

[New issue](#)[Jump to bottom](#)

## heap-buffer-overflow in bitStream.h:58:61 #432

🔒 Closed cemonatk opened this issue on May 27, 2021 · 0 commentsLabels 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

```
bitStream.h:58:61 is called after HevcHdrUnit::deserialize // hevc.cpp:995:39.
```

System info:

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

To run PoC after unzip:

[getCurVal\\_3.zip](#)

```
$ ./tsmuxer getCurVal_3
```

Asan output:

```
tsMuxeR version git-f6ab2a2. github.com/justdan96/tsMuxer
=====
==7777==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x612000020fde at pc 0x00000042ca17 bp 0x7ffc8ba3e270 sp 0x7ffc8ba3e268
READ of size 1 at 0x612000020fde thread T0
#0 0x42ca16 in BitStreamReader::getCurVal(unsigned int*) /src/build/./tsMuxer/bitStream.h:58:61
#1 0x42ca16 in BitStreamReader::getBits(unsigned int) /src/build/./tsMuxer/bitStream.h:87:24
#2 0x50a120 in HevcHdrUnit::deserialize() /src/build/./tsMuxer/hevc.cpp:995:39
#3 0x52bb4a in HEVCStreamReader::checkStream(unsigned char*, int) /src/build/./tsMuxer/hevcStreamReader.cpp:88:24
#4 0x6d0b97 in METADemuxer::detectTrackReader(unsigned char*, int, AbstractStreamReader::ContainerType, int, int) /src/build/./tsMuxer/metaDemuxer.cpp:770:21
#5 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
#6 0x5df87e in detectStreamReader(char const*, MPLSParser*, bool) /src/build/./tsMuxer/main.cpp:120:34
#7 0x5efd05 in main /src/build/./tsMuxer/main.cpp:698:17
#8 0x7fe506733564 in __libc_start_main csu/../csu/libc-start.c:332:16
#9 0x2ebded in _start (/home/Fuzzer_Instance_21/tmux/tsMuxer/bin/tsMuxeR+0x2ebded)

0x612000020fde is located 0 bytes to the right of 286-byte region [0x612000020ec0,0x612000020fde)
allocated by thread T0 here:
#0 0x39823d in operator new[](unsigned long) (/home/Fuzzer_Instance_21/tmux/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:58:61 in BitStreamReader::getCurVal(unsigned int*)
Shadow bytes around the buggy address:
 0x0c247fffc1a0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
 0x0c247fffc1b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c247fffc1c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa fa
 0x0c247fffc1d0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
 0x0c247fffc1e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c247fffc1f0: 00 00 00 00 00 00 00 00 00 00 00 00[06]fa fa fa fa
 0x0c247fffc200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c247fffc210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c247fffc220: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c247fffc230: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c247fffc240: 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
==7777==ABORTING
```

jcdr428 mentioned this issue on May 30, 2021

[bug] Buffer overflow when SEI payloadSize > bits left #439

1 - Merged

 xavery closed this as completed in [8028fb8](#) on Jun 9, 2021

  jcd428 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

2 participants

