New issue

Jump to bottom

BUG : free on unknown addrees in MP4BOX at gf_hinter_track_finalize media_tools/isom_hinter.c:956 #1883

Closed 3 tasks done **AntsKnows** opened this issue on Aug 20, 2021 · 0 comments

AntsKnows commented on Aug 20, 2021 • edited

- [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 ...).

It's a pointer free on unknown addrees bug caused by freeing a uninitialized pointer.

Step to reproduce:
1.get latest commit code (GPAC version 1.1.0-DEV-rev1170-g592ba26-master)
2.compile with --enable-sanitizer
3.run ./MP4BOX -hint poc_isom_hinter -out /dev/null

Env:
Ubunut 20.04 , clang 10.0.0

ASAN report

```
==40495==ERROR: AddressSanitizer: SEGV on unknown address 0x7f0eebe5ccf8 (pc 0x7f0eef8765fc bp 0x7f0eebe5ccf8 sp 0x7ffecbe40880 T0)
    #0 0x7f0eef8765fb  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x215fb)
    #1 0x7f0eef8ed29d in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x9829d)
    #2 0x7f0eed579cb9 in gf_hinter_track_finalize media_tools/isom_hinter.c:956
    #3 0x42842d in HintFile /home/lly/gpac_public/applications/mp4box/main.c:3533
    #4 0x42e4e4 in mp4boxMain /home/lly/gpac_public/applications/mp4box/main.c:6329
    #5 0x7f0eead8983f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #6 0x413bc8 in _start (/home/lly/gpac_public/bin/gcc/MP4Box+0x413bc8)
```

Buggy code and reason:
in isom_hinter.c:950

```
for (i=0; i<gf_isom_get_sample_description_count(tkHint->file, tkHint->TrackNum); i++) {
    u8 *tx3g;   <---with out init
    ...
    gf_isom_text_get_encoded_tx3g(..., &tx3g, &tx3g_len);  <--- supposed to init tx3g
    ...
    gf_free(tx3g); <--- free tx3g
   ...
              }
```

It is supposed to init tx3g in gf_isom_text_get_encoded_tx3g, but in gf_isom_text_get_encoded_tx3g, it might forget that mission.

```
GF_Err gf_isom_text_get_encoded_tx3g(GF_ISOFile *file, u32 track, u32 sidx, u32 sidx_offset, u8 **tx3g, u32 *tx3g_size)
{
        ...
        //  it returns without init tx3g once a->type equals another value;
        if ((a->type != GF_ISOM_BOX_TYPE_TX3G) && (a->type != GF_ISOM_BOX_TYPE_TEXT)) return GF_BAD_PARAM;

        ...
        *tx3g = NULL;  <--- real init here
        *tx3g_size = 0;
        gf_bs_get_content(bs, tx3g, tx3g_size);
        gf_bs_del(bs);
        return GF_OK;
}
```

poc_isom_hinter.zip

AntsKnows changed the title ~~BUG : free on unknown addrees~~ **BUG : free on unknown addrees in MP4BOX at gf_hinter_track_finalize media_tools/isom_hinter.c:956** on Aug 27, 2021

jeanlf closed this as completed in `b09c75d` on Aug 30, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant