New issue

Jump to bottom

Memory Leak in gf_odf_new_iod odf/odf_code.c:415 #2285

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

FDU-Sec commented on Oct 11

Description

Memory Leak in gf_odf_new_iod odf/odf_code.c:415

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 -xmt poc1.xmt
```

POC

https://github.com/FDU-Sec/poc/blob/main/gpac/poc1.xmt

ASAN

```
XMT: MPEG-4 (XMT) Scene Parsing
[XMT Parsing] Invalid XML document: Invalid character '<' - Line 13: </decSpeci (line 13)
Error loading scene: Corrupted Data in file/stream

        Error: Corrupted Data in file/stream

=================================================================
==40452==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 80 byte(s) in 1 object(s) allocated from:
    #0 0x7fab5407ab40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fab51a63192 in gf_odf_new_iod odf/odf_code.c:415
    #2 0x7fab51a6c843 in gf_odf_desc_new odf/odf_codec.c:244
    #3 0x7fab51d0244f in xmt_parse_descriptor scene_manager/loader_xmt.c:1942
    #4 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
    #5 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
    #6 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
    #7 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #8 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #9 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #10 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #11 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #12 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #13 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #14 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #15 0x7fab4f439c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 112 byte(s) in 1 object(s) allocated from:
    #0 0x7fab5407ab40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fab51a614d2 in gf_odf_new_esd odf/odf_code.c:126
    #2 0x7fab51a6c843 in gf_odf_desc_new odf/odf_codec.c:244
    #3 0x7fab51d0244f in xmt_parse_descriptor scene_manager/loader_xmt.c:1942
    #4 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
    #5 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
    #6 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
    #7 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #8 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #9 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #10 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #11 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #12 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #13 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #14 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #15 0x7fab4f439c86 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 0x7fab5407af30 in realloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdef30)
    #1 0x7fab513fa07e in realloc_chain utils/list.c:621
    #2 0x7fab513fa07e in gf_list_add utils/list.c:630
    #3 0x7fab51d028ce in xmt_parse_descriptor scene_manager/loader_xmt.c:1987
    #4 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
    #5 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
    #6 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
```

```
    #7 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #8 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #9 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #10 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #11 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #12 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #13 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #14 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #15 0x7fab4f439c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 64 byte(s) in 1 object(s) allocated from:
    #0 0x7fab5407ab40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fab51a68722 in gf_odf_new_dcd odf/odf_code.c:1107
    #2 0x7fab51a6c843 in gf_odf_desc_new odf/odf_codec.c:244
    #3 0x7fab51d0244f in xmt_parse_descriptor scene_manager/loader_xmt.c:1942
    #4 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
    #5 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
    #6 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
    #7 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #8 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #9 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #10 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #11 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #12 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #13 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #14 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #15 0x7fab4f439c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7fab5407ab40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fab513f9e5d in gf_list_new utils/list.c:601
    #2 0x7fab51a6151c in gf_odf_new_esd odf/odf_code.c:130
    #3 0x7fab51a6c843 in gf_odf_desc_new odf/odf_codec.c:244
    #4 0x7fab51d0244f in xmt_parse_descriptor scene_manager/loader_xmt.c:1942
    #5 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
    #6 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
    #7 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
    #8 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #9 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #10 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #11 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #12 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #13 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #14 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #15 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #16 0x7fab4f439c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7fab5407ab40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fab513f9e5d in gf_list_new utils/list.c:601
    #2 0x7fab51a6153b in gf_odf_new_esd odf/odf_code.c:131
    #3 0x7fab51a6c843 in gf_odf_desc_new odf/odf_codec.c:244
    #4 0x7fab51d0244f in xmt_parse_descriptor scene_manager/loader_xmt.c:1942
    #5 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
    #6 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
    #7 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
```

```
    #8 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #9 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #10 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #11 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #12 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #13 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #14 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #15 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #16 0x7fab4f439c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7fab5407ab40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fab513f9e5d in gf_list_new utils/list.c:601
    #2 0x7fab51a631ff in gf_odf_new_iod odf/odf_code.c:421
    #3 0x7fab51a6c843 in gf_odf_desc_new odf/odf_codec.c:244
    #4 0x7fab51d0244f in xmt_parse_descriptor scene_manager/loader_xmt.c:1942
    #5 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
    #6 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
    #7 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
    #8 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #9 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #10 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #11 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #12 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #13 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #14 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #15 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #16 0x7fab4f439c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7fab5407ab40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fab513f9e5d in gf_list_new utils/list.c:601
    #2 0x7fab51a614f4 in gf_odf_new_esd odf/odf_code.c:129
    #3 0x7fab51a6c843 in gf_odf_desc_new odf/odf_codec.c:244
    #4 0x7fab51d0244f in xmt_parse_descriptor scene_manager/loader_xmt.c:1942
    #5 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
    #6 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
    #7 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
    #8 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #9 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #10 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #11 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #12 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #13 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #14 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #15 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #16 0x7fab4f439c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7fab5407ab40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fab513f9e5d in gf_list_new utils/list.c:601
    #2 0x7fab51a68740 in gf_odf_new_dcd odf/odf_code.c:1110
    #3 0x7fab51a6c843 in gf_odf_desc_new odf/odf_codec.c:244
    #4 0x7fab51d0244f in xmt_parse_descriptor scene_manager/loader_xmt.c:1942
    #5 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
    #6 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
```

```
    #7 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
    #8 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #9 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #10 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #11 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #12 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #13 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #14 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #15 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #16 0x7fab4f439c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7fab5407ab40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fab513f9e5d in gf_list_new utils/list.c:601
    #2 0x7fab51a6321e in gf_odf_new_iod odf/odf_code.c:423
    #3 0x7fab51a6c843 in gf_odf_desc_new odf/odf_codec.c:244
    #4 0x7fab51d0244f in xmt_parse_descriptor scene_manager/loader_xmt.c:1942
    #5 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
    #6 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
    #7 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
    #8 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #9 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #10 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #11 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #12 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #13 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #14 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #15 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #16 0x7fab4f439c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7fab5407ab40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fab513f9e5d in gf_list_new utils/list.c:601
    #2 0x7fab51a631e0 in gf_odf_new_iod odf/odf_code.c:420
    #3 0x7fab51a6c843 in gf_odf_desc_new odf/odf_codec.c:244
    #4 0x7fab51d0244f in xmt_parse_descriptor scene_manager/loader_xmt.c:1942
    #5 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
    #6 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
    #7 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
    #8 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #9 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #10 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #11 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #12 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #13 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #14 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #15 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #16 0x7fab4f439c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

Indirect leak of 16 byte(s) in 1 object(s) allocated from:
    #0 0x7fab5407ab40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fab513f9e5d in gf_list_new utils/list.c:601
    #2 0x7fab51a631b4 in gf_odf_new_iod odf/odf_code.c:419
    #3 0x7fab51a6c843 in gf_odf_desc_new odf/odf_codec.c:244
    #4 0x7fab51d0244f in xmt_parse_descriptor scene_manager/loader_xmt.c:1942
    #5 0x7fab51d0553d in xmt_node_start scene_manager/loader_xmt.c:2571
```

```
    #6 0x7fab51436f35 in xml_sax_node_start utils/xml_parser.c:304
    #7 0x7fab5143a20f in xml_sax_parse_attribute utils/xml_parser.c:393
    #8 0x7fab5143a20f in xml_sax_parse utils/xml_parser.c:911
    #9 0x7fab5143bdfd in gf_xml_sax_parse_intern utils/xml_parser.c:1072
    #10 0x7fab5143c6b7 in gf_xml_sax_parse utils/xml_parser.c:1100
    #11 0x7fab5143c9c8 in xml_sax_read_file utils/xml_parser.c:1187
    #12 0x7fab5143d5c4 in gf_xml_sax_parse_file utils/xml_parser.c:1299
    #13 0x7fab51cf010a in load_xmt_run scene_manager/loader_xmt.c:3134
    #14 0x564329084177 in dump_isom_scene /gpac/applications/mp4box/filedump.c:207
    #15 0x56432906e4b4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6336
    #16 0x7fab4f439c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

SUMMARY: AddressSanitizer: 464 byte(s) leaked in 12 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 `d82e134` on Oct 11

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant