New issue

Jump to bottom

Floating point exception #139

Closed **strongcourage** opened this issue on Jul 28, 2019 · 5 comments

strongcourage commented on Jul 28, 2019

Hi,

I found a FPE bug on the latest commit `fd0c01d` on master.
PoC: https://github.com/strongcourage/PoCs/blob/master/libheif_fd0c01d/PoC_fpe_box.cc:62
Command: examples/heif-info $PoC
Valgrind says:

```
==1112== Process terminating with default action of signal 8 (SIGFPE)
==1112==  Integer divide by zero at address 0x80362AC81
==1112==    at 0x528354: Fraction (box.cc:62)
==1112==    by 0x528354: operator- (box.cc:100)
==1112==    by 0x528354: heif::Box_clap::get_height_rounded() const (box.cc:2263)
==1112==    by 0x48F697: heif::HeifContext::interpret_heif_file() (heif_context.cc:696)
==1112==    by 0x49A40A: heif::HeifContext::read_from_file(char const*) (heif_context.cc:351)
==1112==    by 0x40859F: heif_context_read_from_file (heif.cc:184)
==1112==    by 0x404290: main (heif_info.cc:145)
Floating point exception
```

Thanks,
Manh Dung

fancycode commented on Aug 2, 2019 Member

@farindk Could you please take a look? The same probably applies to the other `XXX_rounded` methods in `Box_clap`.

farindk commented on Aug 2, 2019 Contributor

Thanks for this very strange edge case :-)
Fixed in `5c3dff7`

farindk closed this as completed on Aug 2, 2019

fancycode commented on Aug 2, 2019 Member

No longer crashes but now triggers an undefined behavior error (unfortunately not more output):

```
box.cc:123:43: runtime error: signed integer overflow: -2147483647 * 2 cannot be represented in type 'int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior box.cc:123:43 in
```

farindk commented on Aug 2, 2019 Contributor

Let's just limit the resolution of the Fractions to get around all of these numeric edge cases:
`2710c93`

fgeek commented on Jul 26, 2021

CVE-2020-19498 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

4 participants