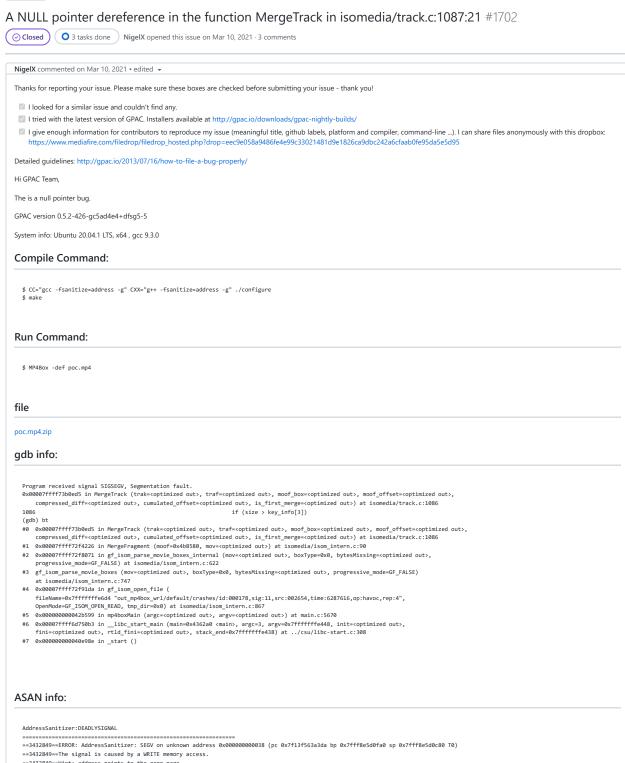


New issue



Jump to bottom

```
==3432849==ERROR: AddressSanitizer: SEGV on unknown address 0x0000000000000 (pc 0x7f13f563a3da bp 0x7fff8e5d0fa0 sp 0x7fff8e5d0c80 T0)
==3432849==The signal is caused by a WRITE memory access.
==3432849==Thir: address points to the zero page.
#0 0x7f13f56a3ada in MergeFrack /home/topsec/Downloads/gpac/src/isomedia/isom_intern.c:90:7
#1 0x7f13f54d5bc8 in MergeFragment /home/topsec/Downloads/gpac/src/isomedia/isom_intern.c:90:7
#2 0x7f13f54d5bc8 in MergeFragment /home/topsec/Downloads/gpac/src/isomedia/isom_intern.c:622:9
#3 0x7f13f54e190f in gf_isom_parse_movie_boxes_internal /home/topsec/Downloads/gpac/src/isomedia/isom_intern.c:747:6
#4 0x7f13f54e190f in gf_isom_parse_movie_boxes /home/topsec/Downloads/gpac/src/isomedia/isom_intern.c:621:9
#5 0x4f0f92 in mphboxMain /home/topsec/Downloads/gpac/src/isomedia/isom_intern.c:867:19
#5 0x4f0f92 in mphboxMain /home/topsec/Downloads/gpac/aplications/mphbox/main.c:5670:12
#6 0x7f13f6a0bc in _libc_start_main /build/glibc-exitMB/glibc-2.31/csu/../csu/libc-start.c:308:16
#7 0x4289ed in _start (/home/topsec/Downloads/gpac/afl_build/bin/gcc/MP4Box+0x4289ed)

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV /home/topsec/Downloads/gpac/src/isomedia/track.c:1087:21 in MergeTrack
==3432849==ABORTING
```

HX from Topsec alpha Security Team

jeanlf commented on Mar 11, 2021

I cannot access the poc file, could you re-upload it?

NigelX commented on Mar 11, 2021

Author

(a) jeanlf closed this as completed in c4a5109 on Mar 11, 2021

setharnold commented on Apr 9, 2021

CVE-2021-28300 has been assigned to this issue.

Thanks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

