New issue

Jump to bottom

Runtime error: member access within null pointer of type 'GF_M2TS_ES *[8192]' (mpegts.c:2541) #1267

Closed **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_mpegts.c:2541
Command: MP4Box -info $PoC
ASAN says:

```
Multiple different PAT on single TS found, ignoring new PAT declaration (table id 127 - extended table id 0)
[MPEG-2 TS] Invalid PMT es descriptor size for PID 0
[MPEG-2 TS] PID 0 reused across programs 4096 and 19527, not completely supported
/home/dungnguyen/gueb-testing/gpac-head/src/media_tools/mpegts.c:2541:9: runtime error: member access within null pointer of type 'GF_M2TS_ES *[8192]'
```

Valgrind says:

```
==15789== Invalid read of size 4
==15789==    at 0xBC3CBC: gf_m2ts_process_pmt (mpegts.c:2541)
==15789==    by 0xBAD409: gf_m2ts_section_complete (mpegts.c:1610)
==15789==    by 0xBAE791: gf_m2ts_gather_section.isra.14 (mpegts.c:1740)
==15789==    by 0xBB8FFF: gf_m2ts_process_packet (mpegts.c:3446)
==15789==    by 0xBB8FFF: gf_m2ts_process_data (mpegts.c:3507)
==15789==    by 0xBD3B58: gf_m2ts_probe_file (mpegts.c:4641)
==15789==    by 0xB9B594: gf_media_import (media_import.c:10998)
==15789==    by 0x49B08B: convert_file_info (fileimport.c:124)
==15789==    by 0x4621D5: mp4boxMain (main.c:4804)
==15789==    by 0x57BC82F: (below main) (libc-start.c:291)
==15789==  Address 0x10 is not stack'd, malloc'd or (recently) free'd
```

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

thanks for the report, now fixed

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
Closed

SEGV on unknown addres on gf_odf_delete_descriptor #1271
Closed

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants