**Vulnerability Disclosure – Poppler library (latest version)**

**Title:** Denial of Service (crash) due to access Null pointer when parsing an illegal pdf file.

**Vendor:** Open Source (<https://poppler.freedesktop.org/> )

**Affected Product name(s) and versions:** Poppler latest version including 0.54.0 and before

Software that use poppler library, e.g: Evince

Evince (<https://wiki.gnome.org/Apps/Evince>)

**Platform used (OS):** Linux – Ubuntu 16.04 x86\_64

**Summary of the issue:**

Perf\_test utility will crash (segmentation fault) when parsing an illegal PDF file due to the program access a null pointer.

**Example output:**

./ perf-test ~/poc/heap-buffer-overflow-619405/poc.pdf

started: /home/root/poc/heap-buffer-overflow-619405/poc.pdf

load splash: 0.00 ms

page count: 1

ASAN:DEADLYSIGNAL

=================================================================

==96731==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000028 (pc 0x7f2da9eccb81 bp 0x0c2600001b86 sp 0x7ffcd31999b0 T0)

#0 0x7f2da9eccb80 (/home/root/poppler/build\_clang/libpoppler.so.67+0x5d2b80)

#1 0x7f2da9ec46a1 (/home/root/poppler/build\_clang/libpoppler.so.67+0x5ca6a1)

#2 0x7f2da9ec3a67 (/home/root/poppler/build\_clang/libpoppler.so.67+0x5c9a67)

#3 0x7f2da9e44b78 (/home/root/poppler/build\_clang/libpoppler.so.67+0x54ab78)

#4 0x7f2da9c448c1 (/home/root/poppler/build\_clang/libpoppler.so.67+0x34a8c1)

#5 0x7f2da9c090d5 (/home/root/poppler/build\_clang/libpoppler.so.67+0x30f0d5)

#6 0x7f2da9c27164 (/home/root/poppler/build\_clang/libpoppler.so.67+0x32d164)

#7 0x7f2da9c261d1 (/home/root/poppler/build\_clang/libpoppler.so.67+0x32c1d1)

#8 0x7f2da9d293f8 (/home/root/poppler/build\_clang/libpoppler.so.67+0x42f3f8)

#9 0x7f2da9d290fa (/home/root/poppler/build\_clang/libpoppler.so.67+0x42f0fa)

#10 0x7f2da9d32ece (/home/root/poppler/build\_clang/libpoppler.so.67+0x438ece)

#11 0x4f08a3 (/home/root/poppler/build\_clang/test/perf-test+0x4f08a3)

#12 0x7f2da868782f (/lib/x86\_64-linux-gnu/libc.so.6+0x2082f)

#13 0x419fb8 (/home/root/poppler/build\_clang/test/perf-test+0x419fb8)

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV (/home/root/poppler/build\_clang/libpoppler.so.67+0x5d2b80)

==96731==ABORTING

**Debug info:**

Program received signal SIGSEGV, Segmentation fault.

0x00007ffff797fb81 in JPXStream::readUByte (x=0x28, this=<optimized out>) at /home/root/poppler/poppler/JPXStream.cc:3351

3351 \*x = (Guint)c0;

(gdb) bt

#0 0x00007ffff797fb81 in JPXStream::readUByte (x=0x28, this=<optimized out>) at /home/root/poppler/poppler/JPXStream.cc:3351

#1 JPXStream::readCodestream (this=<optimized out>, len=<optimized out>) at /home/root/poppler/poppler/JPXStream.cc:1205

#2 0x00007ffff79776a2 in JPXStream::readBoxes (this=<optimized out>) at /home/root/poppler/poppler/JPXStream.cc:780

#3 0x00007ffff7976a68 in JPXStream::reset (this=0x61300000db00) at /home/root/poppler/poppler/JPXStream.cc:275

#4 0x00007ffff78f7b79 in SplashOutputDev::drawImage (this=0x61300000dcc0, state=<optimized out>, ref=<optimized out>, str=0x61300000db00, width=999, height=999, colorMap=<optimized out>,

interpolate=<optimized out>, maskColors=0x40, inlineImg=240) at /home/root/poppler/poppler/SplashOutputDev.cc:3556

#5 0x00007ffff76f78c2 in Gfx::doImage (this=<optimized out>, ref=0x7fffffffd320, str=<optimized out>,

inlineImg=<error reading variable: access outside bounds of object referenced via synthetic pointer>) at /home/root/poppler/poppler/Gfx.cc:4711

