Segmentation fault in xpdf-4.04/xpdf/TextOutputDev.cc:988 in TextLine::TextLine()

Post Reply Search this topic… 4 posts • Page **1** of **1**

elvadisas

Segmentation fault in xpdf-4.04/xpdf/TextOutputDev.cc:988 in TextLine::TextLine()

Mon Apr 25, 2022 11:56 pm

Hello,
In Xpdf 4.04, I crashed pdftotext with the provided test case.There is a Segmentation fault on pdftotext. It can be triggered by sending a crafted PDF file to the pdftotext(verson 4.0.4) binary.

Enviroment:
--Tested on Ubuntu 20.04.2 LTS x86_64,AFL++
--gcc version 9.3.0
--xpdf version xpdf 4.04
https://dl.xpdfreader.com/xpdf-4.04.tar.gz

run in the terminal:

```
gdb --args $HOME/fuzzing_xpdf/install/bin/pdftotext $HOME/fuzzing_xpdf/test/poc1 $HOME/fuzzing_xpdf/output
```

The stack straces are as follow:

```
Program received signal SIGSEGV, Segmentation fault.
0x000000000050154d in TextLine::TextLine (this=<optimized out>, wordsA=<optimized out>,
wordsA@entry=0x6030000101b0, xMinA=xMinA@entry=0, yMinA=yMinA@entry=0, xMaxA=xMaxA@entry=0,
yMaxA=yMaxA@entry=0, fontSizeA=fontSizeA@entry=0)
at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:988
988 hyphenated = text[len - 1] == (Unicode)'-';
(gdb) bt
#0 0x000000000050154d in TextLine::TextLine (this=<optimized out>, wordsA=<optimized out>,
wordsA@entry=0x6030000101b0, xMinA=xMinA@entry=0, yMinA=yMinA@entry=0, xMaxA=xMaxA@entry=0,
yMaxA=yMaxA@entry=0,
fontSizeA=fontSizeA@entry=0) at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:988
#1 0x0000000000541917 in TextPage::buildLine (this=<optimized out>, this@entry=0x612000000640, charsA=<optimized
out>, charsA@entry=0x603000010180, rot=<optimized out>, xMin=<optimized out>, yMin=<optimized out>,
xMax=<optimized out>, yMax=<optimized out>) at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:5162
#2 0x000000000053f260 in TextPage::buildLine (this=this@entry=0x612000000640, blk=blk@entry=0x606000004340) at
/home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:5084
#3 0x000000000053eab2 in TextPage::buildLines (this=this@entry=0x612000000640, blk=0x606000004340,
lines=lines@entry=0x603000010150, splitSuperLines=splitSuperLines@entry=0)
at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:4884
#4 0x000000000053e9dc in TextPage::buildLines (this=this@entry=0x612000000640, blk=<optimized out>,
blk@entry=0x6060000041c0, lines=lines@entry=0x603000010150, splitSuperLines=splitSuperLines@entry=0)
at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:4892
#5 0x000000000053c2e0 in TextPage::buildColumn (this=this@entry=0x612000000640, blk=blk@entry=0x6060000041c0) at
```

```
/home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:4708
#6 0x000000000053c1d6 in TextPage::buildColumns2 (this=this@entry=0x612000000640, blk=0x6060000041c0,
columns=columns@entry=0x603000010120, primaryLR=primaryLR@entry=1)
at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:4678
#7 0x000000000053c11c in TextPage::buildColumns2 (this=this@entry=0x612000000640, blk=<optimized out>,
blk@entry=0x606000005120, columns=columns@entry=0x603000010120, primaryLR=primaryLR@entry=1)
at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:4690
#8 0x000000000050a6b5 in TextPage::buildColumns (this=0x612000000640, tree=0x606000005120, primaryLR=1) at
/home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:4666
#9 TextPage::writeReadingOrder (this=0x612000000640, outputStream=outputStream@entry=0x615000001200,
outputFunc=outputFunc@entry=0x550c10 <outputToFile(void*, char const*, int)>, uMap=uMap@entry=0x606000001dc0,
space=space@entry=0x7fffffffdde0 " ", spaceLen=spaceLen@entry=1, eol=0x7fffffffde00 "\n6\340E", eolLen=1) at
/home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:1754
#10 0x000000000050a0d9 in TextPage::write (this=<optimized out>, outputStream=<optimized out>, outputFunc=
<optimized out>) at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/TextOutputDev.cc:1686
#11 0x0000000000602264 in Gfx::~Gfx (this=0x60f0000008b0) at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/Gfx.cc:618
#12 0x000000000075700b in Page::displaySlice (this=<optimized out>, out=<optimized out>, hDPI=<optimized out>, vDPI=
<optimized out>, rotate=<optimized out>, useMediaBox=<optimized out>, crop=<optimized out>, sliceX=<optimized out>,
sliceY=<optimized out>, sliceW=<optimized out>, sliceH=<optimized out>, printing=<optimized out>, abortCheckCbk=
<optimized out>, abortCheckCbkData=<optimized out>) at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/Page.cc:455
#13 0x00000000007563f2 in Page::display (this=0xfffffffffffffffc, out=0x8, hDPI=-1.8325506472120096e-06, vDPI=0,
rotate=8193, useMediaBox=0, crop=-134463488, printing=<optimized out>, abortCheckCbk=0x0, abortCheckCbkData=0x0)
at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/Page.cc:368
#14 0x00000000007659af in PDFDoc::displayPage (this=<optimized out>, out=<optimized out>, page=1, hDPI=<optimized
out>, vDPI=<optimized out>, rotate=<optimized out>, useMediaBox=<optimized out>, crop=<optimized out>,
printing=<optimized out>, abortCheckCbk=<optimized out>, abortCheckCbkData=<optimized out>) at
/home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/PDFDoc.cc:442
#15 PDFDoc::displayPages (this=<optimized out>, out=<optimized out>, firstPage=<optimized out>, lastPage=<optimized
out>, hDPI=<optimized out>, vDPI=<optimized out>, rotate=<optimized out>, useMediaBox=<optimized out>,
crop=<optimized out>, printing=<optimized out>, abortCheckCbk=<optimized out>, abortCheckCbkData=<optimized out>)
at /home/elva/fuzzing_xpdf/xpdf-4.04/xpdf/PDFDoc.cc:460
#16 0x00000000005564b0 in main (argc=<optimized out>, argv=<optimized out>) at /home/elva/fuzzing_xpdf/xpdf-
4.04/xpdf/pdftotext.cc:306
```

