


New issue

Jump to bottom

Runtime error: left shift of negative value (mpegts.c:2373) #1265

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

commented on Jul 5, 2019

Hi,

Our fuzzer found a crash on MP4Box (the latest commit [987169b](#) on master) due to an invalid read on function `gf_m2ts_process_pmt` (mpegts.c:2373).

PoC: https://github.com/strongcourage/PoCs/blob/master/gpac_987169b/PoC_re_mpegts.c:2373

Command: `MP4Box -info $PoC`

ASAN says:

```
/home/dungnguyen/gueb-testing/gpac-head/src/media_tools/mpegts.c:1655:25: runtime error: left shift of negative value -77
```

Valgrind says:

```
==22089== Invalid read of size 1
==22089== at 0x8C1918: gf_m2ts_process_pmt (mpegts.c:2373)
==22089== by 0x8AD409: gf_m2ts_section_complete (mpegts.c:1610)
==22089== by 0x8AE791: gf_m2ts_gather_section.isra.14 (mpegts.c:1740)
==22089== by 0x8B8FFF: gf_m2ts_process_packet (mpegts.c:3446)
==22089== by 0x8B8FFF: gf_m2ts_process_data (mpegts.c:3507)
==22089== by 0x8D3B58: gf_m2ts_probe_file (mpegts.c:4641)
==22089== by 0x89B594: gf_media_import (media_import.c:10998)
==22089== by 0x49B088: convert_file_info (fileimport.c:124)
==22089== by 0x4621D5: mp4boxMain (main.c:4804)
==22089== by 0x57BC82F: (below main) (libc-start.c:291)
==22089== Address 0x5d8e773 is 29 bytes before a block of size 80 in arena "client"
```

Thanks,
Manh Dung

commented on Jul 7, 2019 Contributor

thanks for the report, now fixed

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

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

