gpac / gpac Public

Code Issues 11 Pull requests 2 Wiki Security Insights

New issue

Jump to bottom

There is a use-after-free detected by AddressSanitizer #2109

Closed AAArdu opened this issue on Feb 7 · 0 comments

AAArdu commented on Feb 7

Description

There is a use-after-free detected by AddressSanitizer

System info

```
Ubuntu 20.04.2 LTS
clang version 12.0.0-++20210402082642+04ba60cfe598-1~exp1~20210402063359.71
MP4Box - GPAC version 1.1.0-DEV-rev1727-g8be34973d-master
```

Build command

```
./configure --static-mp4box --prefix=`realpath ./install` --enable-sanitizer --cc=clang --
cxx=clang++
```

crash command

```
MP4Box -lsr -out /dev/null poc_file
```

Pocs

poc.zip

Crash output

```
==28733==ERROR: AddressSanitizer: heap-use-after-free on address 0x603000002bc0 at pc
0x000000721f36 bp 0x7ffec8945940 sp 0x7ffec8945938
READ of size 2 at 0x603000002bc0 thread T0
    #0 0x721f35 in
gf_node_get_attribute_by_tag/programs/mp4box/builds/build10/src/scenegraph/xml_ns.c:934:18
    #1 0x70ca13 in
gf_dom_listener_del/programs/mp4box/builds/build10/src/scenegraph/dom_events.c:161:6
    #2 0x70ccaa in
gf_dom_event_remove_all_listeners/programs/mp4box/builds/build10/src/scenegraph/dom_events.c:196:3
    #3 0x5c54f5 in
gf_node_free/programs/mp4box/builds/build10/src/scenegraph/base_scenegraph.c:1601:4
    #4 0x6dac25 in gf_svg_node_del/programs/mp4box/builds/build10/src/scenegraph/svg_types.c:126:2
    #5 0x5bf0f1 in
gf_node_unregister/programs/mp4box/builds/build10/src/scenegraph/base_scenegraph.c:761:3
    #6 0x5bfb17 in
gf_sg_reset/programs/mp4box/builds/build10/src/scenegraph/base_scenegraph.c:479:3
    #7 0x5be86d in gf_sg_del/programs/mp4box/builds/build10/src/scenegraph/base_scenegraph.c:162:2
    #8 0x4eba5d in
dump_isom_scene/programs/mp4box/builds/build10/applications/mp4box/filedump.c:221:2
    #9 0x4e0bda in mp4boxMain/programs/mp4box/builds/build10/applications/mp4box/main.c:6146:7
    #10 0x7f9d3ecb80b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #11 0x41ea6d in _start (/zhengjie/cmdline-
fuzz/programs/mp4box/builds/build10/bin/gcc/MP4Box+0x41ea6d)

0x603000002bc0 is located 0 bytes inside of 24-byte region [0x603000002bc0,0x603000002bd8)
freed by thread T0 here:
    #0 0x499a62 in free (/zhengjie/cmdline-
fuzz/programs/mp4box/builds/build10/bin/gcc/MP4Box+0x499a62)
    #1 0x7215a7 in
gf_node_delete_attributes/programs/mp4box/builds/build10/src/scenegraph/xml_ns.c:728:3
    #2 0x6dac15 in gf_svg_node_del/programs/mp4box/builds/build10/src/scenegraph/svg_types.c:124:2
    #3 0x5bf0f1 in
gf_node_unregister/programs/mp4box/builds/build10/src/scenegraph/base_scenegraph.c:761:3
    #4 0x5bfb17 in
gf_sg_reset/programs/mp4box/builds/build10/src/scenegraph/base_scenegraph.c:479:3
    #5 0x5be86d in gf_sg_del/programs/mp4box/builds/build10/src/scenegraph/base_scenegraph.c:162:2
    #6 0x4eba5d in
dump_isom_scene/programs/mp4box/builds/build10/applications/mp4box/filedump.c:221:2
    #7 0x4e0bda in mp4boxMain/programs/mp4box/builds/build10/applications/mp4box/main.c:6146:7
    #8 0x7f9d3ecb80b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

previously allocated by thread T0 here:
    #0 0x499ccd in malloc (/zhengjie/cmdline-
fuzz/programs/mp4box/builds/build10/bin/gcc/MP4Box+0x499ccd)
    #1 0x72217c in
gf_node_create_attribute_from_datatype/programs/mp4box/builds/build10/src/scenegraph/xml_ns.c:737:2

    #2 0x72217c in
gf_xml_create_attribute/programs/mp4box/builds/build10/src/scenegraph/xml_ns.c:541:9
    #3 0x72217c in
gf_node_get_attribute_by_tag/programs/mp4box/builds/build10/src/scenegraph/xml_ns.c:946:9
    #4 0xaf1c3f in lsr_read_rare_full/programs/mp4box/builds/build10/src/laser/lsr_dec.c:1446:21
    #5 0xaf01c7 in lsr_read_listener/programs/mp4box/builds/build10/src/laser/lsr_dec.c:4355:2
    #6 0xb00747 in
lsr_read_scene_content_model/programs/mp4box/builds/build10/src/laser/lsr_dec.c:4600:7
    #7 0xaff8a0 in
lsr_read_group_content/programs/mp4box/builds/build10/src/laser/lsr_dec.c:4785:8
    #8 0xaeb4d9 in lsr_read_rectClip/programs/mp4box/builds/build10/src/laser/lsr_dec.c:3987:2
    #9 0xb00752 in
lsr_read_scene_content_model/programs/mp4box/builds/build10/src/laser/lsr_dec.c:4519:7
    #10 0xaff8a0 in
lsr_read_group_content/programs/mp4box/builds/build10/src/laser/lsr_dec.c:4785:8
    #11 0xae55a4 in lsr_read_svg/programs/mp4box/builds/build10/src/laser/lsr_dec.c:4192:2
    #12 0xadf7ae in
lsr_read_command_list/programs/mp4box/builds/build10/src/laser/lsr_dec.c:5886:9
    #13 0xaddbfb in
lsr_decode_laser_unit/programs/mp4box/builds/build10/src/laser/lsr_dec.c:6133:6
    #14 0xade67f in
gf_laser_decode_command_list/programs/mp4box/builds/build10/src/laser/lsr_dec.c:230:6
    #15 0xa356af in
gf_sm_load_run_isom/programs/mp4box/builds/build10/src/scene_manager/loader_isom.c:307:10
    #16 0x4eb9a1 in
dump_isom_scene/programs/mp4box/builds/build10/applications/mp4box/filedump.c:203:14
    #17 0x4e0bda in mp4boxMain/programs/mp4box/builds/build10/applications/mp4box/main.c:6146:7
    #18 0x7f9d3ecb80b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: heap-use-after-
free/programs/mp4box/builds/build10/src/scenegraph/xml_ns.c:934:18 in gf_node_get_attribute_by_tag
Shadow bytes around the buggy address:
  0x0c067fff8520: fd fa fa fa fd fd fd fa fa fa fd fd fd fa fa fa
  0x0c067fff8530: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd fa
  0x0c067fff8540: fa fa fd fd fd fa fa fa fd fd fd fa fa fd fd
  0x0c067fff8550: fd fa fa fa fd fd fd fa fa fa fd fd fd fd fa fa
  0x0c067fff8560: fd fd fd fa fa fa fd fd fd fa fa fa 00 00 00 fa
=>0x0c067fff8570: fa fa fd fd fd fd fa fa[fd]fd fd fa fa fa fd fd
  0x0c067fff8580: fd fd fa fa fd fd fd fa fa fa fd fd fd fa fa fa
  0x0c067fff8590: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd fa
  0x0c067fff85a0: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
  0x0c067fff85b0: fd fa fa fa fd fd fd fa fa fa fd fd fd fa fa fa
  0x0c067fff85c0: fd fd fd fa fa fa fd fd fd fd fa fa fd fd fd 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
==28733==ABORTING
```

jeanlf closed this as completed in 9723dd0 on Feb 8

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant