New issue

Jump to bottom

A Null Pointer Dereference In function gf_filter_pck_get_data #1728

Closed **treebacker** opened this issue on Apr 2, 2021 · 0 comments

treebacker commented on Apr 2, 2021 • edited

In filters/reframe_latm.c:480. There is a Null Pointer Dereference, when call `gf_filter_pck_get_data` .
The first arg pck may be null with a crafted mp4 file.

As below code shows:
`

```
if (!pck) {
        if (gf_filter_pid_is_eos(ctx->ipid)) {  // check1
                if (!ctx->latm_buffer_size) {     // check2
                        if (ctx->opid)
                                gf_filter_pid_set_eos(ctx->opid);
                        if (ctx->src_pck) gf_filter_pck_unref(ctx->src_pck);
                        ctx->src_pck = NULL;
                        return GF_EOS;
                }
        } else {
                return GF_OK;
        }
}
```

Although there are checks to test if pck is null. But when check1 is true and check2 is false, the checks are nothing.
The command line:

```
ubuntu@VM-0-3-ubuntu:~[illegible]gpac_lasted/gpac$ ./bin/gcc/gpac --version
[Core] Cannot open directory "/home/ubuntu/treebacker/fuzzwork/dataset/tprogram/gpac-1.0.1/bin/gcc/" for enumeration: 2
Nothing to do, check usage "gpac -h"
gpac - GPAC command line filter engine - version 1.1.0-DEV-rev663-ga19a19e70-master
(c) 2000-2021 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

ubuntu@VM-0-3-ubuntu:~[illegible]dataset/tprogram/gpac_lasted/gpac$ ./bin/gcc/gpac -info ~/treebacker/fuzzwork/output_cve/gpac_last/uni
[Core] Cannot open directory "/home/ubuntu/treebacker/fuzzwork/dataset/tprogram/gpac-1.0.1/bin/gcc/" for enumeration: 2
ID3 tag detected size 1901568 but probe data only 1317 bytes, will rely on file extension (try increasing probe size using --block_size)
ID3 tag detected size 1901568 but probe data only 1317 bytes, will rely on file extension (try increasing probe size using --block_size)
PID 1 name bug1 Configure - properties:
        SourcePath: /home/ubuntu/treebacker/fuzzwork/output_cve/gpac_last/uniq/bug1
        URL: /home/ubuntu/treebacker/fuzzwork/output_cve/gpac_last/uniq/bug1
        MIMEType: audio/aac+latm
        Cached: true
        DownloadSize: 1317
        Duration: 2138/96000
        DataRef: true
        StreamType: Audio
        CodecID: MPEG-4 AAC Audio
        SamplesPerFrame: 1024
        Unframed: false
        PlaybackMode: forward
        Bitrate: 113870
        DecoderConfig: 2 bytes (CRC32 0x26BF89C5)
        ProfileLevel: 15
        SampleRate: 96000
        Timescale: 96000
        NumChannels: 1
PID 1 name bug1 Reconfigure after 1 packets - properties:
        SourcePath: /home/ubuntu/treebacker/fuzzwork/output_cve/gpac_last/uniq/bug1
        URL: /home/ubuntu/treebacker/fuzzwork/output_cve/gpac_last/uniq/bug1
        MIMEType: audio/aac+latm
        Cached: true
        DownloadSize: 1317
        Duration: 2138/96000
        DataRef: true
        StreamType: Audio
        CodecID: MPEG-4 AAC Audio
        SamplesPerFrame: 1024
        Unframed: false
        PlaybackMode: forward
        Bitrate: 113870
        DecoderConfig: 2 bytes (CRC32 0x26BF89C5)
        ProfileLevel: 15
        SampleRate: 96000
        Timescale: 96000
        NumChannels: 1
Segmentation fault
```

In gdb:

```
(gdb) c
Continuing.
PID 1 name bug1 Configure - properties:
        SourcePath: /home/ubuntu/treebacker/fuzzwork/output_cve/gpac_last/uniq/bug1
        URL: /home/ubuntu/treebacker/fuzzwork/output_cve/gpac_last/uniq/bug1
        MIMEType: audio/aac+latm
        Cached: true
        DownloadSize: 1317
        Duration: 2138/96000
        DataRef: true
        StreamType: Audio
        CodecID: MPEG-4 AAC Audio
        SamplesPerFrame: 1024
        Unframed: false
        PlaybackMode: forward
        Bitrate: 113870
        DecoderConfig: 2 bytes (CRC32 0x26BF89C5)
        ProfileLevel: 15
        SampleRate: 96000
        Timescale: 96000
        NumChannels: 1
PID 1 name bug1 Reconfigure after 1 packets - properties:
        SourcePath: /home/ubuntu/treebacker/fuzzwork/output_cve/gpac_last/uniq/bug1
        URL: /home/ubuntu/treebacker/fuzzwork/output_cve/gpac_last/uniq/bug1
        MIMEType: audio/aac+latm
        Cached: true
        DownloadSize: 1317
        Duration: 2138/96000
        DataRef: true
        StreamType: Audio
        CodecID: MPEG-4 AAC Audio
        SamplesPerFrame: 1024
        Unframed: false
        PlaybackMode: forward
        Bitrate: 113870
        DecoderConfig: 2 bytes (CRC32 0x26BF89C5)
        ProfileLevel: 15
        SampleRate: 96000
        Timescale: 96000
        NumChannels: 1

Breakpoint 1, latm_dmx_process (filter=0x73d4d0) at filters/reframe_latm.c:480
480             data = (char *) gf_filter_pck_get_data(pck, &pck_size);
(gdb) p pck
$3 = (GF_FilterPacket *) 0x0
(gdb) n

Program received signal SIGSEGV, Segmentation fault.
gf_filter_pck_get_data (pck=0x0, size=0x7fffffffc2c4) at filter_core/filter_pck.c:1279
1279            pck=pck->pck;
```

null pointer dereference

The crafted file:
bug1.zip

jeanlf closed this as completed in b2db2f9 on Apr 8, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant