New issue

Jump to bottom

A integer (heap) overflow in function adts_dmx_process #1723

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

treebacker commented on Mar 29, 2021

In `filters/reframe_adts.c` , function `adts_dmx_process` .
There is a sub codes like as below:
`
size = ctx->hdr.frame_size - ctx->hdr.hdr_size;
offset = ctx->hdr.hdr_size;
.....
memcpy(output, sync + offset, size);
`
However, with crafted file, ctx->hdr.frame_size may be smaller than ctx->hdr.hdr_size.
So, the size may be a negative number, which results a heap overflow in memcpy.

In Command line:
gpac -info bug6

```
ubuntu@VM-0-3-ubuntu:~/[redacted]/gpac-1.0.1$ ./debug_bin/gcc/gpac -info ~/tr[redacted]e/gpac/uniq/bug6
Segmentation fault
```

In gdb:

```
Starting program: /[redacted]/gpac-1.0.1/debug_bin/gcc/gpac -info ~/t[redacted]e/gpac/uniq/bug6
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGSEGV, Segmentation fault.
__memmove_avx_unaligned_erms () at ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:435
435     ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S: No such file or directory.
(gdb) bt
#0  __memmove_avx_unaligned_erms () at ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:435
#1  0x00007ffff78bea6a in adts_dmx_process (filter=0x5555557a5d70) at filters/reframe_adts.c:715
#2  0x00007ffff77a79fc in gf_filter_process_task (task=0x555555794f40) at filter_core/filter.c:2158
#3  0x00007ffff7799b91 in gf_fs_thread_proc (sess_thread=0x5555557866c0) at filter_core/filter_session.c:1467
#4  0x00007ffff779a49a in gf_fs_run (fsess=0x555555786630) at filter_core/filter_session.c:1704
#5  0x000055555555e49c in gpac_main (argc=3, argv=0x5555557872b0) at main.c:2116
#6  0x000055555555e771 in main (argc=3, argv=0x7fffffffe8a8) at main.c:2171
(gdb) b filters/reframe_adts.c:715
Breakpoint 1 at 0x7ffff78bea4e: file filters/reframe_adts.c, line 715.
(gdb) r
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: [redacted]/debug_bin/gcc/gpac -info ~[redacted]e/gpac/uniq/bug6
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, adts_dmx_process (filter=0x5555557a5d70) at filters/reframe_adts.c:715
715                     memcpy(output, sync + offset, size);
(gdb) p size
$1 = 4294967290
(gdb) p ctx->hdr.frame_size
$2 = 1
(gdb) p  ctx->hdr.hdr_size
$3 = 7
(gdb) p output
$4 = (u8 *) 0x7ffef3946010 ""
(gdb) n

Program received signal SIGSEGV, Segmentation fault.
__memmove_avx_unaligned_erms () at ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:435
435     ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S: No such file or directory.
(gdb)
```

negative

heap overflow

The crafted file is in the attached zip:
bug6.zip

jeanlf added a commit that referenced this issue on Mar 29, 2021

`fixed potential crash in adts reframer with broken streams - cf #1723` ✓ 22774aa

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