New issue

Jump to bottom

A Null Pointer Dereference In gf_filter_pck_new_alloc_internal #1719

Closed **treebacker** opened this issue on Mar 29, 2021 · 0 comments

treebacker commented on Mar 29, 2021 • edited

There is a `Null Pointer Dereference` in function `filter_core/filter_pck.c:104:gf_filter_pck_new_alloc_internal` ,
The `pid` comes from function `av1dmx_parse_flush_sample` , the `ctx.opid` maybe NULL.
Result a crash in `gf_filter_pck_new_alloc_internal` .

In command line:
gpac -info bug2

```
ubuntu@VM-0-3-ubuntu:~ /gpac-1.0.1$ ./bin/gcc/gpac -info ~/ /gpac/uniq/bug2
[AV1] unknown OBU type 10 (size 571). Skipping.
Segmentation fault
```

In gdb:

```
Starting program: / am/gpac-1.0.1/bin/gcc/gpac -info ~/ e/gpac/uniq/bug2
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[AV1] unknown OBU type 10 (size 571). Skipping.

Program received signal SIGSEGV, Segmentation fault.
gf_filter_pck_new_alloc_internal (pid=0x0, data_size=571, data=0x737d50, no_block_check=GF_TRUE) at filter_core/filter_pck.c:104
104             if (PID_IS_INPUT(pid)) {
(gdb) bt
#0  gf_filter_pck_new_alloc_internal (pid=0x0, data_size=571, data=0x737d50, no_block_check=GF_TRUE) at filter_core/filter_pck.c:104
#1  0x00007ffff764f6b8 in av1dmx_parse_flush_sample (filter=<optimized out>, ctx=0x737d50) at filters/reframe_av1.c:728
#2  0x00007ffff76506b8 in av1dmx_process (filter=0x730d70) at filters/reframe_av1.c:897
#3  0x00007ffff7423236 in gf_filter_process_task (task=<optimized out>) at filter_core/filter.c:2158
#4  0x00007ffff7404882 in gf_fs_thread_proc (sess_thread=<optimized out>) at filter_core/filter_session.c:1467
#5  0x00007ffff7403c59 in gf_fs_run (fsess=0x711630) at filter_core/filter_session.c:1704
#6  0x000000000040ea7b in gpac_main (argc=<optimized out>, argv=0x7122b0) at main.c:2116
#7  0x00007ffff658ebf7 in __libc_start_main (main=0x404460 <main>, argc=3, argv=0x7fffffffe8b8, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe8a8)
    at ../csu/libc-start.c:310
#8  0x000000000040439a in _start ()
(gdb) b filter_core/filter_pck.c:104
Breakpoint 1 at 0x7ffff73ae104: file filter_core/filter_pck.c, line 104.
(gdb) r
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/ubuntu/t  1.0.1/bin/gcc/gpac -info ~/  gpac/uniq/bug2
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[AV1] unknown OBU type 10 (size 571). Skipping.

Breakpoint 1, gf_filter_pck_new_alloc_internal (pid=0x0, data_size=571, data=0x737d50, no_block_check=GF_TRUE) at filter_core/filter_pck.c:104
104             if (PID_IS_INPUT(pid)) {
(gdb) p pid
$1 = (GF_FilterPid *) 0x0
(gdb) n

Program received signal SIGSEGV, Segmentation fault.
gf_filter_pck_new_alloc_internal (pid=0x0, data_size=571, data=0x737d50, no_block_check=GF_TRUE) at filter_core/filter_pck.c:104
104             if (PID_IS_INPUT(pid)) {
(gdb) b filters/reframe_av1.c:728
Breakpoint 2 at 0x7ffff764f654: file filters/reframe_av1.c, line 728.
(gdb) r
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /  bin/gcc/gpac -info ~/  e/gpac/uniq/bug2
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[AV1] unknown OBU type 10 (size 571). Skipping.

Breakpoint 2, av1dmx_parse_flush_sample (filter=<optimized out>, ctx=0x737d50) at filters/reframe_av1.c:728
728             pck = gf_filter_pck_new_alloc(ctx->opid, pck_size, &output);
(gdb) p ctx->opid
$2 = (GF_FilterPid *) 0x0
(gdb) p pck_size
$3 = 571
(gdb) p output
```

Null Pointer Dereference

The crafted file is in attach zip:
bug2.zip

jeanlf closed this as completed in `13dad7d` on Mar 29, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant