New issue Jump to bottom

A NULL pointer dereference in gf_filter_pid_set_property_full #2223

Closed 3 tasks Janette88 opened this issue on Jul 7 · 0 comments

Janette88 commented on Jul 7

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/

Description:
`A crash happened on MP4Box(GPAC version 2.1-DEV-revUNKNOWN-master) due to a null pointer dereference vulnerability in gf_filter_pid_set_property_full function (filter_core/filter_pid.c:5250) .

`

MP4Box version

```
./MP4Box -version
MP4Box - GPAC version 2.1-DEV-revUNKNOWN-master
(c) 2000-2022 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io

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: --enable-sanitizer
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_IPV6 GPAC_HAS_SSL GPAC_HAS_SOCK_UN
GPAC_MINIMAL_ODF GPAC_HAS_QJS GPAC_HAS_LINUX_DVB  GPAC_DISABLE_3D
```

poc

poc.zip

command

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

crash output

```
[AVC|H264] Warning: Error parsing NAL unit
filter_core/filter_pid.c:5250:6: runtime error: member access within null pointer of type 'struct
GF_FilterPid'
```

gdb output

```
pwndbg> r
Starting program: /home/fuzz/gpac2.1/gpac/bin/gcc/MP4Box -info ../../../test/segv2/poc
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
[AVC|H264] Warning: Error parsing NAL unit
filter_core/filter_pid.c:5250:6: runtime error: member access within null pointer of type 'struct
GF_FilterPid'
[Inferior 1 (process 2239153) exited with code 01]
pwndbg> b filter_pid.c:5250
Breakpoint 1 at 0x7ffff4b829f6: filter_pid.c:5250. (6 locations)
pwndbg> r
Starting program: /home/fuzz/gpac2.1/gpac/bin/gcc/MP4Box -info ../../../test/segv2/poc
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, gf_filter_pid_set_property_full (is_info=GF_FALSE, value=0x7ffffffe9150,
dyn_name=0x0, prop_name=0x0, prop_4cc=1347244884, pid=0x613000000040) at
filter_core/filter_pid.c:5301
5301            return gf_filter_pid_set_property_full(pid, prop_4cc, NULL, NULL, value,
GF_FALSE);
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
─────────────────────────────────────────────────────────────────────────────────────────────────────
 REGISTERS
]────────────────────────────────────────────────────────────────────────────────────────────────────

 RAX  0x0
 RBX  0x7ffffffe8f50 ◂— 0x41b58ab3
 RCX  0xfffffffd22a ◂— 0x0
 RDX  0x7ffffffe9150 ◂— 0x2
 RDI  0x613000000040 ◂— 0x613000000040 /* '@' */
 RSI  0x504d5354
 R8   0x0
 R9   0x7ffff58cb4f0 (global_log_tools+496) ◂— 0x2
 R10  0x7ffff24ab3f1 ◂— 'gf_filter_pid_set_property'
 R11  0x7ffff4b84110 (gf_filter_pid_set_property) ◂— endbr64
 R12  0x613000000040 ◂— 0x613000000040 /* '@' */
 R13  0x7ffffffe9150 ◂— 0x2
 R14  0x504d5354
 R15  0xffffffd1ea ◂— 0x0
 RBP  0x7ffffffe9060 —▸ 0x7ffffffe9380 —▸ 0x7ffffffea0d0 —▸ 0x7ffffffea170 —▸ 0x7ffffffea280 ◂—
...
 RSP  0x7ffffffe8f30 ◂— 0x0
 RIP  0x7ffff4b841c6 (gf_filter_pid_set_property+182) ◂— test   r12, r12
─────────────────────────────────────────────────────────────────────────────────────────────────
 DISASM
]────────────────────────────────────────────────────────────────────────────────────────────────

 ► 0x7ffff4b841c6 <gf_filter_pid_set_property+182>    test   r12, r12
   0x7ffff4b841c9 <gf_filter_pid_set_property+185>    je     gf_filter_pid_set_property+1477
<gf_filter_pid_set_property+1477>

   0x7ffff4b841cf <gf_filter_pid_set_property+191>    test   r12b, 7
   0x7ffff4b841d3 <gf_filter_pid_set_property+195>    jne    gf_filter_pid_set_property+1477
<gf_filter_pid_set_property+1477>

   0x7ffff4b841d9 <gf_filter_pid_set_property+201>    mov    rax, r12
   0x7ffff4b841dc <gf_filter_pid_set_property+204>    shr    rax, 3
   0x7ffff4b841e0 <gf_filter_pid_set_property+208>    cmp    byte ptr [rax + 0x7fff8000], 0
   0x7ffff4b841e7 <gf_filter_pid_set_property+215>    jne    gf_filter_pid_set_property+1447
<gf_filter_pid_set_property+1447>

   0x7ffff4b841ed <gf_filter_pid_set_property+221>    cmp    r12, qword ptr [r12]
   0x7ffff4b841f1 <gf_filter_pid_set_property+225>    jne    gf_filter_pid_set_property+1016
<gf_filter_pid_set_property+1016>

   0x7ffff4b841f7 <gf_filter_pid_set_property+231>    mov    esi, r14d
─────────────────────────────────────────────────────────────────────────────────────────────────
 SOURCE (CODE)
]────────────────────────────────────────────────────────────────────────────────────────────────

In file: /home/fuzz/gpac2.1/gpac/src/filter_core/filter_pid.c
   5296
   5297 GF_EXPORT
   5298 GF_Err gf_filter_pid_set_property(GF_FilterPid *pid, u32 prop_4cc, const GF_PropertyValue
*value)
   5299 {
   5300         if (!prop_4cc) return GF_BAD_PARAM;
 ► 5301         return gf_filter_pid_set_property_full(pid, prop_4cc, NULL, NULL, value,
GF_FALSE);
   5302 }
   5303
   5304 GF_EXPORT
   5305 GF_Err gf_filter_pid_set_property_str(GF_FilterPid *pid, const char *name, const
GF_PropertyValue *value)
   5306 {
─────────────────────────────────────────────────────────────────────────────────────────────────
 STACK
]────────────────────────────────────────────────────────────────────────────────────────────────

00:0000│ rsp 0x7ffffffe8f30 ◂— 0x0
01:0008│     0x7ffffffe8f38 ◂— 0x0
02:0010│     0x7ffffffe8f40 —▸ 0x7ffffffe9030 —▸ 0x7ffff54af2c0 ◂— 0x6372636170672e /* '.gpacrc'
*/
03:0018│     0x7ffffffe8f48 —▸ 0x7ffffffe8f50 ◂— 0x41b58ab3
```

```
04:0020│ rbx 0x7fffffffe8f50 ◂— 0x41b58ab3
05:0028│     0x7fffffffe8f58 —▸ 0x7ffff5640eff ◂— '1 48 100 11 szName:5290'
06:0030│     0x7fffffffe8f60 —▸ 0x7ffff4b84110 (gf_filter_pid_set_property) ◂— endbr64
07:0038│     0x7fffffffe8f68 —▸ 0x618000000c80 —▸ 0x7ffff6de03e0 (FileInRegister) —▸ 0x7ffff56a6580
◂— 0x6e6966 /* 'fin' */
──────────────────────────────────────────────────────────────────────────────────────────────────────
 BACKTRACE
]─────────────────────────────────────────────────────────────────────────────────────────────────────

 ► f 0   0x7ffff4b841c6 gf_filter_pid_set_property+182
   f 1   0x7ffff4b841c6 gf_filter_pid_set_property+182
   f 2   0x7ffff4c06993 gf_filter_pid_raw_new+595
   f 3   0x7ffff4dc30b1 filein_process+2721
   f 4   0x7ffff4c0eb6d gf_filter_process_task+3581
   f 5   0x7ffff4bd4953 gf_fs_thread_proc+2275
   f 6   0x7ffff4be0c67 gf_fs_run+455
   f 7   0x7ffff462a677 gf_media_import+10263
──────────────────────────────────────────────────────────────────────────────────────────────────────

──────────────────────────────────────────────────────────────────────────────────────────────────────

pwndbg> bt
#0  gf_filter_pid_set_property_full (is_info=GF_FALSE, value=0x7fffffffe9150, dyn_name=0x0,
prop_name=0x0, prop_4cc=1347244884, pid=0x613000000040) at filter_core/filter_pid.c:5301
#1  gf_filter_pid_set_property (pid=pid@entry=0x613000000040, prop_4cc=prop_4cc@entry=1347244884,
value=0x7fffffffe9150) at filter_core/filter_pid.c:5301
#2  0x00007ffff4c06993 in gf_filter_pid_raw_new (filter=filter@entry=0x618000000c80,
url=0x603000000f40 "../../../test/segv2/poc", local_file=<optimized out>, mime_type=<optimized
out>, fext=<optimized out>, probe_data=<optimized out>, probe_size=<optimized out>, trust_mime=
<optimized out>, out_pid=<optimized out>) at filter_core/filter.c:3891
#3  0x00007ffff4dc30b1 in filein_process (filter=<optimized out>) at filters/in_file.c:481
#4  0x00007ffff4c0eb6d in gf_filter_process_task (task=0x607000000b10) at
filter_core/filter.c:2639
#5  0x00007ffff4bd4953 in gf_fs_thread_proc (sess_thread=sess_thread@entry=0x616000000110) at
filter_core/filter_session.c:1857
#6  0x00007ffff4be0c67 in gf_fs_run (fsess=fsess@entry=0x616000000080) at
filter_core/filter_session.c:2118
#7  0x00007ffff462a677 in gf_media_import (importer=importer@entry=0x7fffffffeaa50) at
media_tools/media_import.c:1226
#8  0x0000555555651a12 in convert_file_info (inName=<optimized out>, track_id=0x555555764fb0
<info_track_id>) at fileimport.c:130
#9  0x000055555562279f in mp4box_main (argc=<optimized out>, argv=<optimized out>) at
mp4box.c:6265
#10 0x00007ffff1949083 in __libc_start_main (main=0x5555555f6a00 <main>, argc=3,
argv=0x7fffffffe488, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>,
stack_end=0x7fffffffe478) at ../csu/libc-start.c:308
#11 0x00005555555f6afe in _start () at mp4box.c:6811
pwndbg> p pid
$2 = (GF_FilterPid *) 0x613000000040
pwndbg> c
Continuing.
[AVC|H264] Warning: Error parsing NAL unit

Breakpoint 1, gf_filter_pid_set_property_full (is_info=GF_FALSE, value=0x7fffffffe9810,
dyn_name=0x0, prop_name=0x0, prop_4cc=1146050121, pid=0x0) at filter_core/filter_pid.c:5301
5301            return gf_filter_pid_set_property_full(pid, prop_4cc, NULL, NULL, value,
GF_FALSE);
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
............
until.......

pwndbg> p pid
$3 = (GF_FilterPid *) 0x0
pwndbg> i b
Num     Type           Disp Enb Address            What
1       breakpoint     keep y   <MULTIPLE>
        breakpoint already hit 9 times
1.1                         y   0x00007ffff4b829f6 in gf_filter_pid_set_property_full at
filter_core/filter_pid.c:5250
1.2                         y   0x00007ffff4b8314e in gf_filter_pid_set_property_full at
filter_core/filter_pid.c:5250
1.3                         y   0x00007ffff4b834d1 in gf_filter_pid_set_property_full at
filter_core/filter_pid.c:5250
1.4                         y   0x00007ffff4b8393e in gf_filter_pid_set_property_full at
filter_core/filter_pid.c:5250
1.5                         y   0x00007ffff4b83cc1 in gf_filter_pid_set_property_full at
filter_core/filter_pid.c:5250
1.6                         y   0x00007ffff4b841c6 in gf_filter_pid_set_property_full at
filter_core/filter_pid.c:5250
pwndbg> n
filter_core/filter_pid.c:5250:6: runtime error: member access within null pointer of type 'struct
GF_FilterPid'
[Inferior 1 (process 2239158) exited with code 01]
```

source code

```
5246 static GF_Err gf_filter_pid_set_property_full(GF_FilterPid *pid, u32 prop_4cc, const char
*prop_name, char *dyn_name, const GF_PropertyValue *value, Bool is_info)
5247 {
5248    GF_PropertyMap *map;
5249    const GF_PropertyValue *oldp;
5250    if (PID_IS_INPUT(pid)) {    //**here**//
5251            GF_LOG(GF_LOG_ERROR, GF_LOG_FILTER, ("Attempt to write property on input PID in
filter %s - ignoring\n", pid->filter->name));
5252            return GF_BAD_PARAM;
5253    }
```

jeanlf closed this as completed in b43f9d1 on Jul 12

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant