New issue

Jump to bottom

A NULL pointer dereference in the function MergeTrack in isomedia/track.c:1087:21 #1702

Closed 3 tasks done **NigelX** opened this issue on Mar 10, 2021 · 3 comments

NigelX commented on Mar 10, 2021 • edited

Thanks for reporting your issue. Please make sure these boxes are checked before submitting your issue - thank you!

- [x] I looked for a similar issue and couldn't find any.
- [x] I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
- [x] 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

Detailed guidelines: http://gpac.io/2013/07/16/how-to-file-a-bug-properly/

Hi GPAC Team,

The is a null pointer bug.

GPAC version 0.5.2-426-gc5ad4e4+dfsg5-5

System info: Ubuntu 20.04.1 LTS, x64 , gcc 9.3.0

Compile Command:

```
$ CC="gcc -fsanitize=address -g" CXX="g++ -fsanitize=address -g" ./configure
$ make
```

Run Command:

```
$ MP4Box -def poc.mp4
```

file

poc.mp4.zip

gdb info:

```
Program received signal SIGSEGV, Segmentation fault.
0x00007ffff73b0ed5 in MergeTrack (trak=<optimized out>, traf=<optimized out>, moof_box=<optimized out>, moof_offset=<optimized out>,
    compressed_diff=<optimized out>, cumulated_offset=<optimized out>, is_first_merge=<optimized out>) at isomedia/track.c:1086
1086                                                    if (size > key_info[3])
(gdb) bt
#0  0x00007ffff73b0ed5 in MergeTrack (trak=<optimized out>, traf=<optimized out>, moof_box=<optimized out>, moof_offset=<optimized out>,
    compressed_diff=<optimized out>, cumulated_offset=<optimized out>, is_first_merge=<optimized out>) at isomedia/track.c:1086
#1  0x00007ffff72f4226 in MergeFragment (moof=0x4b8580, mov=<optimized out>) at isomedia/isom_intern.c:90
#2  0x00007ffff72f8071 in gf_isom_parse_movie_boxes_internal (mov=<optimized out>, boxType=0x0, bytesMissing=<optimized out>,
    progressive_mode=GF_FALSE) at isomedia/isom_intern.c:622
#3  gf_isom_parse_movie_boxes (mov=<optimized out>, boxType=0x0, bytesMissing=<optimized out>, progressive_mode=GF_FALSE)
    at isomedia/isom_intern.c:747
#4  0x00007ffff72f91da in gf_isom_open_file (
    fileName=0x7fffffffe6d4 "out_mp4box_wrl/default/crashes/id:000178,sig:11,src:002654,time:6287616,op:havoc,rep:4",
    OpenMode=GF_ISOM_OPEN_READ, tmp_dir=0x0) at isomedia/isom_intern.c:867
#5  0x000000000042b599 in mp4boxMain (argc=<optimized out>, argv=<optimized out>) at main.c:5670
#6  0x00007ffff6d750b3 in __libc_start_main (main=0x4362a0 <main>, argc=3, argv=0x7fffffffe448, init=<optimized out>,
    fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe438) at ../csu/libc-start.c:308
#7  0x000000000040e98e in _start ()
```

ASAN info:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==3432849==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000038 (pc 0x7f13f563a3da bp 0x7fff8e5d0fa0 sp 0x7fff8e5d0c80 T0)
==3432849==The signal is caused by a WRITE memory access.
==3432849==Hint: address points to the zero page.
    #0 0x7f13f563a3da in MergeTrack /home/topsec/Downloads/gpac/src/isomedia/track.c:1087:21
    #1 0x7f13f54db5c8 in MergeFragment /home/topsec/Downloads/gpac/src/isomedia/isom_intern.c:90:7
    #2 0x7f13f54e190f in gf_isom_parse_movie_boxes_internal /home/topsec/Downloads/gpac/src/isomedia/isom_intern.c:622:9
    #3 0x7f13f54e190f in gf_isom_parse_movie_boxes /home/topsec/Downloads/gpac/src/isomedia/isom_intern.c:747:6
    #4 0x7f13f54e3dea in gf_isom_open_file /home/topsec/Downloads/gpac/src/isomedia/isom_intern.c:867:19
    #5 0x4f0f92 in mp4boxMain /home/topsec/Downloads/gpac/applications/mp4box/main.c:5670:12
    #6 0x7f13f46b70b2 in __libc_start_main /build/glibc-eX1tMB/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 — Contributor

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

NigelX commented on Mar 11, 2021 — Author

file poc.mp4.zip

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