

New issue

Jump to bottom

# heap buffer overflow issue with gpac MP4Box #1840

Closed dhbbb opened this issue on Jul 5, 2021 · 0 comments

dhbbb commented on Jul 5, 2021

Hello,  
A heap-buffer-overflow has occurred when running program MP4Box,which leads to a Deny of Service caused by dividing zero without sanity check,this can reproduce on the lattest commit.  
System info:  
Ubuntu 20.04.1 : clang 10.0.0 , gcc 9.3.0  
  
[poc.zip](#)  
  
file: media.c  
function:gf\_isom\_get\_3gpp\_audio\_esd  
line: 105  
As below code shows:

```
97         gf_bs_write_data(bs, "\\x41\\x6D\\x7F\\x5E\\x15\\xB1\\xD0\\x11\\xBA\\x91\\x00\\x80\\x5F\\xB4\\xB9\\x7E", 16);
98         gf_bs_write_u16_le(bs, 1);
99         memset(szName, 0, 80);
100        strcpy(szName, "QCELP-13K(GPAC-emulated)");
101        gf_bs_write_data(bs, szName, 80);
102        ent = &stbl->TimeToSample->entries[0];
103        sample_rate = entry->samplerate_hi;
104        block_size = ent ? ent->sampleDelta : 160;
105        gf_bs_write_u16_le(bs, 8*sample_size*sample_rate/block_size);    <----- block_size can be zero
106        gf_bs_write_u16_le(bs, sample_size);
107        gf_bs_write_u16_le(bs, block_size);
108        gf_bs_write_u16_le(bs, sample_rate);
109        gf_bs_write_u16_le(bs, entry->bitspersample);
110        gf_bs_write_u32_le(bs, sample_size ? 0 : 7);
```

Verification steps:  
1.Get the source code of gpac  
2.Compile

```
cd gpac-master
CC=gcc CXX=g++ CFLAGS="-fsanitize=address" CXXFLAGS="-fsanitize=address" ./configure
make
```

3.run MP4Box

```
./MP4Box -hint poc -out /dev/null
```

In Command line:

```
[iso file] Unknown box type esJs in parent enca
[iso file] Unknown box type stts in parent enca
[iso file] Box "enca" (start 1455) has 5 extra bytes
[iso file] Box "enca" is larger than container box
[iso file] Box "stds" size 171 (start 1439) invalid (read 192)
Floating point exception
```

gdb info

```

Program received signal SIGFPE, Arithmetic exception.
[-----registers-----]
RAX: 0x0
RBX: 0x5555555de770 --> 0x656e6361 ('acne')
RCX: 0x0
RDX: 0x0
RSI: 0x7fffffff8030 ("QCELP-13K(GPAC-emulated)")
RDI: 0x5555555dc7d0 --> 0x0
RBP: 0x7fffffff80d0 --> 0x5555555e0cb0 --> 0x3
RSP: 0x7fffffff7e30 --> 0x0
RIP: 0x7fffffff9ab0c7 (<Media_GetESD+3127>:      dlv   r15d)
R8 : 0xbb80
R9 : 0x200
R10: 0x7ffff7721439 ("gf_bs_write_u16_le")
R11: 0x7ffff77c13c0 (<gf_bs_write_u16_le>:      endbr64)
R12: 0x5555555dc7d0 --> 0x0
R13: 0x7fffffff8030 ("QCELP-13K(GPAC-emulated)")
R14: 0x0
R15: 0x0
EFLAGS: 0x10256 (carry PARITY ADJUST ZERO sign trap INTERRUPT direction overflow)
[-----code-----]
0x7ffff796b8bb <Media_GetESD+3115>: mov     DWORD PTR [rsp+0xc],r8d
0x7ffff796b8c0 <Media_GetESD+3120>: imul   eax,r8d
0x7ffff796b8c4 <Media_GetESD+3124>: shl    eax,0x3
=> 0x7ffff796b8c7 <Media_GetESD+3127>: dlv    r15d
0x7ffff796b8ca <Media_GetESD+3130>: mov     esi,eax
0x7ffff796b8cc <Media_GetESD+3132>: call   0x7ffff77b1fc0 <gf_bs_write_u16_le@plt>
0x7ffff796b8d1 <Media_GetESD+3137>: mov     esi,r14d
0x7ffff796b8d4 <Media_GetESD+3140>: mov     rdi,r12
[-----stack-----]
0000 0x7fffffff7e30 --> 0x0
0008 0x7fffffff7e30 --> 0xbb800000ff00
0016 0x7fffffff7e40 --> 0x0
0024 0x7fffffff7e40 --> 0xfffffffffffff00
0032 0x7fffffff7e50 --> 0x0
0040 0x7fffffff7e50 --> 0x0
0048 0x7fffffff7e60 ('.' <repeats 16 times>, "-W\035\003-W\035\003-W\035\003-W\035\004")
0056 0x7fffffff7e68 (".....-W\035\003-W\035\003-W\035\003-W\035\004")
[-----]
Legend: code, data, rodata, value
Stopped reason: SIGFPE

```

asan info

```

=====
==967870==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000001874 at pc 0x7f3a53c0836c bp 0x7ffcce36e790 sp 0x7ffcce36e780
READ of size 4 at 0x602000001874 thread T0
#0 0x7f3a53c0836b in gf_isom_get_3gpp_audio_esd isomedia/media.c:104
#1 0x7f3a53c0836b in Media_GetESD isomedia/media.c:330
#2 0x7f3a53b1ac04 in gf_isom_get_decoder_config isomedia/isom_read.c:1329
#3 0x7f3a53b56d2e in gf_isom_guess_specification isomedia/isom_read.c:4035
#4 0x5602827ad1d1 in HintFile /home/.../gpac/gpac-master-A/applications/mp4box/main.c:3379
#5 0x5602827c4d54 in mp4boxMain /home/.../gpac/gpac-master-A/applications/mp4box/main.c:6297
#6 0x7f3a52d080b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
#7 0x560282777fd1 in _start (/home/.../gpac/gpac-master-A/bin/gcc/MP4Box+0x48fd1)

0x602000001874 is located 3 bytes to the right of 1-byte region [0x602000001870,0x602000001871)
allocated by thread T0 here:
#0 0x7f3a53be6bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
#1 0x7f3a539e10ec in stts_box_read isomedia/box_code_base.c:5788

SUMMARY: AddressSanitizer: heap-buffer-overflow isomedia/media.c:104 in gf_isom_get_3gpp_audio_esd
Shadow bytes around the buggy address:
 0x0c047fff82b0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
 0x0c047fff82c0: fa fa fd fd fa fa fd fd fa fa fa fa fa fa 00 00
 0x0c047fff82d0: fa fa 01 fa fa fa 00 00 fa fa 00 00 fa fa 00 00
 0x0c047fff82e0: fa fa 00 00 fa fa 01 fa fa fa 00 00 fa fa 00 00
 0x0c047fff82f0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
->0x0c047fff8300: fa fa 00 00 fa fa 00 fa fa fa 00 00 fa fa[01]fa
 0x0c047fff8310: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 fa
 0x0c047fff8320: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
 0x0c047fff8330: fa fa 01 fa fa fa 00 00 fa fa 00 00 fa fa 00 00
 0x0c047fff8340: fa fa 00 00 fa fa fd fd fa fa fd fd fa fa fd fd
 0x0c047fff8350: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASAN internal: fe
Left alloca redzone: ca
Right alloca redzone: cb
Shadow gap: cc
==967870==ABORTING

```

 jeanlf closed this as completed in [6007c71](#) on Jul 5, 2021

Assignees

No one assigned

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

