New issue

Jump to bottom

null pointer dereference in LineBuffer::FetchRegion in linebuffer.cpp #74

Closed sleicasper opened this issue on May 31 · 1 comment

sleicasper commented on May 31

stack trace

```
jpeg Copyright (C) 2012-2018 Thomas Richter, University of Stuttgart
and Accusoft

For license conditions, see README.license for details.

*** Warning -1038 in Tables::ParseTables, line 1386, file tables.cpp
*** Reason is: found invalid marker, probably a marker size is out of range

*** Warning -1038 in Tables::ParseTables, line 1386, file tables.cpp
*** Reason is: found invalid marker, probably a marker size is out of range

*** Warning -1038 in Tables::ParseTables, line 1386, file tables.cpp
*** Reason is: found invalid marker, probably a marker size is out of range

*** Warning -1038 in Frame::StartParseHiddenScan, line 869, file frame.cpp
*** Reason is: Start of Scan SOS marker missing

*** Warning -1038 in Frame::ParseTrailer, line 1084, file frame.cpp
*** Reason is: missing an EOI marker at the end of the stream

*** Warning -1038 in Image::ParseTrailer, line 1463, file image.cpp
*** Reason is: expecting an EOI marker at the end of the stream

AddressSanitizer:DEADLYSIGNAL
=================================================================
==3119686==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x55f759202a0f bp
0x7ffdc6846690 sp 0x7ffdc6846660 T0)
==3119686==The signal is caused by a READ memory access.
==3119686==Hint: address points to the zero page.
    #0 0x55f759202a0e in LineBuffer::FetchRegion(int, Line const*, int*)
/home/casper/targets/struct/libjpeg_th/source/SRC/control/linebuffer.cpp:322
    #1 0x55f75921a1ed in LineBitmapRequester::ReconstructRegion(RectAngle<int> const&,
```

```
RectangleRequest const*)
/home/casper/targets/struct/libjpeg_th/source/SRC/control/linebitmaprequester.cpp:565
    #2 0x55f758f3aa7d in Image::ReconstructRegion(BitMapHook*, RectangleRequest const*)
/home/casper/targets/struct/libjpeg_th/source/SRC/codestream/image.cpp:1111
    #3 0x55f758f232a9 in JPEG::InternalDisplayRectangle(JPG_TagItem*)
/home/casper/targets/struct/libjpeg_th/source/SRC/interface/jpeg.cpp:721
    #4 0x55f758f22f99 in JPEG::DisplayRectangle(JPG_TagItem*)
/home/casper/targets/struct/libjpeg_th/source/SRC/interface/jpeg.cpp:699
    #5 0x55f758f06399 in Reconstruct(char const*, char const*, int, char const*, bool)
/home/casper/targets/struct/libjpeg_th/source/SRC/cmd/reconstruct.cpp:331
    #6 0x55f758ef2ea9 in main /home/casper/targets/struct/libjpeg_th/source/SRC/cmd/main.cpp:747
    #7 0x7fa22d05d082 in __libc_start_main ../csu/libc-start.c:308
    #8 0x55f758eef9ad in _start (/home/casper/targets/struct/libjpeg_th/source/SRC/jpeg+0x459ad)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV
/home/casper/targets/struct/libjpeg_th/source/SRC/control/linebuffer.cpp:322 in
LineBuffer::FetchRegion(int, Line const*, int*)
==3119686==ABORTING
```

poc:

poc.zip

reproduce:

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

thorfdbg commented on May 31 — Owner

Thanks, has been fixed.

thorfdbg closed this as completed on May 31

Assignees

No one assigned

Labels

None yet

Projects

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants