New issue

Jump to bottom

SEGV in box.cc:2408 #138

Closed **strongcourage** opened this issue on Jul 27, 2019 · 2 comments

strongcourage commented on Jul 27, 2019

Hi,

I found a bug on the latest commit `fd0c01d` on master.
PoC: https://github.com/strongcourage/PoCs/blob/master/libheif_fd0c01d/PoC_segv_box.cc:2408
Command: examples/heif-convert $PoC /tmp/out.png
ASAN says:

```
==16874==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000050 (pc 0x00000048143c bp 0x7ffc1ade73a0 sp 0x7ffc1ade7370 T0)
    #0 0x48143b in std::vector<heif::Box_iref::Reference, std::allocator<heif::Box_iref::Reference> >::begin() const /usr/include/c++/5/bits/stl_vector.h:557
    #1 0x475604 in heif::Box_iref::get_references(unsigned int, unsigned int) const ../../libheif/box.cc:2408
    #2 0x4293b6 in heif::HeifContext::get_id_of_non_virtual_child_image(unsigned int, unsigned int&) const ../../libheif/heif_context.cc:816
    #3 0x42979a in heif::HeifContext::Image::get_luma_bits_per_pixel() const ../../libheif/heif_context.cc:839
    #4 0x40c1a4 in heif_image_handle_get_luma_bits_per_pixel ../../libheif/heif.cc:455
    #5 0x4060fc in main ../../examples/heif_convert.cc:209
    #6 0x7f1ac522d82f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #7 0x404f68 in _start (/home/dungnguyen/PoCs/libheif_fd0c01d/heif-convert-asan+0x404f68)
```

Thanks,
Manh Dung

fancycode closed this as completed in `f7399b6` on Aug 2, 2019

fancycode commented on Aug 2, 2019 Member

Thanks for reporting!

fgeek commented on Jul 26, 2021

CVE-2020-19499 has been assigned for this issue.

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants