


New issue

Jump to bottom

## Segmentation fault (ASAN: SEGV on unknown address) in the FixTrackID function of isom\_intern.c:133 #1346

 Closed gutiniao opened this issue on Nov 13, 2019 · 1 comment

gutiniao commented on Nov 13, 2019

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](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 isom\_intern.c at gpac 0.8.0.

Triggered by

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

Poc


009-invalid-FixTrackID

The ASAN information is as follows:

```
./MP4Box -diso 009-invalid-FixTrackID -out /dev/null
[iso file] Box "avcC" (start 939) has 34 extra bytes
[iso file] Unknown box type 0000 in parent sinf
[iso file] Unknown box type 74E80368 in parent moov
[iso file] Unknown box type tfhd in parent moof
[iso file] Box "UNKN" is larger than container box
[iso file] Box "moof" size 1463 (start 2004) invalid (read 7972)
ASAN:DEADLYSIGNAL
=====
==13653==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000028 (pc 0x564b3322e701 bp 0x600000000110 sp 0x7fff462fc3f0 T0)
==13653==The signal is caused by a READ memory access.
==13653==Hint: address points to the zero page.
#0 0x564b3322e700 in FixTrackID isomedia/isom_intern.c:133
#1 0x564b3322e700 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:372
#2 0x564b3322fbca in gf_isom_open_file isomedia/isom_intern.c:615
#3 0x564b32f78852 in mp4boxMain /home/liuz/gpac-master/applications/mp4box/main.c:4767
#4 0x7fd75e925b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#5 0x564b32f69b19 in _start (/usr/local/gpac-asan3/bin/MP4Box+0x163b19)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/isom_intern.c:133 in FixTrackID
==13653==ABORTING
```

 gutiniao changed the title ~~There is a heap buffer overflow in the FixTrackID function of isom\_intern.c:133~~ Segmentation fault (ASAN: SEGV on unknown address) in the FixTrackID function of isom\_intern.c:133 on Dec 3, 2019

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

 add nullptr check in fixtrackid (#1346)

6040a59


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

