gf_odf_parse_descriptor odf/descriptors.c:109
    #8 0x7f86226db3ef in gf_odf_desc_read odf/odf_codec.c:301
    #9 0x7f86226db647 in gf_odf_desc_copy odf/odf_codec.c:389
    #10 0x7f862269a405 in Media_GetESD isomedia/media.c:411
    #11 0x7f86226baeba in GetESD isomedia/track.c:87
    #12 0x7f8622670961 in gf_isom_get_esd isomedia/isom_read.c:1298
    #13 0x7f862279ef3b in gf_hinter_track_new media_tools/isom_hinter.c:294
    #14 0x5563ffefecd3 in HintFile /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:3402
    #15 0x5563fff09e18 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6186
    #16 0x5563fff0a5e9 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6312
    #17 0x7f86221eb0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7f8622e8abc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f8622464d02 in gf_malloc utils/alloc.c:150
    #2 0x7f86224597c0 in gf_list_new utils/list.c:601
    #3 0x7f86226d653c in gf_odf_new_esd odf/odf_code.c:131
    #4 0x7f86226cfe4d in gf_odf_create_descriptor odf/desc_private.c:42
    #5 0x7f86226d0bee in gf_odf_parse_descriptor odf/descriptors.c:88
    #6 0x7f86226db3ef in gf_odf_desc_read odf/odf_codec.c:301
    #7 0x7f86226db647 in gf_odf_desc_copy odf/odf_codec.c:389
    #8 0x7f862269a405 in Media_GetESD isomedia/media.c:411
    #9 0x7f86226baeba in GetESD isomedia/track.c:87
    #10 0x7f8622670961 in gf_isom_get_esd isomedia/isom_read.c:1298
    #11 0x7f862279ef3b in gf_hinter_track_new media_tools/isom_hinter.c:294
    #12 0x5563ffefecd3 in HintFile /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:3402
    #13 0x5563fff09e18 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6186
    #14 0x5563fff0a5e9 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6312
    #15 0x7f86221eb0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7f8622e8abc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f8622464d02 in gf_malloc utils/alloc.c:150
    #2 0x7f86224597c0 in gf_list_new utils/list.c:601
    #3 0x7f86226d652a in gf_odf_new_esd odf/odf_code.c:130
    #4 0x7f86226cfe4d in gf_odf_create_descriptor odf/desc_private.c:42
    #5 0x7f86226d0bee in gf_odf_parse_descriptor odf/descriptors.c:88
    #6 0x7f86226db3ef in gf_odf_desc_read odf/odf_codec.c:301
    #7 0x7f86226db647 in gf_odf_desc_copy odf/odf_codec.c:389
    #8 0x7f862269a405 in Media_GetESD isomedia/media.c:411
    #9 0x7f86226baeba in GetESD isomedia/track.c:87
    #10 0x7f8622670961 in gf_isom_get_esd isomedia/isom_read.c:1298
    #11 0x7f862279ef3b in gf_hinter_track_new media_tools/isom_hinter.c:294
    #12 0x5563ffefecd3 in HintFile /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:3402
    #13 0x5563fff09e18 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6186
    #14 0x5563fff0a5e9 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6312
    #15 0x7f86221eb0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7f8622e8abc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f8622464d02 in gf_malloc utils/alloc.c:150
    #2 0x7f86224597c0 in gf_list_new utils/list.c:601
    #3 0x7f86226d6518 in gf_odf_new_esd odf/odf_code.c:129
    #4 0x7f86226cfe4d in gf_odf_create_descriptor odf/desc_private.c:42
    #5 0x7f86226d0bee in gf_odf_parse_descriptor odf/descriptors.c:88
    #6 0x7f86226db3ef in gf_odf_desc_read odf/odf_codec.c:301
    #7 0x7f86226db647 in gf_odf_desc_copy odf/odf_codec.c:389
    #8 0x7f862269a405 in Media_GetESD isomedia/media.c:411
    #9 0x7f86226baeba in GetESD isomedia/track.c:87
    #10 0x7f8622670961 in gf_isom_get_esd isomedia/isom_read.c:1298
    #11 0x7f862279ef3b in gf_hinter_track_new media_tools/isom_hinter.c:294
    #12 0x5563ffefecd3 in HintFile /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:3402
    #13 0x5563fff09e18 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6186
    #14 0x5563fff0a5e9 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6312
    #15 0x7f86221eb0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: 224 byte(s) leaked in 5 allocation(s).
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
memleak.zip

jeanlf closed this as completed in `cd3738d` on Apr 9, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant