New issue

Jump to bottom

Heap use after free in Q_IsTypeOn at gpac/src/bifs/unquantize.c #2315

Closed **Mist1987** opened this issue 19 days ago · 0 comments

Mist1987 commented 19 days ago

Description

Heap use after free in Q_IsTypeOn at gpac/src/bifs/unquantize.c:175:12

System info

Ubuntu 20.04 lts

Version info

```
MP4Box - GPAC version 2.1-DEV-rev478-g696e6f868-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 --enable-debug
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_IPV6 GPAC_HAS_SSL GPAC_HAS_SOCK_UN GPAC_MINIMAL_ODF GPAC_HAS_QJS GPAC_HAS_FAAD GPAC_HAS_MAD GPAC_HAS_LIBA52 GPAC_HAS_JPEG GPAC_HAS_PN
```

compile

```
./configure --enable-sanitizer --enable-debug
make
```

crash command

```
MP4Box -bt poc
```

POC

POC-uaf

Crash output

```
/home/zw/AFL_Fuzz_Datas/gpac/bin/gcc/MP4Box -bt poc

[iso file] Unknown box type vref in parent dinf
[iso file] Missing dref box in dinf
[iso file] Unknown box type vref in parent dinf
[iso file] Missing dref box in dinf
MPEG-4 BIFS Scene Parsing
=================================================================
==1578219==ERROR: AddressSanitizer: heap-use-after-free on address 0x610000001ad4 at pc 0x7f8194636c1d bp 0x7fff91f55420 sp 0x7fff91f55418
READ of size 4 at 0x610000001ad4 thread T0
    #0 0x7f8194636c1c in Q_IsTypeOn /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/unquantize.c:175:12
    #1 0x7f8194643390 in gf_bifs_dec_unquant_field /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/unquantize.c:398:7
    #2 0x7f81945890e1 in gf_bifs_dec_sf_field /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/field_decode.c:84:7
    #3 0x7f8194597e3f in BD_DecMFFieldList /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/field_decode.c:327:8
    #4 0x7f819459cd2f in gf_bifs_dec_field /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/field_decode.c:564:9
    #5 0x7f819459df3a in gf_bifs_dec_node_list /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/field_decode.c:626:7
    #6 0x7f81945965a8 in gf_bifs_dec_node /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/field_decode.c:928:7
    #7 0x7f8194598014 in BD_DecMFFieldList /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/field_decode.c:330:15
    #8 0x7f819459cd2f in gf_bifs_dec_field /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/field_decode.c:564:9
    #9 0x7f81945c0e7b in BM_ParseFieldReplace /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:734:21
    #10 0x7f81945c4923 in BM_ParseReplace /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:847:10
    #11 0x7f81945c7f12 in BM_ParseCommand /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:915:8
    #12 0x7f81945c9706 in gf_bifs_flush_command_list /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:964:9
    #13 0x7f81945cc012 in gf_bifs_decode_command_list /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:1044:3
    #14 0x7f8195bc921f in gf_sm_load_run_isom /home/zw/AFL_Fuzz_Datas/gpac/src/scene_manager/loader_isom.c:303:10
    #15 0x7f8195a86732 in gf_sm_load_run /home/zw/AFL_Fuzz_Datas/gpac/src/scene_manager/scene_manager.c:719:28
    #16 0x577f50 in dump_isom_scene /home/zw/AFL_Fuzz_Datas/gpac/applications/mp4box/filedump.c:207:14
    #17 0x53949f in mp4box_main /home/zw/AFL_Fuzz_Datas/gpac/applications/mp4box/mp4box.c:6369:7
    #18 0x549801 in main /home/zw/AFL_Fuzz_Datas/gpac/applications/mp4box/mp4box.c:6834:1
    #19 0x7f8192985082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-start.c:308:16
    #20 0x42ac5d in _start (/home/zw/AFL_Fuzz_Datas/gpac/bin/gcc/MP4Box+0x42ac5d)

0x610000001ad4 is located 148 bytes inside of 192-byte region [0x610000001a40,0x610000001b00)
freed by thread T0 here:
    #0 0x4a5c52 in free (/home/zw/AFL_Fuzz_Datas/gpac/bin/gcc/MP4Box+0x4a5c52)
```

```
    #1 0x7f8193259324 in gf_free /home/zw/AFL_Fuzz_Datas/gpac/src/utils/alloc.c:165:2
    #2 0x7f819378d74a in gf_node_free /home/zw/AFL_Fuzz_Datas/gpac/src/scenegraph/base_scenegraph.c:1622:2
    #3 0x7f81938a38fc in QuantizationParameter_Del /home/zw/AFL_Fuzz_Datas/gpac/src/scenegraph/mpeg4_nodes.c:11981:2
    #4 0x7f81938962b1 in gf_sg_mpeg4_node_del /home/zw/AFL_Fuzz_Datas/gpac/src/scenegraph/mpeg4_nodes.c:37743:3
    #5 0x7f8193774108 in gf_node_del /home/zw/AFL_Fuzz_Datas/gpac/src/scenegraph/base_scenegraph.c:1904:59
    #6 0x7f8193763dc2 in gf_node_unregister /home/zw/AFL_Fuzz_Datas/gpac/src/scenegraph/base_scenegraph.c:763:3
    #7 0x7f8193772a1c in gf_node_try_destroy /home/zw/AFL_Fuzz_Datas/gpac/src/scenegraph/base_scenegraph.c:669:9
    #8 0x7f81937ce9cc in gf_sg_command_del /home/zw/AFL_Fuzz_Datas/gpac/src/scenegraph/commands.c:72:7
    #9 0x7f81945ca742 in gf_bifs_flush_command_list /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:990:5
    #10 0x7f81945cc012 in gf_bifs_decode_command_list /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:1044:3
    #11 0x7f8195bc921f in gf_sm_load_run_isom /home/zw/AFL_Fuzz_Datas/gpac/src/scene_manager/loader_isom.c:303:10
    #12 0x7f8195a86732 in gf_sm_load_run /home/zw/AFL_Fuzz_Datas/gpac/src/scene_manager/scene_manager.c:719:28
    #13 0x577f50 in dump_isom_scene /home/zw/AFL_Fuzz_Datas/gpac/applications/mp4box/filedump.c:207:14
    #14 0x53949f in mp4box_main /home/zw/AFL_Fuzz_Datas/gpac/applications/mp4box/mp4box.c:6369:7
    #15 0x549801 in main /home/zw/AFL_Fuzz_Datas/gpac/applications/mp4box/mp4box.c:6834:1
    #16 0x7f8192985082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-start.c:308:16

previously allocated by thread T0 here:
    #0 0x4a5ebd in malloc (/home/zw/AFL_Fuzz_Datas/gpac/bin/gcc/MP4Box+0x4a5ebd)
    #1 0x7f8193259214 in gf_malloc /home/zw/AFL_Fuzz_Datas/gpac/src/utils/alloc.c:150:9
    #2 0x7f819381fc84 in QuantizationParameter_Create /home/zw/AFL_Fuzz_Datas/gpac/src/scenegraph/mpeg4_nodes.c:12496:2
    #3 0x7f819388ffa6 in gf_sg_mpeg4_node_new /home/zw/AFL_Fuzz_Datas/gpac/src/scenegraph/mpeg4_nodes.c:36871:10
    #4 0x7f8193796799 in gf_node_new /home/zw/AFL_Fuzz_Datas/gpac/src/scenegraph/base_scenegraph.c:1996:51
    #5 0x7f8194595f4a in gf_bifs_dec_node /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/field_decode.c:900:15
    #6 0x7f8194598014 in BD_DecMFFieldList /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/field_decode.c:330:15
    #7 0x7f819459cd2f in gf_bifs_dec_field /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/field_decode.c:564:9
    #8 0x7f81945c0e7b in BM_ParseFieldReplace /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:734:21
    #9 0x7f81945c4923 in BM_ParseReplace /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:847:10
    #10 0x7f81945c7f12 in BM_ParseCommand /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:915:8
    #11 0x7f81945c9706 in gf_bifs_flush_command_list /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:964:9
    #12 0x7f81945cc012 in gf_bifs_decode_command_list /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/memory_decoder.c:1044:3
    #13 0x7f8195bc921f in gf_sm_load_run_isom /home/zw/AFL_Fuzz_Datas/gpac/src/scene_manager/loader_isom.c:303:10
    #14 0x7f8195a86732 in gf_sm_load_run /home/zw/AFL_Fuzz_Datas/gpac/src/scene_manager/scene_manager.c:719:28
    #15 0x577f50 in dump_isom_scene /home/zw/AFL_Fuzz_Datas/gpac/applications/mp4box/filedump.c:207:14
    #16 0x53949f in mp4box_main /home/zw/AFL_Fuzz_Datas/gpac/applications/mp4box/mp4box.c:6369:7
    #17 0x549801 in main /home/zw/AFL_Fuzz_Datas/gpac/applications/mp4box/mp4box.c:6834:1
    #18 0x7f8192985082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-start.c:308:16

SUMMARY: AddressSanitizer: heap-use-after-free /home/zw/AFL_Fuzz_Datas/gpac/src/bifs/unquantize.c:175:12 in Q_IsTypeOn
Shadow bytes around the buggy address:
  0x0c207fff8300: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fff8310: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c207fff8320: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fff8330: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c207fff8340: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c207fff8350: fd fd fd fd fd fd fd fd fd[fd]fd fd fd fd fd
  0x0c207fff8360: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c207fff8370: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa
  0x0c207fff8380: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8390: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff83a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==1578219==ABORTING
```

Occurrences:

gpac/src/bifs/unquantize.c:175:12 in Q_IsTypeOn

Impact

can cause a program to crash, use unexpected values, or execute code.

Report of the Information Security Laboratory of Ocean University of China @OUC_ISLOUC @OUC_Blue_Whale

jeanlf closed this as completed in `1016912` 19 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Development

No branches or pull requests

1 participant