


New issue

Jump to bottom

## Runtime error: left shift of 128 by 24 places cannot be represented in type 'int' (mpegs.c:2236) #1266

 **strongcourage** opened this issue on Jul 5, 2019 · 1 comment

**strongcourage** commented on Jul 5, 2019


Hi,  
Our fuzzer found a crash on MP4Box (the latest commit [987169b](#) on master).  
PoC: [https://github.com/strongcourage/PoCs/blob/master/gpac\\_987169b/PoC\\_re\\_mpegs.c:2236](https://github.com/strongcourage/PoCs/blob/master/gpac_987169b/PoC_re_mpegs.c:2236)  
Command: MP4Box -info \$PoC  
ASAN says:

```
/home/dungnguyen/gueb-testing/gpac-head/src/media_tools/mpegs.c:3089:23: runtime error: left shift of 128 by 24 places cannot be represented in type 'int'
```

Valgrind says:

```
==21951== Invalid read of size 1
==21951== at 0x8C1380: gf_m2ts_process_pmt (mpegs.c:2236)
==21951== by 0x8AD409: gf_m2ts_section_complete (mpegs.c:1610)
==21951== by 0x8AE791: gf_m2ts_gather_section.isra.14 (mpegs.c:1740)
==21951== by 0x8B8FFF: gf_m2ts_process_packet (mpegs.c:3446)
==21951== by 0x8B8FFF: gf_m2ts_process_data (mpegs.c:3507)
==21951== by 0x8D3B58: gf_m2ts_probe_file (mpegs.c:4641)
==21951== by 0x89B594: gf_media_import (media_import.c:10998)
==21951== by 0x49B08B: convert_file_info (fileimport.c:124)
==21951== by 0x4621D5: mp4boxMain (main.c:4804)
==21951== by 0x57BC82F: (below main) (libc-start.c:291)
==21951== Address 0x5d8c465 is 0 bytes after a block of size 5 alloc'd
==21951== at 0x4C2D8BF: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21951== by 0x8AB2FA: gf_m2ts_section_complete (mpegs.c:1550)
==21951== by 0x8AE791: gf_m2ts_gather_section.isra.14 (mpegs.c:1740)
==21951== by 0x8B8FFF: gf_m2ts_process_packet (mpegs.c:3446)
==21951== by 0x8B8FFF: gf_m2ts_process_data (mpegs.c:3507)
==21951== by 0x8D3B58: gf_m2ts_probe_file (mpegs.c:4641)
==21951== by 0x89B594: gf_media_import (media_import.c:10998)
==21951== by 0x49B08B: convert_file_info (fileimport.c:124)
==21951== by 0x4621D5: mp4boxMain (main.c:4804)
==21951== by 0x57BC82F: (below main) (libc-start.c:291)
```

Thanks,  
Manh Dung

 **jeanlf** added a commit that referenced this issue on Jul 7, 2019

 be more strict on the PMT parsing - cf [#1266](#) [#1267](#)

f0af024

**jeanlf** commented on Jul 7, 2019

Contributor

could not reproduce exactly the same error but we made PMT parsing more resistant to broken streams

 **jeanlf** closed this as completed on Jul 7, 2019

 This was referenced on Jul 7, 2019

**SEGV on unknown address on gf\_list\_count #1270**



**SEGV on unknown addres on gf\_odf\_delete\_descriptor #1271**



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants

