New issue

Jump to bottom

A global-buffer-overflow in hevcdecoderconfigrecord.cpp:311:37 #86

Closed seviezhou opened this issue on Aug 4, 2020 · 1 comment

seviezhou commented on Aug 4, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), heif (latest master 2fc78e)

Configure

cmake ../srcs -DCMAKE_CXX_FLAGS="-fsanitize=address -g" -DCMAKE_C_FLAGS="-fsanitize=address -g" -DCMAKE_EXE_LINKER_FLAGS="-fsanitize=address"

Command line

modify example.cpp, use example7() to receive filename from commandline.

./build/bin/example @@

AddressSanitizer output

```
=================================================================
==13667==ERROR: AddressSanitizer: global-buffer-overflow on address 0x000000953646 at pc 0x0000008202aa bp 0x7fff634d9ae0 sp 0x7fff634d9ad8
READ of size 2 at 0x000000953646 thread T0
    #0 0x8202a9 in HevcDecoderConfigurationRecord::getPicWidth() const /home/seviezhou/heif/srcs/common/hevcdecoderconfigrecord.cpp:311:37
    #1 0x8826a9 in HEIF::WriterImpl::getConfigIndex(HEIF::DecoderConfigId, unsigned short&) /home/seviezhou/heif/srcs/writer/writermetaimpl.cpp:1199:70
    #2 0x87e1bf in HEIF::WriterImpl::addImage(HEIF::MediaDataId const&, HEIF::ImageId&) /home/seviezhou/heif/srcs/writer/writermetaimpl.cpp:199:31
    #3 0x52072f in main /home/seviezhou/heif/srcs/examples/example.cpp:104:29
    #4 0x7f2f25a0083f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #5 0x41f0b8 in _start (/home/seviezhou/heif/build/bin/example+0x41f0b8)

0x000000953646 is located 26 bytes to the left of global variable 'subHeightC' defined in '/home/seviezhou/heif/srcs/common/hevcdecoderconfigrecord.cpp:316:20' (0x953660) of size 8
0x000000953646 is located 30 bytes to the right of global variable 'subWidthC' defined in '/home/seviezhou/heif/srcs/common/hevcdecoderconfigrecord.cpp:310:20' (0x953620) of size 8
SUMMARY: AddressSanitizer: global-buffer-overflow /home/seviezhou/heif/srcs/common/hevcdecoderconfigrecord.cpp:311:37 in HevcDecoderConfigurationRecord::getPicWidth() const
Shadow bytes around the buggy address:
  0x000080122670: f9 f9 f9 f9 00 00 00 00 00 00 00 00 00 00 00 00
  0x000080122680: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 f9 f9
  0x000080122690: f9 f9 f9 f9 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801226a0: 00 00 00 00 00 00 07 f9 f9 f9 f9 f9 00 00 00 00
  0x0000801226b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0000801226c0: 00 00 00 00 00 f9 f9 f9[f9]f9 f9 f9 00 f9 f9 f9
  0x0000801226d0: f9 f9 f9 f9 00 00 00 00 01 f9 f9 f9 f9 f9 f9 f9
  0x0000801226e0: 00 00 00 00 00 00 00 00 00 02 f9 f9 f9 f9 f9 f9
  0x0000801226f0: 00 00 00 00 00 00 00 00 00 00 f9 f9 f9 f9 f9 f9
  0x000080122700: 00 00 00 02 f9 f9 f9 f9 00 00 00 f9 f9 f9 f9 f9
  0x000080122710: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==13667==ABORTING
```

POC

global-overflow-getPicWidth-hevcdecoderconfigrecord-311.zip

lassehe commented on Aug 12, 2020 Collaborator

Thank you for reporting this. The issue was fixed in commit b26a708 .

lassehe closed this as completed on Aug 12, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants