New issue

Jump to bottom

# Segmentation fault caused by buffer overflow using mp4box in avc_compute_poc, av_parsers.c:5988 #1899

Closed  3 tasks done  **5hadowblad3** opened this issue on Aug 27, 2021 · 0 comments

**5hadowblad3** commented on Aug 27, 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 ...).

Hi, there.

There is a segmentation fault caused by buffer overflow in avc_compute_poc, av_parsers.c:5988 in commit `592ba26` .

Here is my environment, compiler info and gpac version:

```
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.6 LTS
Release:        16.04
Codename:       xenial
gcc: 5.4.0

MP4Box - GPAC version 1.1.0-DEV-rev1170-g592ba26-master
(c) 2000-2021 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io
        MINI build (encoders, decoders, audio and video output disabled)

Please cite our work in your research:
        GPAC Filters: https://doi.org/10.1145/3339825.3394929
        GPAC: https://doi.org/10.1145/1291233.1291452

GPAC Configuration: --static-bin --enable-debug
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_SOCK_UN GPAC_MINIMAL_ODF GPAC_HAS_QJS GPAC_HAS_FREETYPE GPAC_HAS_JPEG GPAC_HAS_PNG  GPAC_DISABLE_3D
```

To reproduce, run

```
./MP4Box -info poc
```

POC:
poc.zip
(unzip first)

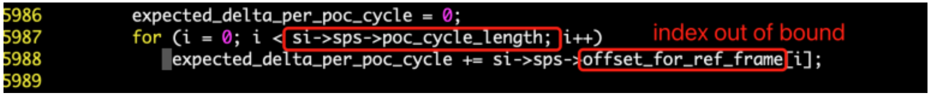
Program output:

```
[Core] exp-golomb read failed, not enough bits in bitstream !
[Core] exp-golomb read failed, not enough bits in bitstream !
[Core] exp-golomb read failed, not enough bits in bitstream !
[Core] exp-golomb read failed, not enough bits in bitstream !
[Core] exp-golomb read failed, not enough bits in bitstream !
[avc-h264] offset_for_ref_frame overflow from poc_cycle_length
[AVC|H264] Warning: Error parsing NAL unit
[AVC|H264] Error parsing Sequence Param Set
[Core] exp-golomb read failed, not enough bits in bitstream !
[Core] exp-golomb read failed, not enough bits in bitstream !
[Core] exp-golomb read failed, not enough bits in bitstream !
[Core] exp-golomb read failed, not enough bits in bitstream !
Segmentation fault (core dumped)
```

Here is the trace reported by gdb:

```
Stopped reason: SIGSEGV
gef➤  bt
#0  0x0000000000b82f00 in avc_compute_poc (si=si@entry=0x7fffffff5020) at /mnt/data/playground/gpac/src/media_tools/av_parsers.c:5988
#1  0x0000000000bce182 in gf_avc_parse_nalu (bs=<optimized out>, avc=0x24ae050) at /mnt/data/playground/gpac/src/media_tools/av_parsers.c:6191
#2  0x000000000144109d in naludmx_parse_nal_avc (is_islice=<synthetic pointer>, is_slice=<synthetic pointer>, skip_nal=<synthetic pointer>, nal_type=0x3, size=0xf, data=0x248dfba
"Cd\234\316s", <incomplete sequence \350>, ctx=0x24ada70) at /mnt/data/playground/gpac/src/filters/reframe_nalu.c:2348
#3  naludmx_process (filter=0x24a0bd0) at /mnt/data/playground/gpac/src/filters/reframe_nalu.c:2874
#4  0x0000000000fe4c18 in gf_filter_process_task (task=0x2492ed0) at /mnt/data/playground/gpac/src/filter_core/filter.c:2441
#5  0x0000000000f7b909 in gf_fs_thread_proc (sess_thread=sess_thread@entry=0x248c2b0) at /mnt/data/playground/gpac/src/filter_core/filter_session.c:1640
#6  0x0000000000f93558 in gf_fs_run (fsess=fsess@entry=0x248c220) at /mnt/data/playground/gpac/src/filter_core/filter_session.c:1877
#7  0x0000000000c18b4b in gf_media_import (importer=importer@entry=0x7fffffff5bf0) at /mnt/data/playground/gpac/src/media_tools/media_import.c:1178
#8  0x0000000000497345 in convert_file_info (inName=0x7fffffffe159 "tmp", trackID=0x0) at /mnt/data/playground/gpac/applications/mp4box/fileimport.c:128
#9  0x0000000000456aaa in mp4boxMain (argc=<optimized out>, argv=<optimized out>) at /mnt/data/playground/gpac/applications/mp4box/main.c:5925
#10 0x0000000001f06bb6 in generic_start_main ()
#11 0x0000000001f071a5 in __libc_start_main ()
#12 0x000000000041c4e9 in _start ()
```

The reason for this bug is that the program does not check whether the length of a buffer fit its actual size.



```
5986            expected_delta_per_poc_cycle = 0;
5987            for (i = 0; i < si->sps->poc_cycle_length; i++)
5988                expected_delta_per_poc_cycle += si->sps->offset_for_ref_frame[i];
5989
```

**jeanlf** closed this as completed in `04dbf08` 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