

[New issue](#)[Jump to bottom](#)

# null pointer dereference in Component::SubXOf in component.hpp #73

✓ Closed sleicasper opened this issue on May 30 · 2 comments

sleicasper commented on May 30

## reproduce steps

1. compile libjpeg with address sanitizer
2. run ./jpeg ./poc /dev/null

## poc

[poc.zip](#)

## stack trace

```
=====
==3114171==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000c (pc 0x562098ed89e0 bp
0x7ffc18eca130 sp 0x7ffc18eca120 T0)
==3114171==The signal is caused by a READ memory access.
==3114171==Hint: address points to the zero page.
#0 0x562098ed89df in Component::SubXOf() const ../marker/component.hpp:145
#1 0x562098f2a796 in PredictiveScan::FindComponentDimensions()
/home/casper/targets/struct/libjpeg_th/source/SRC/codestream/predictivescan.cpp:113
#2 0x562098f2b7b3 in LosslessScan::StartParseScan(ByteStream*, Checksum*, BufferCtrl*)
/home/casper/targets/struct/libjpeg_th/source/SRC/codestream/losslessscan.cpp:111
#3 0x562098f61d3c in Scan::StartParseScan(ByteStream*, Checksum*, BufferCtrl*)
/home/casper/targets/struct/libjpeg_th/source/SRC/marker/scan.cpp:981
#4 0x562098f553fe in Frame::StartParseScan(ByteStream*, Checksum*)
/home/casper/targets/struct/libjpeg_th/source/SRC/marker/frame.cpp:847
#5 0x562098eda266 in JPEG::ReadInternal(JPG_TagItem*)
/home/casper/targets/struct/libjpeg_th/source/SRC/interface/jpeg.cpp:296
#6 0x562098ed9779 in JPEG::Read(JPG_TagItem*)
/home/casper/targets/struct/libjpeg_th/source/SRC/interface/jpeg.cpp:210
#7 0x562098ebd38 in Reconstruct(char const*, char const*, int, char const*, bool)
/home/casper/targets/struct/libjpeg_th/source/SRC/cmd/reconstruct.cpp:121
```

```
#8 0x562098eacea9 in main /home/casper/targets/struct/libjpeg_th/source/SRC/cmd/main.cpp:747
#9 0x7fbacbbb3082 in __libc_start_main ../csu/libc-start.c:308
#10 0x562098ea99ad in _start (/home/casper/targets/struct/libjpeg_th/source/SRC/jpeg+0x459ad)
```


AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV ../marker/component.hpp:145 in Component::SubXOf() const  
==3114171==ABORTING

✉ **thorfdbg** commented on May 30

Owner

Thanks, has been addressed and fixed.

 **thorfdbg** closed this as completed on May 31

**thorfdbg** commented on May 31

Owner

Done.

#### Assignees

No one assigned

#### Labels

None yet

#### Projects

None yet

#### Milestone

No milestone

#### Development

No branches or pull requests

2 participants

