New issue

Jump to bottom

A heap overflow in function gf_hevc_read_pps_bs_internal #1722

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

treebacker commented on Mar 29, 2021 • edited

In `media_tools/av_parsers.c` , function `gf_hevc_read_pps_bs_internal` .
There is a loop as below:
`

```
	pps->num_tile_columns = 1 + gf_bs_read_ue_log(bs, "num_tile_columns_minus1");
	pps->num_tile_rows = 1 + gf_bs_read_ue_log(bs, "num_tile_rows_minus1");
	pps->uniform_spacing_flag = gf_bs_read_int_log(bs, 1, "uniform_spacing_flag");
	if (!pps->uniform_spacing_flag) {
		for (i = 0; i < pps->num_tile_columns - 1; i++) {
			pps->column_width[i] = 1 + gf_bs_read_ue_log_idx(bs, "column_width_minus1", i);
		}
```

`

However, with crafted file, **pps->num_tile_columns** may be larger than sizeof(pps->column_width), which results a heap overflow in the loop.

In Command line:
gpac -info bug5

```
ubuntu@VM-0-3-ubuntu:~/gpac-1.0.1$ ./debug_bin/gcc/gpac -info ~/ /gpac/uniq/bug5
[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
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
[HEVC] Warning: Error parsing NAL unit
Segmentation fault
```

In gdb:

```
(gdb)
7982            if (pps->tiles_enabled_flag) {
(gdb)
7983                    pps->num_tile_columns = 1 + gf_bs_get_ue(bs);
(gdb)
7984                    pps->num_tile_rows = 1 + gf_bs_get_ue(bs);
(gdb) p pps->num_tile_columns
$3 = 1073741824
(gdb) n
7985                    pps->uniform_spacing_flag = gf_bs_read_int(bs, 1);
(gdb)
7986                    if (!pps->uniform_spacing_flag) {                    integere larger than buffer size
(gdb)
7987                            for (i = 0; i < pps->num_tile_columns - 1; i++) {
(gdb)
7988                                    pps->column_width[i] = 1 + gf_bs_get_ue(bs);
(gdb) c
Continuing.

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff757728e in gf_media_hevc_read_pps_bs_internal (bs=0x5555557a4990, hevc=0x7ffff7fb0010) at media_tools/av_parsers.c:7988
7988                                    pps->column_width[i] = 1 + gf_bs_get_ue(bs);
(gdb) x/40x pps->num_tile_columns
0x40000000:     Cannot access memory at address 0x40000000
(gdb) x/40x  pps->column_width
0x7ffff7fc3e3c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3e4c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3e5c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3e6c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3e7c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3e8c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3e9c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3eac: 0x0000000100000001      0x0000000100000001      heap overflow
0x7ffff7fc3ebc: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3ecc: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3edc: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3eec: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3efc: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3f0c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3f1c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3f2c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3f3c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3f4c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3f5c: 0x0000000100000001      0x0000000100000001
0x7ffff7fc3f6c: 0x0000000100000001      0x0000000100000001
```

The crafted file is in the attached zip:
bug5.zip

treebacker changed the title ~~A stack overflow in function gf_hevc_read_pps_bs_internal~~ A heap overflow in function gf_hevc_read_pps_bs_internal on Mar 29, 2021

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