

New issue

[Jump to bottom](#)

3 UAF bugs in box_funcs.c #1440

Closed

3 tasks done

strongcourage opened this issue on Mar 24, 2020 · 4 comments

strongcourage commented on Mar 24, 2020

Thanks for reporting your issue. Please make sure these boxes are checked before submitting your issue - thank you!

- ☒ I looked for a similar issue and couldn't find any.
- ☒ I tried with the latest version of GPAC. Installers available at <http://gpac.io/downloads/gpac-nightly-builds/>
- ☒ I give enough information for contributors to reproduce my issue (meaningful title, github labels, platform and compiler, command-line ...). I can share files anonymously with this dropbox: https://www.mediafire.com/filedrop/filedrop_hosted.php?drop=eec9e058a9486fe4e99c33021481d9e1826ca9dbc242a6cfaab0fe95da5e5d95

Detailed guidelines: <http://gpac.io/2013/07/16/how-to-file-a-bug-properly/>

Hi GPAC Team,

I found 3 new UAF bugs on the latest commit [56eaea8](#) of GPAC version 0.8.0.

I think it is probably due to an **incomplete fix** of the UAF bug [#1340](#). Actually, these new bugs share the same buggy function which is `gf_isom_box_del()` in `src/isomedia/box_funcs.c` with [#1340](#), but have different alloc function `esds_New()` in `src/isomedia/box_code_base.c` (instead of `stco_New()`).

Command: `MP4Box -info $POC` or `MP4Box -diso $POC`

1) UAF Bug 1

PoC: https://github.com/strongcourage/PoCs/blob/master/gpac_56eaea8/uaf1

ASAN says:

```
=====
==31565==ERROR: AddressSanitizer: heap-use-after-free on address 0x60400000dde8 at pc 0x0000006c601e bp 0x7fff726c3b70 sp 0x7fff726c3b60
READ of size 8 at 0x60400000dde8 thread T0
#0 0x6c601d in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1504
#1 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#2 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#3 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#4 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#5 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#6 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#7 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#8 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#9 0x6c72cd in gf_isom_box_array_read_ex /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1427
#10 0xae0b0f in mdia_Read /home/dungnguyen/fuzz/gpac/src/isomedia/box_code_base.c:3021
#11 0x6c6456 in gf_isom_box_read /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1532
#12 0x6c6456 in gf_isom_box_parse_ex /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:210
#13 0x6c6e02 in gf_isom_box_array_read_ex /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1425
#14 0xaeffe8 in trak_Read /home/dungnguyen/fuzz/gpac/src/isomedia/box_code_base.c:7188
#15 0x6c6456 in gf_isom_box_read /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1532
#16 0x6c6456 in gf_isom_box_parse_ex /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:210
#17 0x6c6e02 in gf_isom_box_array_read_ex /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1425
#18 0xae3444 in moov_Read /home/dungnguyen/fuzz/gpac/src/isomedia/box_code_base.c:3749
#19 0x6c7764 in gf_isom_box_read /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1532
#20 0x6c7764 in gf_isom_box_parse_ex /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:210
#21 0x6c7f04 in gf_isom_parse_root_box /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:42
#22 0x6dd940 in gf_isom_parse_movie_boxes /home/dungnguyen/fuzz/gpac/src/isomedia/isom_intern.c:207
#23 0x6e05d3 in gf_isom_parse_movie_boxes /home/dungnguyen/fuzz/gpac/src/isomedia/isom_intern.c:195
#24 0x6e05d3 in gf_isom_open_file /home/dungnguyen/fuzz/gpac/src/isomedia/isom_intern.c:616
#25 0x43375d in mp4boxMain /home/dungnguyen/fuzz/gpac/applications/mp4box/main.c:4814
#26 0x7fca8b7382f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#27 0x41e4f8 in _start (/home/dungnguyen/PoCs/gpac_new/MP4Box+0x41e4f8)

0x60400000dde8 is located 24 bytes inside of 48-byte region [0x60400000ddd0,0x60400000de00)
freed by thread T0 here:
#0 0x7fca8c61732a in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x9832a)
#1 0x6c5f9f in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1512

previously allocated by thread T0 here:
#0 0x7fca8c617662 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98662)
#1 0xad6b8d in esds_New /home/dungnguyen/fuzz/gpac/src/isomedia/box_code_base.c:1287

SUMMARY: AddressSanitizer: heap-use-after-free /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1504 gf_isom_box_del
```

strongcourage commented on Mar 24, 2020

Author

2) UAF Bug 2

PoC: https://github.com/strongcourage/PoCs/blob/master/gpac_56eaea8/uaf2

ASAN says:

```
=====
==13425==ERROR: AddressSanitizer: heap-use-after-free on address 0x60400000dde8 at pc 0x0000006c601e bp 0x7ffec486f2b0 sp 0x7ffec486f2a0
READ of size 8 at 0x60400000dde8 thread T0
#0 0x6c601d in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1504
#1 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#2 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#3 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#4 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#5 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#6 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
```

```
#7 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#8 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#9 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#10 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#11 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#12 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#13 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#14 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#15 0x6c6066 in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#16 0x6e00f8 in gf_isom_delete_movie /home/dungnguyen/fuzz/gpac/src/isomedia/isom_intern.c:658
#17 0x42f981 in mp4BoxMain /home/dungnguyen/fuzz/gpac/applications/mp4box/main.c:5819
#18 0x7f460342e82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#19 0x41e4f8 in _start (/home/dungnguyen/PoCs/gpac_56eaea8/MP4Box+0x41e4f8)

0x6040000dde8 is located 24 bytes inside of 48-byte region [0x6040000ddd0,0x6040000dde0)
freed by thread T0 here:
#0 0x7f46041d232a in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x9832a)
#1 0x6c5f9f in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1512

previously allocated by thread T0 here:
#0 0x7f46041d2662 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98662)
#1 0xadbb68d in esds_New /home/dungnguyen/fuzz/gpac/src/isomedia/box_code_base.c:1287

SUMMARY: AddressSanitizer: heap-use-after-free /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1504 gf_isom_box_del
```

strongcourage commented on Mar 24, 2020

Author

3) UAF Bug 3

PoC: https://github.com/strongcourage/PoCs/blob/master/gpac_56eaea8/uaf3

ASAN says:

```
=====
==27915==ERROR: AddressSanitizer: heap-use-after-free on address 0x6040000dda8 at pc 0x0000006c601e bp 0x7fffc791a180 sp 0x7fffc791a170
READ of size 8 at 0x6040000dda8 thread T0
#0 0x6c601d in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1504
#1 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#2 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#3 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#4 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#5 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#6 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#7 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#8 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#9 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#10 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#11 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#12 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#13 0x6c5f5e in gf_isom_box_array_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:272
#14 0x6c5f5e in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1520
#15 0x6c77ae in gf_isom_box_parse_ex /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:221
#16 0x6c7fb4 in gf_isom_parse_root_box /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:42
#17 0x6d9d40 in gf_isom_parse_movie_boxes /home/dungnguyen/fuzz/gpac/src/isomedia/isom_intern.c:207
#18 0x6e05d3 in gf_isom_parse_movie_boxes /home/dungnguyen/fuzz/gpac/src/isomedia/isom_intern.c:195
#19 0x6e05d3 in gf_isom_open_file /home/dungnguyen/fuzz/gpac/src/isomedia/isom_intern.c:616
#20 0x43375d in mp4BoxMain /home/dungnguyen/fuzz/gpac/applications/mp4box/main.c:4814
#21 0x7efe8551f82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#22 0x41e4f8 in _start (/home/dungnguyen/PoCs/gpac_56eaea8/MP4Box+0x41e4f8)

0x6040000dda8 is located 24 bytes inside of 48-byte region [0x6040000dd90,0x6040000ddc0)
freed by thread T0 here:
#0 0x7efe862c332a in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x9832a)
#1 0x6c5f9f in gf_isom_box_del /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1512

previously allocated by thread T0 here:
#0 0x7efe862c3662 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98662)
#1 0xadbb68d in esds_New /home/dungnguyen/fuzz/gpac/src/isomedia/box_code_base.c:1287

SUMMARY: AddressSanitizer: heap-use-after-free /home/dungnguyen/fuzz/gpac/src/isomedia/box_funcs.c:1504 gf_isom_box_del
```

 aureliendavid added a commit that referenced this issue on Mar 26, 2020

 fix UAF in audio_sample_entry_Read (#1440)

6063b1a

aureliendavid commented on Mar 26, 2020

Contributor

Hi,

This should be fixed by the commit above. You can close the issue if you confirm it fixed.

Thanks for the report.


strongcourage commented on Mar 26, 2020

Author

Hi Aurelien,

Thanks for your patch. I do confirm that those UAF bugs have been fixed completely.

Best.

 strongcourage closed this as completed on Mar 26, 2020

  Clingto mentioned this issue on Dec 15, 2020



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

