New issue

Jump to bottom

heap-buffer-overflow in BitStreamWriter::flushBits #424

Closed   **cemonatk** opened this issue on May 22, 2021 · 1 comment

Labels   bug

cemonatk commented on May 22, 2021 • edited

Hi, please see asan output and poc file below.

Found by **Cem Onat Karagun of Diesec**

System info:
Ubuntu 21.04
tsMuxeR version git-f6ab2a2

To run PoC:

```
$ ./tsmuxer crash_2
```

```
tsMuxeR version git-f6ab2a2. github.com/justdan96/tsMuxer
This HEVC stream doesn't contain fps value. Muxing fps is absent too. Set muxing FPS to default 25.0 value.
HEVC manual defined fps doesn't equal to stream fps. Change HEVC fps from 0.181784 to 25
=================================================================
==2946348==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60400001eaf2 at pc 0x00000051552c bp 0x7ffc6a2a1220 sp 0x7ffc6a2a1218
READ of size 4 at 0x60400001eaf2 thread T0
    #0 0x51552b in BitStreamWriter::flushBits() /src/build/../tsMuxer/bitStream.h:224:37
    #1 0x51552b in HevcUnit::updateBits(int, int, int) /src/build/../tsMuxer/hevc.cpp:85:15
    #2 0x5263af in HEVCStreamReader::updateStreamFps(void*, unsigned char*, unsigned char*, int) /src/build/../tsMuxer/hevcStreamReader.cpp:364:10
    #3 0x72f351 in MPEGStreamReader::updateFPS(void*, unsigned char*, unsigned char*, int) /src/build/../tsMuxer/mpegStreamReader.cpp:310:9
    #4 0x52bfa4 in HEVCStreamReader::checkStream(unsigned char*, int) /src/build/../tsMuxer/hevcStreamReader.cpp:68:17
    #5 0x6d0b97 in METADemuxer::detectTrackReader(unsigned char*, int, AbstractStreamReader::ContainerType, int, int) /src/build/../tsMuxer/metaDemuxer.cpp:770:21
    #6 0x6c7255 in METADemuxer::DetectStreamReader(BufferedReaderManager&, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&, bool)
/src/build/../tsMuxer/metaDemuxer.cpp:684:35
    #7 0x5df87e in detectStreamReader(char const*, MPLSParser*, bool) /src/build/../tsMuxer/main.cpp:120:34
    #8 0x5efd05 in main /src/build/../tsMuxer/main.cpp:698:17
    #9 0x7fb676137564 in __libc_start_main csu/../csu/libc-start.c:332:16
    #10 0x2ebded in _start (/home/Fuzzer_Instance_49/txmux/tsMuxer/bin/tsMuxeR+0x2ebded)

0x60400001eaf5 is located 0 bytes to the right of 37-byte region [0x60400001ead0,0x60400001eaf5)
allocated by thread T0 here:
    #0 0x39823d in operator new[](unsigned long) (/home/Fuzzer_Instance_49/txmux/tsMuxer/bin/tsMuxeR+0x39823d)
    #1 0x514859 in HevcUnit::decodeBuffer(unsigned char const*, unsigned char const*) /src/build/../tsMuxer/hevc.cpp:40:19

SUMMARY: AddressSanitizer: heap-buffer-overflow /src/build/../tsMuxer/bitStream.h:224:37 in BitStreamWriter::flushBits()
Shadow bytes around the buggy address:
  0x0c087fffbd00: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c087fffbd10: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c087fffbd20: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c087fffbd30: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c087fffbd40: fa fa fd fd fd fd fd fa fa fa 00 00 00 00 00 00
=>0x0c087fffbd50: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00[05]fa
  0x0c087fffbd60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fffbd70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fffbd80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fffbd90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fffbda0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
==2946348==ABORTING
```

cemonatk commented on May 22, 2021   Author

crash_2.zip

jcdr428 mentioned this issue on May 22, 2021

[Bug] Buffer overflow with non-hevc stream #422

Merged

xavery pushed a commit that referenced this issue on Jun 9, 2021

```
[Bug] Buffer overflow with non-hevc stream (#422)   …
```

✓ d77ed5e

xavery closed this as completed on Jun 9, 2021

jcdr428 added the bug label on Jun 23

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants