


New issue

Jump to bottom

Runtime error: member access within null pointer of type 'struct GF_Box' #1263

 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) due to a null pointer dereference bug on function ilst_item_Read (box_code_apple.c:119).
PoC: https://github.com/strongcourage/PoCs/blob/master/gpac_987169b/PoC_npd_ilst_item_Read
Command: MP4Box -info \$PoC


```
[iso file] Read Box type data (0x64617461) at position 32034 has size 0 but is not at root/file level, skipping
==18913== Invalid read of size 8
==18913==    at 0xF69508: ilst_item_Read (box_code_apple.c:119)
==18913==    by 0x818970: gf_isom_box_read (box_funcs.c:1528)
==18913==    by 0x818970: gf_isom_box_parse_ex (box_funcs.c:208)
==18913==    by 0xF68BEA: ilst_Read (box_code_apple.c:47)
==18913==    by 0x818970: gf_isom_box_read (box_funcs.c:1528)
==18913==    by 0x818970: gf_isom_box_parse_ex (box_funcs.c:208)
==18913==    by 0x819EEB: gf_isom_box_array_read_ex (box_funcs.c:1419)
==18913==    by 0xFE4AC8: meta_Read (box_code_meta.c:128)
==18913==    by 0x818970: gf_isom_box_read (box_funcs.c:1528)
==18913==    by 0x818970: gf_isom_box_parse_ex (box_funcs.c:208)
==18913==    by 0x819EEB: gf_isom_box_array_read_ex (box_funcs.c:1419)
==18913==    by 0xF843D0: udta_Read (box_code_base.c:7998)
==18913==    by 0x818970: gf_isom_box_read (box_funcs.c:1528)
==18913==    by 0x818970: gf_isom_box_parse_ex (box_funcs.c:208)
==18913==    by 0x819EEB: gf_isom_box_array_read_ex (box_funcs.c:1419)
==18913==    by 0xF8F40C: moov_Read (box_code_base.c:3751)
==18913== Address 0x8 is not stack'd, malloc'd or (recently) free'd
Segmentation fault
```

ASAN says:

```
[iso file] Read Box type data (0x64617461) at position 32034 has size 0 but is not at root/file level, skipping
/home/dungnguyen/gueb-testing/gpac-head/src/isomedia/box_code_apple.c:119:26: runtime error: member access within null pointer of type 'struct GF_Box'
```

Thanks,
Manh Dung

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


 fixed potential crash - cf #1263

6170024

jeanlf commented on Jul 7, 2019

Contributor

thanks for the report, now fixed

 jeanlf closed this as completed on Jul 7, 2019

  Clingto mentioned this issue on Nov 9, 2019

ERROR: AddressSanitizer: NULL pointer dereference in ilst_item_Read isomedia/box_code_apple.c:119 #1338



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

