# Abort in SingleComponentLSScan::ParseMCU #75

Closed sleicasper opened this issue on Jun 8 · 1 comment

**sleicasper** commented on Jun 8

## stack trace

```
_____________________________________________________________________________________

pwndbg> bt
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
#1  0x00007ffff7053859 in __GI_abort () at abort.c:79
#2  0x00007ffff7053729 in __assert_fail_base (fmt=0x7ffff71e9588 "%s%s%s:%u: %s%sAssertion `%s'
failed.\n%n", assertion=0x5555564a4120 <str> "lines > 0", file=0x5555564a4040 <str>
"singlecomponentlsscan.cpp", line=100, function=<optimized out>) at assert.c:92
#3  0x00007ffff7064fd6 in __GI___assert_fail (assertion=0x5555564a4120 <str> "lines > 0",
file=0x5555564a4040 <str> "singlecomponentlsscan.cpp", line=100, function=0x5555564a4080
<__PRETTY_FUNCTION__._ZN21SingleComponentLSScan8ParseMCUEv> "virtual bool
SingleComponentLSScan::ParseMCU()") at assert.c:101
#4  0x00005555558189f0 in SingleComponentLSScan::ParseMCU (this=0x624000002120) at
singlecomponentlsscan.cpp:100
#5  0x000055555567a528 in JPEG::ReadInternal (this=<optimized out>, this@entry=0x61b000000098,
tags=tags@entry=0x7fffffffd5a0) at jpeg.cpp:345
#6  0x0000555555677709 in JPEG::Read (this=0x61b000000098, tags=0x7fffffffce10) at jpeg.cpp:210
#7  0x000055555560ff53 in Reconstruct (infile=<optimized out>, outfile=<optimized out>,
colortrafo=<optimized out>, alpha=<optimized out>, upsample=<optimized out>) at
reconstruct.cpp:121
#8  0x00005555555c350e in main (argc=<optimized out>, argv=<optimized out>) at main.cpp:747
#9  0x00007ffff7055083 in __libc_start_main (main=0x5555555bafe0 <main(int, char**)>, argc=3,
argv=0x7fffffffe318, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>,
stack_end=0x7fffffffe308) at ../csu/libc-start.c:308
#10 0x00005555555b55ae in _start ()
```

## poc

poc.zip

## reproduce

- run `./jpeg ./poc /dev/null`

**thorfdbg** commented on Jun 8 Owner

Fixed - thank you.

**thorfdbg** closed this as completed on Jun 8

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants