

New issue

Jump to bottom

Segmentation fault casued by null pointer dereference using mp4box in naludmx_parse_nal_avc, reframe_nalu.c:2474 #1886

Closed

3 tasks done

Shadowblad3 opened this issue on Aug 24, 2021 · 1 comment

Shadowblad3 commented on Aug 24, 2021 • edited

- ☒ 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 ...).

Hi, there.

There is a segmentation fault caused by null pointer dereference in naludmx_parse_nal_avc, reframe_nalu.c:2474 in commit 592ba26 .

Here is my environment, compiler info and gpac version:

```
Distributor ID: Ubuntu
Description: Ubuntu 16.04.6 LTS
Release: 16.04
Codename: xenial
gcc: 5.4.0

MP4Box - GPAC version 1.1.0-DEV-rev1170-g592ba26-master
(c) 2000-2021 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io
MINI build (encoders, decoders, audio and video output disabled)

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: --static-bin --enable-debug
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_SOCK_UN GPAC_MINIMAL_ODF GPAC_HAS_QJS GPAC_HAS_FREETYPE GPAC_HAS_JPEG GPAC_HAS_PNG GPAC_DISABLE_3D
```

To reproduce, run

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


POC:

[poc.zip](#)
(unzip first)

Here is the trace reported by gdb:

```
#0 0x00000000008ac435 in naludmx_parse_nal_avc (ctx=0x1259a80, data=0x1239f73 "tr\372!", size=0xe, nal_type=0x14, skip_nal=0x7fffffff4fc4, is_slice=0x7fffffff4fd0, is_islice=0x7fffffff4fd4) at /mnt/data/playground/gpac/src/filters/reframe_nalu.c:2474
#1 0x00000000008ad7d3 in naludmx_process (filter=0x124cbe0) at /mnt/data/playground/gpac/src/filters/reframe_nalu.c:2874
#2 0x00000000007480a0 in gf_filter_process_task (task=0x123eee0) at /mnt/data/playground/gpac/src/filter_core/filter.c:2441
#3 0x000000000073798c in gf_fs_thread_proc (sess_thread=0x12382e0) at /mnt/data/playground/gpac/src/filter_core/filter_session.c:1640
#4 0x0000000000738305 in gf_fs_run (fsess=0x1238250) at /mnt/data/playground/gpac/src/filter_core/filter_session.c:1877
#5 0x00000000006571ea in gf_media_import (importer=0x7fffffff5bf0) at /mnt/data/playground/gpac/src/media_tools/media_import.c:1178
#6 0x000000000042cdf9 in convert_file_info (inName=0x7fffffff163 "tmp", trackID=0x0) at /mnt/data/playground/gpac/applications/mp4box/fileimport.c:128
#7 0x0000000000004168c3 in mp4boxMain (argc=0x7, argv=0x7fffffffddb8) at /mnt/data/playground/gpac/applications/mp4box/main.c:5925
#8 0x0000000000418d6b in main (argc=0x7, argv=0x7fffffffddb8) at /mnt/data/playground/gpac/applications/mp4box/main.c:6455
#9 0x0000000000c0aa06 in generic_start_main ()
#10 0x0000000000c0aaff5 in __libc_start_main ()
#11 0x0000000000403f39 in _start ()
```

aureliendavid added a commit that referenced this issue on Aug 24, 2021

 add some null guards to prevent segfaults ...


70607fc

aureliendavid commented on Aug 24, 2021

Contributor

closed by 70607fc

reopen if needed

 aureliendavid closed this as completed on Aug 24, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

