New issue

Jump to bottom

buffer overflow #334

Closed **lxumei** opened this issue on Aug 20, 2020 · 4 comments

lxumei commented on Aug 20, 2020 • edited

Reproduce steps:

1. compile provided test.c
2. run command: `./test poc`

Stack trace:

```
#0  __GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1  0x00007ffff6fb08b1 in __GI_abort () at abort.c:79
#2  0x00007ffff6ff9907 in __libc_message (action=action@entry=(do_abort | do_backtrace),
    fmt=fmt@entry=0x7ffff7126be8 "*** %s ***: %s terminated\n") at ../sysdeps/posix/libc_fatal.c:181
#3  0x00007ffff70a4eaf in __GI___fortify_fail_abort (need_backtrace=need_backtrace@entry=0x1,
    msg=msg@entry=0x7ffff7126b65 "buffer overflow detected") at fortify_fail.c:33
#4  0x00007ffff70a4ed1 in __GI___fortify_fail (msg=msg@entry=0x7ffff7126b65 "buffer overflow detected") at fortify_fail.c:44
#5  0x00007ffff70a2bc0 in __GI___chk_fail () at chk_fail.c:28
#6  0x00007ffff70a1e52 in __strcpy_chk (dest=dest@entry=0x7ffffff43e08 "",
    src=src@entry=0x7ffffff43354 "!\v", '!' <repeats 30 times>, "H\001\006", destlen=destlen@entry=0x20) at strcpy_chk.c:30
#7  0x00007ffff7ac6134 in strcpy (__src=0x7ffffff43354 "!\v", '!' <repeats 30 times>, "H\001\006", __dest=0x7ffffff43e08 "")
    at /usr/include/x86_64-linux-gnu/bits/string_fortified.h:90
#8  LibRaw::parseHassyModel (this=this@entry=0x7ffffff43250) at src/metadata/hasselblad_model.cpp:136
#9  0x00007ffff7ab7fa8 in LibRaw::GetNormalizedModel (this=this@entry=0x7ffffff43250) at src/metadata/normalize_model.cpp:723
#10 0x00007ffff7a86c18 in LibRaw::identify (this=this@entry=0x7ffffff43250) at src/metadata/identify.cpp:1003
#11 0x00007ffff7b43f9e in LibRaw::open_datastream (this=0x7ffffff43250, stream=0x55555576a230) at src/utils/open.cpp:390
#12 0x00007ffff7b4c90d in LibRaw::open_buffer (this=0x7ffffff43250, buffer=0x555555769130, size=0xe1) at src/utils/open.cpp:153
#13 0x000055555555534b in LLVMFuzzerTestOneInput (data=0x555555769130 "II*", size=0xe1) at runlibraw.c:35
#14 0x000055555554f0a in main (argc=argc@entry=0x2, argv=argv@entry=0x7fffffffe3c8) at runlibraw.c:100
#15 0x00007ffff6f91b97 in __libc_start_main (main=0x555555554e00 <main(int, char**)>, argc=0x2, argv=0x7fffffffe3c8,
    init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe3b8) at ../csu/libc-start.c:310
#16 0x000055555555502a in _start ()
```

Poc:
poc.tar.gz

lxumei closed this as completed on Aug 20, 2020

lxumei mentioned this issue on Aug 23, 2020

segmentation fault in LibRaw::parse_tiff_ifd #335

Closed

LibRaw commented on Aug 24, 2020 • edited — Owner

This one:
fixed by this: 78d323e

limburgher commented on Sep 24, 2020

That's a link to the fix for #335, is that the same?

LibRaw commented on Sep 24, 2020 — Owner

335 is not libraw error but compiler error.

limburgher commented on Sep 24, 2020

Ok, thank you!

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development

No branches or pull requests

3 participants