New issue

Jump to bottom

Bug: Memcpy from unknown addrees in MP4BOX at src/utils/bitstream.c:1028 #1885

Closed ○ 3 tasks done **AntsKnows** opened this issue on Aug 23, 2021 · 0 comments

AntsKnows commented on Aug 23, 2021 • edited

- ☑ 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 ...).

It's a memcpy from unknown addrees bug.

Step to reproduce:
1.get latest commit code (GPAC version 1.1.0-DEV-rev1170-g592ba2689-master)
2.compile with --enable-sanitizer
3.run ./MP4BOX -hint poc_isom_hinter -out /dev/null

Env:
Ubunut 20.04 , clang 12.0.1

ASAN report

```
=================================================================
==194694==ERROR: AddressSanitizer: unknown-crash on address 0x03e8ef58ac20 at pc 0x0000004a3cd7 bp 0x7ffdef589370 sp 0x7ffdef588b38
READ of size 24912 at 0x03e8ef58ac20 thread T0
    #0 0x4a3cd6 in __asan_memcpy (/home/lly/pro/gpac_public/bin/gcc/MP4Box+0x4a3cd6)
    #1 0x7f35556d80ef in gf_bs_write_data /home/lly/pro/gpac_public/src/utils/bitstream.c:1028:4
    #2 0x7f3555da5a1a in gf_odf_write_default /home/lly/pro/gpac_public/src/odf/odf_code.c:1320:3
    #3 0x7f3555da92ec in gf_odf_desc_write_bs /home/lly/pro/gpac_public/src/odf/odf_codec.c:325:6
    #4 0x7f3555da92ec in gf_odf_desc_write /home/lly/pro/gpac_public/src/odf/odf_codec.c:343:6
    #5 0x7f3555da9661 in gf_odf_desc_copy /home/lly/pro/gpac_public/src/odf/odf_codec.c:387:6
    #6 0x7f3555cb8760 in gf_isom_set_extraction_slc /home/lly/pro/gpac_public/src/isomedia/isom_write.c:5468:9
    #7 0x7f3555fa467b in gf_hinter_finalize /home/lly/pro/gpac_public/src/media_tools/isom_hinter.c:1245:5
    #8 0x4e8d21 in HintFile /home/lly/pro/gpac_public/applications/mp4box/main.c:3550:2
    #9 0x4f5988 in mp4boxMain /home/lly/pro/gpac_public/applications/mp4box/main.c:6329:7
    #10 0x7f355476d0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
    #11 0x429a6d in _start (/home/lly/pro/gpac_public/bin/gcc/MP4Box+0x429a6d)

Address 0x03e8ef58ac20 is located in the high shadow area.
```

Buggy code
in bitstream.c:

```
u32 gf_bs_write_data(GF_BitStream *bs, const u8 *data, u32 nbBytes)
{
...
memcpy(bs->original + bs->position - bs->bytes_out, data, nbBytes);  <---data is not inited
...
}
```

poc.zip

AntsKnows changed the title ~~Bug: Memcpy from unknown addrees~~ Bug: Memcpy from unknown addrees in MP4BOX at src/utils/bitstream.c:1028 on Aug 27, 2021

jeanlf closed this as completed in `f5a038e` on Aug 30, 2021

This was referenced on Aug 30, 2021

Segmentation fault using mp4box in gf_odf_desc_copy, odf_codec.c:381 #1888
Closed

Segmentation fault using mp4box in gf_odf_size_descriptor, desc_private.c:380 #1889
Closed

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development

No branches or pull requests

1 participant