you can reproduced the bug by the follow step:

```
cmake -DCMAKE_BUILD_TYPE=Debug $HOME/fuzzing_xpdf/xpdf-4.04 -
DCMAKE_INSTALL_PREFIX=$HOME/fuzzing_xpdf/install/ -DCMAKE_CXX_COMPILER=afl-clang-fast++

AFL_USE_ASAN=1 make
Sudo AFL_USE_ASAN=1 make install

$HOME/fuzzing_xpdf/install/bin/pdftotext $HOME/fuzzing_xpdf/test/poc1 $HOME/fuzzing_xpdf/output
```

you can download this POC file at ATTACHMENTS
Thank you.

ATTACHMENTS

poc1.rar
(1.06 KiB) Downloaded 194 times

derekn

Re: Segmentation fault in xpdf-4.04/xpdf/TextOutputDev.cc:988 in TextLine::TextLine()

Mon May 02, 2022 9:02 pm

That was a bug in the text extractor, related to characters drawn at very large y coordinates.
I'll have it fixed in the next release.

Thanks for the bug report.

H00K1998

Sun Jun 19, 2022 4:04 am

Hello friend, can you tell me how to apply for that CVE number? My email is 2023128485@qq.com thank you 😕

Last edited by H00K1998 on Mon Jun 20, 2022 8:43 am, edited 1 time in total.

H00K1998

Re: Segmentation fault in xpdf-4.04/xpdf/TextOutputDev.cc:988 in TextLine::TextLine()

Sun Jun 19, 2022 4:04 am

CVE-2022-30524

Post Reply

4 posts • Page **1** of **1**

‹ Return to “Xpdf open source”

Jump to

Board index

Delete cookies All times are UTC