#6 0x00007ffff76bc0d6 in Gfx::opXObject (this=0x611000009a00, args=<optimized out>, numArgs=<optimized out>) at /home/root/poppler/poppler/Gfx.cc:4213

#7 0x00007ffff76da165 in Gfx::go (this=<optimized out>, topLevel=<error reading variable: access outside bounds of object referenced via synthetic pointer>) at /home/root/poppler/poppler/Gfx.cc:767

#8 0x00007ffff76d91d2 in Gfx::display (this=<optimized out>, obj=<optimized out>, topLevel=<error reading variable: access outside bounds of object referenced via synthetic pointer>)

at /home/root/poppler/poppler/Gfx.cc:729

#9 0x00007ffff77dc3f9 in Page::displaySlice (this=0x611000009b40, out=<optimized out>, hDPI=72, vDPI=5.2727351433383131e-310, rotate=0, useMediaBox=<optimized out>, crop=<optimized out>, sliceX=-1,

sliceY=<optimized out>, sliceW=<optimized out>, sliceH=<optimized out>, printing=<optimized out>, abortCheckCbk=<optimized out>, abortCheckCbkData=<optimized out>,

annotDisplayDecideCbk=<optimized out>, annotDisplayDecideCbkData=<optimized out>, copyXRef=<optimized out>) at /home/root/poppler/poppler/Page.cc:601

#10 0x00007ffff77dc0fb in Page::display (this=0x60200002def4, out=0x40, hDPI=-1.8325506472120096e-06, vDPI=9.3872472709836843e-322, rotate=2, useMediaBox=<optimized out>, crop=<optimized out>,

printing=<optimized out>, abortCheckCbk=0x0, abortCheckCbkData=0x0, annotDisplayDecideCbk=0x0, annotDisplayDecideCbkData=0x0, copyXRef=<optimized out>) at /home/root/poppler/poppler/Page.cc:521

#11 0x00007ffff77e5ecf in PDFDoc::displayPage (this=0x60f00000ef50, out=0x61300000dcc0, page=1, hDPI=<optimized out>, vDPI=<optimized out>, rotate=0, useMediaBox=false, crop=true,

printing=<optimized out>, abortCheckCbk=<optimized out>, abortCheckCbkData=<optimized out>, annotDisplayDecideCbk=<optimized out>, annotDisplayDecideCbkData=<optimized out>, copyXRef=<optimized out>)

at /home/root/poppler/poppler/PDFDoc.cc:491

#12 0x00000000004f08a4 in PdfEnginePoppler::renderBitmap (pageNo=<optimized out>, zoomReal=100, rotation=0, this=<optimized out>) at /home/root/poppler/test/perf-test.cc:452

#13 RenderPdf (fileName=<optimized out>) at /home/root/poppler/test/perf-test.cc:941

#14 RenderFile (fileName=<optimized out>) at /home/root/poppler/test/perf-test.cc:970

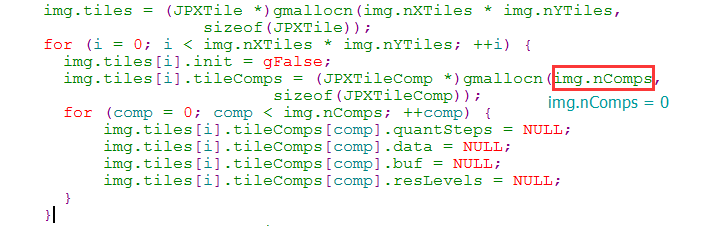
#15 RenderCmdLineArg (cmdLineArg=<optimized out>) at /home/root/poppler/test/perf-test.cc:1224

#16 main (argc=<optimized out>, argv=<optimized out>) at /home/root/poppler/test/perf-test.cc:1269

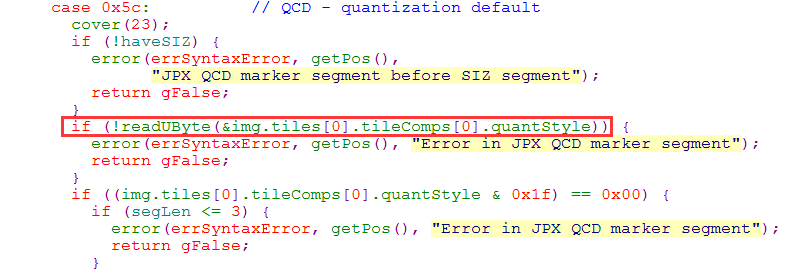
**Explanation:**

The problem stems from assigning Null pointer to img.tiles[0].tileComps. (JPXStream.cc:readCodestream:993) The program try to assign a value to img.tiles[0].tileComps[0].quanStyle in function readCodeStream in JPXStream.cc file.

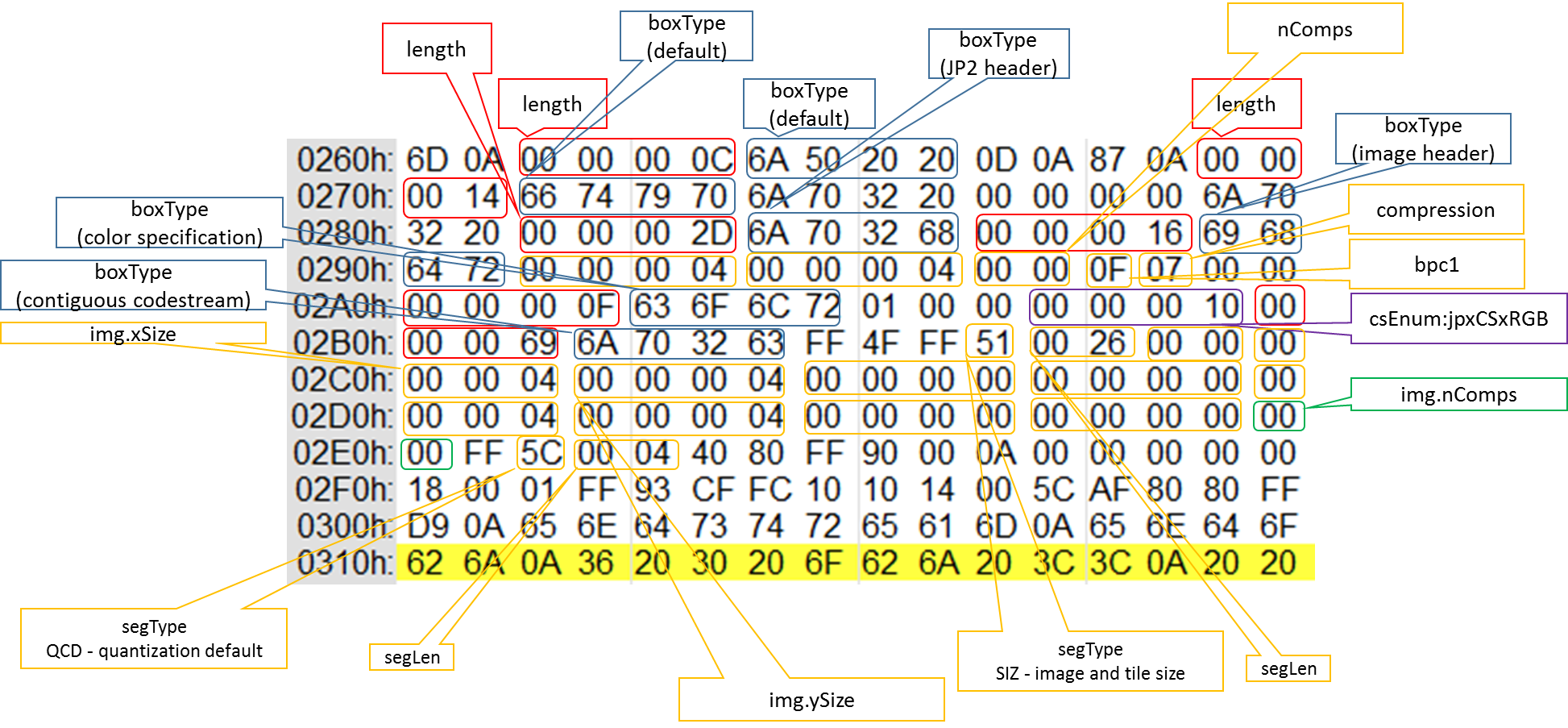
The program checks whether nComps equals img.nComps or not in line 963, but it does not check whether img.nComps equals 0 or not.



Pic 1. Assigning null to img.tiles[0].tileComps



Pic 2. Trying to assign a value to img.tiles[0].tileComps[0].quanStyle



Pic 3: filed of part of PoC file

**Suggestion for patch:**

Add condition check for img.nComps equals 0 or not. If img.nComps == 0, just return gFalse.

**Credits:** Young\_X from VARAS@IIE