gpac / gpac Public

Code Issues 10 Pull requests 2 Wiki Security Insights

New issue Jump to bottom

Memory Leak in gf_list_new utils/list.c:601 #2284

Closed **FDU-Sec** opened this issue on Oct 11 · 0 comments

FDU-Sec commented on Oct 11

Description

Memory Leak in gf_list_new utils/list.c:601

Version

```
$ ./MP4Box -version
MP4Box - GPAC version 2.1-DEV-rev368-gfd054169b-master
(c) 2000-2022 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io

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: --enable-sanitizer
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_IPV6 GPAC_HAS_SOCK_UN GPAC_MINIMAL_ODF
GPAC_HAS_QJS GPAC_HAS_JPEG GPAC_HAS_PNG GPAC_HAS_LINUX_DVB  GPAC_DISABLE_3D
```

Replay

```
git clone https://github.com/gpac/gpac.git
cd gpac
./configure --enable-sanitizer
make -j$(nproc)
./bin/gcc/MP4Box -bt poc
```

POC

https://github.com/FDU-Sec/poc/blob/main/gpac/poc

ASAN

```
[iso file] Box "emsg" (start 0) has 20 extra bytes
[iso file] Read Box type 0000bl (0x0000626C) at position 709 has size 0 but is not at root/file
level. Forbidden, skipping end of parent box !
[iso file] Box "minf" (start 645) has 3344 extra bytes
[iso file] Track with no sample table !
[iso file] Track with no sample description box !
[iso file] Incomplete box mdat - start 4159 size 68
[iso file] Incomplete file while reading for dump - aborting parsing
[iso file] Box "emsg" (start 0) has 20 extra bytes
[iso file] Read Box type 0000bl (0x0000626C) at position 709 has size 0 but is not at root/file
level. Forbidden, skipping end of parent box !
[iso file] Box "minf" (start 645) has 3344 extra bytes
[iso file] Track with no sample table !
[iso file] Track with no sample description box !
[iso file] Incomplete box mdat - start 4159 size 68
[iso file] Incomplete file while reading for dump - aborting parsing
Scene loaded - dumping root scene

=================================================================
==62092==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7f4e18113b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7f4e15492e5d in gf_list_new utils/list.c:601
    #2 0x7f4e159acd1c in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:775
    #3 0x7f4e159af13b in gf_isom_parse_movie_boxes isomedia/isom_intern.c:868
    #4 0x7f4e159af13b in gf_isom_open_file isomedia/isom_intern.c:988
    #5 0x558bdd469254 in mp4box_main /gpac/applications/mp4box/mp4box.c:6175
    #6 0x7f4e134d2c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Direct leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7f4e18113b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7f4e15492e5d in gf_list_new utils/list.c:601
    #2 0x7f4e159acd1c in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:775
    #3 0x7f4e159af13b in gf_isom_parse_movie_boxes isomedia/isom_intern.c:868
    #4 0x7f4e159af13b in gf_isom_open_file isomedia/isom_intern.c:988
    #5 0x558bdd47b106 in dump_isom_scene /gpac/applications/mp4box/filedump.c:166
    #6 0x558bdd4654b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #7 0x7f4e134d2c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 96 byte(s) in 1 object(s) allocated from:
    #0 0x7f4e18113b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7f4e1593720d in emsg_box_new isomedia/box_code_base.c:12515
    #2 0x7f4e15982447 in gf_isom_box_new_ex isomedia/box_funcs.c:1718
    #3 0x7f4e15982447 in gf_isom_box_parse_ex isomedia/box_funcs.c:247
    #4 0x7f4e15983a7c in gf_isom_parse_root_box isomedia/box_funcs.c:38
    #5 0x7f4e159a927c in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:378
    #6 0x7f4e159af13b in gf_isom_parse_movie_boxes isomedia/isom_intern.c:868
    #7 0x7f4e159af13b in gf_isom_open_file isomedia/isom_intern.c:988
    #8 0x558bdd47b106 in dump_isom_scene /gpac/applications/mp4box/filedump.c:166
    #9 0x558bdd4654b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #10 0x7f4e134d2c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
```

```
Indirect leak of 96 byte(s) in 1 object(s) allocated from:
    #0 0x7f4e18113b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7f4e1593720d in emsg_box_new isomedia/box_code_base.c:12515
    #2 0x7f4e15982447 in gf_isom_box_new_ex isomedia/box_funcs.c:1718
    #3 0x7f4e15982447 in gf_isom_box_parse_ex isomedia/box_funcs.c:247
    #4 0x7f4e15983a7c in gf_isom_parse_root_box isomedia/box_funcs.c:38
    #5 0x7f4e159a927c in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:378
    #6 0x7f4e159af13b in gf_isom_parse_movie_boxes isomedia/isom_intern.c:868
    #7 0x7f4e159af13b in gf_isom_open_file isomedia/isom_intern.c:988
    #8 0x558bdd469254 in mp4box_main /gpac/applications/mp4box/mp4box.c:6175
    #9 0x7f4e134d2c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 80 byte(s) in 1 object(s) allocated from:
    #0 0x7f4e18113f30 in realloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdef30)
    #1 0x7f4e1549307e in realloc_chain utils/list.c:621
    #2 0x7f4e1549307e in gf_list_add utils/list.c:630
    #3 0x7f4e159aa6d0 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:776
    #4 0x7f4e159af13b in gf_isom_parse_movie_boxes isomedia/isom_intern.c:868
    #5 0x7f4e159af13b in gf_isom_open_file isomedia/isom_intern.c:988
    #6 0x558bdd47b106 in dump_isom_scene /gpac/applications/mp4box/filedump.c:166
    #7 0x558bdd4654b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #8 0x7f4e134d2c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 80 byte(s) in 1 object(s) allocated from:
    #0 0x7f4e18113f30 in realloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdef30)
    #1 0x7f4e1549307e in realloc_chain utils/list.c:621
    #2 0x7f4e1549307e in gf_list_add utils/list.c:630
    #3 0x7f4e159aa6d0 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:776
    #4 0x7f4e159af13b in gf_isom_parse_movie_boxes isomedia/isom_intern.c:868
    #5 0x7f4e159af13b in gf_isom_open_file isomedia/isom_intern.c:988
    #6 0x558bdd469254 in mp4box_main /gpac/applications/mp4box/mp4box.c:6175
    #7 0x7f4e134d2c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

SUMMARY: AddressSanitizer: 384 byte(s) leaked in 6 allocation(s).
```

Environment

```
Ubuntu 18.04.5 LTS
Clang 10.0.1
gcc 7.5.0
```

Credit

Peng Deng (Fudan University)

jeanlf closed this as completed in 4520e38 on Oct 11

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant