

New issue

[Jump to bottom](#)

There is a heap-buffer-overflow in the gf_media_nalu_remove_emulation_bytes function of av_parsers.c:4722 #1339



gutiniao opened this issue on Nov 12, 2019 · 1 comment

gutiniao commented on Nov 12, 2019 • edited

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/>

A crafted input will lead to crash in av_parsers.c at gpac 0.8.0.

Triggered by

./MP4Box -diso POC -out /dev/null

Poc

001gf_media_nalu_remove_emulation_bytes

The ASAN information is as follows:

```
./MP4Box -diso 001gf_media_nalu_remove_emulation_bytes -out /dev/null
[iso file] Media header timescale is 0 - defaulting to 90000
=====
==23148==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000002d1 at pc 0x5632845c98b0 bp 0x7ffdc21c4e0 sp 0x7ffdc21c4d0
READ of size 1 at 0x602000002d1 thread T0
#0 0x5632845c98af in gf_media_nalu_remove_emulation_bytes media_tools/av_parsers.c:4722
#1 0x5632845c991b in gf_media_avc_read_sps media_tools/av_parsers.c:4737
#2 0x5632843ea9a9 in avcc_Read isomedia/avc_ext.c:2371
#3 0x5632844183d4 in gf_isom_box_read isomedia/box_funcs.c:1528
#4 0x5632844183d4 in gf_isom_box_parse_ex isomedia/box_funcs.c:208
#5 0x563284418e10 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1419
#6 0x5632848afb1 in video_sample_entry_Read isomedia/box_code_base.c:4405
#7 0x5632844183d4 in gf_isom_box_read isomedia/box_funcs.c:1528
#8 0x5632844183d4 in gf_isom_box_parse_ex isomedia/box_funcs.c:208
#9 0x563284418e10 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1419
#10 0x5632844183d4 in gf_isom_box_read isomedia/box_funcs.c:1528
#11 0x5632844183d4 in gf_isom_box_parse_ex isomedia/box_funcs.c:208
#12 0x563284418e10 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1419
#13 0x5632848b38a4 in stbl_Read isomedia/box_code_base.c:5381
#14 0x5632844183d4 in gf_isom_box_read isomedia/box_funcs.c:1528
#15 0x5632844183d4 in gf_isom_box_parse_ex isomedia/box_funcs.c:208
#16 0x563284418e10 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1419
#17 0x5632848ad40b in minf_Read isomedia/box_code_base.c:3500
#18 0x5632844183d4 in gf_isom_box_read isomedia/box_funcs.c:1528
#19 0x5632844183d4 in gf_isom_box_parse_ex isomedia/box_funcs.c:208
#20 0x563284418e10 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1419
#21 0x5632848ab73f in mdia_Read isomedia/box_code_base.c:3021
#22 0x5632844183d4 in gf_isom_box_read isomedia/box_funcs.c:1528
#23 0x5632844183d4 in gf_isom_box_parse_ex isomedia/box_funcs.c:208
#24 0x563284418e10 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1419
#25 0x5632848ba906 in trak_Read isomedia/box_code_base.c:7129
#26 0x5632844183d4 in gf_isom_box_read isomedia/box_funcs.c:1528
#27 0x5632844183d4 in gf_isom_box_parse_ex isomedia/box_funcs.c:208
#28 0x563284418e10 in gf_isom_box_array_read_ex isomedia/box_funcs.c:1419
#29 0x5632848adf64 in moov_Read isomedia/box_code_base.c:3745
#30 0x563284419b35 in gf_isom_box_read isomedia/box_funcs.c:1528
#31 0x563284419b35 in gf_isom_box_parse_ex isomedia/box_funcs.c:208
#32 0x56328441a1e4 in gf_isom_parse_root_box isomedia/box_funcs.c:42
#33 0x563284430f44 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:206
#34 0x563284433bca in gf_isom_open_file isomedia/isom_intern.c:615
#35 0x56328417c852 in mp4boxMain /home/liuz/gpac-master/applications/mp4box/main.c:4767
#36 0x7f0252bccb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#37 0x56328416db19 in _start (/usr/local/gpac-asan3/bin/MP4Box+0x163b19)
```

0x602000002d1 is located 0 bytes to the right of 1-byte region [0x602000002d0,0x602000002d1)
allocated by thread T0 here:

```
#0 0x7f0253855b50 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb50)
#1 0x5632843ea263 in avcc_Read isomedia/avc_ext.c:2343
```

SUMMARY: AddressSanitizer: heap-buffer-overflow media_tools/av_parsers.c:4722 in gf_media_nalu_remove_emulation_bytes


Shadow bytes around the buggy address:

```
0x0c047fff8000: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
0x0c047fff8010: fa fa fd fd fa fa 00 00 fa fa 00 00 fa fa 00 00
0x0c047fff8020: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
0x0c047fff8030: fa fa 00 00 fa fa 00 00 fa fa 00 05 fa fa 00 00
0x0c047fff8040: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
=>0x0c047fff8050: fa fa 00 00 fa fa 00 00 fa fa[01]fa fa fa 01 fa
0x0c047fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c047fff80a0: 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
==23148==ABORTING
```

 aureliendavid added a commit that referenced this issue on Jan 9, 2020

 avcc_Read: add check on zero size malloc ([#1339](#))

7644478


aureliendavid commented on Jan 9, 2020

Contributor

thanks for the report

this should be fixed by the commit above

reopen if needed

 aureliendavid closed this as completed on Jan 9, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

