New issue

Jump to bottom

There are memory leaks in the senc_Parse function of box_code_drm.c:1349 #1342

Closed **gutiniao** opened this issue on Nov 12, 2019 · 1 comment

gutiniao commented on Nov 12, 2019 • edited

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

A crafted input will lead to crash in box_code_drm.c at gpac 0.8.0.

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

Poc
004-memleak-senc1349

The ASAN information is as follows:

```
./MP4Box -diso 004-memleak-senc1349 -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 75876C20 in parent dref
[iso file] Unknown box type 0000 in parent schi
[iso file] Unknown box type stts in parent stsd
[iso file] Unknown box type stsc in parent stsd
[iso file] Unknown box type stsz in parent stsd
[iso file] Unknown box type stco in parent stsd
[iso file] Unknown box type sgpd in parent stsd
[iso file] Unknown box type udta in parent stsd
[iso file] Box "stsd" (start 1439) has 8825 extra bytes
[iso file] Box "stsd" is larger than container box
[iso file] Box "stbl" size 291 (start 1431) invalid (read 9139)
[ISO file] dataReferenceIndex set to 0 in sample entry, overriding to 1
[ISO file] dataReferenceIndex set to 0 in sample entry, overriding to 1
[ISO file] dataReferenceIndex set to 0 in sample entry, overriding to 1
[ISO file] dataReferenceIndex set to 0 in sample entry, overriding to 1
[iso file] senc box without tenc, assuming MS smooth+piff
[isobmf] Failed to parse SENC box, invalid SAI size
[isobmf] could not get cenc info for sample 1: Invalid IsoMedia File
Error opening file 004-memleak-senc1349: Invalid IsoMedia File

=================================================================
==2371==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 32 byte(s) in 1 object(s) allocated from:
    #0 0x7f0fc2519b50 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb50)
    #1 0x564665fcabe9 in senc_Parse isomedia/box_code_drm.c:1349

SUMMARY: AddressSanitizer: 32 byte(s) leaked in 1 allocation(s).
```

about code:

```
#endif
        count = gf_bs_read_u32(bs);
        if (!senc->samp_aux_info) senc->samp_aux_info = gf_list_new();
        for (i=0; i<count; i++) {
                u32 is_encrypted;
---------->GF_CENCSampleAuxInfo *sai = (GF_CENCSampleAuxInfo *)gf_malloc(sizeof(GF_CENCSampleAuxInfo));
                memset(sai, 0, sizeof(GF_CENCSampleAuxInfo));
```

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

`add IV_size check on senc_Parse (#1341, #1342)` a0e6aa8

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