New issue

Jump to bottom

A Integer number overflow in function hevc_parse_slice_segment. #1721

Closed **treebacker** opened this issue on Mar 29, 2021 · 1 comment

treebacker commented on Mar 29, 2021 • edited

There is a integer overflow in media_tools/av_parsers.c:6568, function hevc_parse_slice_segment.
Below code:
`

```
pps_id = gf_bs_read_ue_log(bs, "pps_id");
if (pps_id >= 64)
return -1;


  pps = &hevc->pps[pps_id];
  sps = &hevc->sps[pps->sps_id];
  si->sps = sps;
  si->pps = pps;
```

`

However, function may return a negative number to pps_id, which smaller than 64.
Results a crash in followed execution.

In command Line:
gpac -info bug4

```
ubuntu@VM-0-3-ubuntu:~                    /gpac-1.0.1$ ./debug_bin/gcc/gpac -info                    gpac/uniq/bug4
ID3 tag detected size 120298666 but probe data only 1840 bytes, will rely on file extension (try increasing probe size using --block_size)
ID3 tag detected size 120298666 but probe data only 1840 bytes, will rely on file extension (try increasing probe size using --block_size)
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
Segmentation fault
```

In gdb:

```
Starting program:                                    gpac-1.0.1/debug_bin/gcc/gpac -info ~                                    ac/uniq/bug4
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
ID3 tag detected size 120298666 but probe data only 1840 bytes, will rely on file extension (try increasing probe size using --block_size)
ID3 tag detected size 120298666 but probe data only 1840 bytes, will rely on file extension (try increasing probe size using --block_size)
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit

Breakpoint 1, hevc_parse_slice_segment (bs=0x5555557a4990, hevc=0x7ffff7fb0010, si=0x7fffffffde30) at media_tools/av_parsers.c:6568
6568    {
(gdb) n
6570            u32 num_ref_idx_l0_active = 0, num_ref_idx_l1_active = 0;
(gdb)
6574            Bool RapPicFlag = GF_FALSE;
(gdb)
6575            Bool IDRPicFlag = GF_FALSE;
(gdb)
6577            si->first_slice_segment_in_pic_flag = gf_bs_read_int(bs, 1);
(gdb)
6579            switch (si->nal_unit_type) {
(gdb)
6593            if (RapPicFlag) {
(gdb)
6597            pps_id = gf_bs_get_ue(bs);
(gdb)
6598            if (pps_id >= 64)
(gdb) p pps_id
$2 = -2147481409
(gdb) n
6601            pps = &hevc->pps[pps_id];
(gdb) n
6602            sps = &hevc->sps[pps->sps_id];
(gdb) n

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff7571ce3 in hevc_parse_slice_segment (bs=0x5555557a4990, hevc=0x7ffff7fb0010, si=0x7fffffffde30) at media_tools/av_parsers.c:6602
6602            sps = &hevc->sps[pps->sps_id];
(gdb)
```

pps_id may be a negative number

overflow

The crafted file is in the attached zip:
bug4.zip

jeanlf added a commit that referenced this issue on Mar 29, 2021

`add safety in avc/hevc/vvc sps/pps/vps ID check - cf #1720 #1721 #1722` 51cdb67

jeanlf commented on Mar 29, 2021 Contributor

could not reproduce crash with latest master, but added safety checks. Thanks for the report

jeanlf closed this as completed on Mar 29, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants