New issue

Jump to bottom

heap-buffer-overflow in hevc.cpp:502:37 #436

Closed **cemonatk** opened this issue on May 27, 2021 · 0 comments

Labels bug

cemonatk commented on May 27, 2021

Hi, please see asan output and poc file below.

Found by **Cem Onat Karagun of Diesec**

As you can see on backtrace

```
hevc.cpp:502:37 is called after HevcSpsUnit::deserialize // hevc.cpp:872:17.
```

System info：

```
Ubuntu 21.04
tsMuxeR version git-f6ab2a2
```

To run PoC after unzip:

short_term_1.zip

```
$ ./tsmuxer short_term_1
```

Asan output:

```
tsMuxeR version git-f6ab2a2. github.com/justdan96/tsMuxer
=================================================================
==7825==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61700000dc10 at pc 0x000000510c90 bp 0x7ffd6ec5b000 sp 0x7ffd6ec5aff8
WRITE of size 1 at 0x61700000dc10 thread T0
    #0 0x510c8f in HevcSpsUnit::short_term_ref_pic_set(int) /src/build/../tsMuxer/hevc.cpp:502:37
    #1 0x50ce4c in HevcSpsUnit::deserialize() /src/build/../tsMuxer/hevc.cpp:872:17
    #2 0x52c0c0 in HEVCStreamReader::checkStream(unsigned char*, int) /src/build/../tsMuxer/hevcStreamReader.cpp:74:24
    #3 0x6d0b97 in METADemuxer::detectTrackReader(unsigned char*, int, AbstractStreamReader::ContainerType, int, int) /src/build/../tsMuxer/metaDemuxer.cpp:770:21
    #4 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
    #5 0x5df87e in detectStreamReader(char const*, MPLSParser*, bool) /src/build/../tsMuxer/main.cpp:120:34
    #6 0x5efd05 in main /src/build/../tsMuxer/main.cpp:698:17
    #7 0x7f70e9543564 in __libc_start_main csu/../csu/libc-start.c:332:16
    #8 0x2ebded in _start (/home/Fuzzer_Instance_39/txmux/tsMuxer/bin/tsMuxeR+0x2ebded)

0x61700000dc10 is located 0 bytes to the right of 656-byte region [0x61700000d980,0x61700000dc10)
allocated by thread T0 here:
    #0 0x39812d in operator new(unsigned long) (/home/Fuzzer_Instance_39/txmux/tsMuxer/bin/tsMuxeR+0x39812d)
    #1 0x50cb34 in __gnu_cxx::new_allocator<ShortTermRPS>::allocate(unsigned long, void const*) /usr/lib/gcc/x86_64-linux-
gnu/10/../../../../include/c++/10/ext/new_allocator.h:115:27
    #2 0x50cb34 in std::allocator_traits<std::allocator<ShortTermRPS> >::allocate(std::allocator<ShortTermRPS>&, unsigned long) /usr/lib/gcc/x86_64-linux-
gnu/10/../../../../include/c++/10/bits/alloc_traits.h:460:20
    #3 0x50cb34 in std::_Vector_base<ShortTermRPS, std::allocator<ShortTermRPS> >::_M_allocate(unsigned long) /usr/lib/gcc/x86_64-linux-
gnu/10/../../../../include/c++/10/bits/stl_vector.h:346:20
    #4 0x50cb34 in std::vector<ShortTermRPS, std::allocator<ShortTermRPS> >::_M_default_append(unsigned long) /usr/lib/gcc/x86_64-linux-
gnu/10/../../../../include/c++/10/bits/vector.tcc:635:34
    #5 0x50cb34 in std::vector<ShortTermRPS, std::allocator<ShortTermRPS> >::resize(unsigned long) /usr/lib/gcc/x86_64-linux-
gnu/10/../../../../include/c++/10/bits/stl_vector.h:940:4
    #6 0x50cb34 in HevcSpsUnit::deserialize() /src/build/../tsMuxer/hevc.cpp:869:16

SUMMARY: AddressSanitizer: heap-buffer-overflow /src/build/../tsMuxer/hevc.cpp:502:37 in HevcSpsUnit::short_term_ref_pic_set(int)
Shadow bytes around the buggy address:
  0x0c2e7fff9b30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff9b40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff9b50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff9b60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff9b70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2e7fff9b80: 00 00[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff9b90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff9ba0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff9bb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff9bc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff9bd0: 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
==7825==ABORTING
```

jcdr428 mentioned this issue on May 30, 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 22

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants