New issue

Jump to bottom

bug found in swftools-pdf2swf #182

Open **Cvjark** opened this issue on Jul 3 · 0 comments

Cvjark commented on Jul 3 • edited

Hi, I currently learn to use fuzz tech to detect bugs and I found something in this repo.
in order to reproduce the crash info, please attach ASAN when you compile this repo.

heap buffer overflow

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id3_heap_buffer_overflow.zip

crash info

```
==71111==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62100004fce8 at pc
0x00000063ce64 bp 0x7ffdb8f7dab0 sp 0x7ffdb8f7daa8
READ of size 1 at 0x62100004fce8 thread T0
    #0 0x63ce63 in DCTStream::readHuffSym(DCTHuffTable*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2825:14
    #1 0x638c4a in DCTStream::readDataUnit(DCTHuffTable*, DCTHuffTable*, int*, int*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2345:17
    #2 0x634338 in DCTStream::readMCURow()
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2129:9
    #3 0x632e98 in DCTStream::getChar() /home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2040:12
    #4 0x60e023 in ImageStream::getLine()
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:373:25
    #5 0x60dd51 in ImageStream::getPixel(unsigned char*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:344:5
    #6 0x7c9dc5 in VectorGraphicOutputDev::drawGeneralImage(GfxState*, Object*, Stream*, int, int,
GfxImageColorMap*, int, int, int, int*, Stream*, int, int, int, GfxImageColorMap*)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1303:12
    #7 0x7ccc45 in VectorGraphicOutputDev::drawImage(GfxState*, Object*, Stream*, int, int,
```

```
GfxImageColorMap*, int*, int) /home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1430:5
    #8 0x71dc57 in Gfx::doImage(Object*, Stream*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3664:12
    #9 0x6ec5e0 in Gfx::opXObject(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3336:7
    #10 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #11 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #12 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #13 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #14 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #15 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #16 0x5f87d5 in render2(_gfxpage*, _gfxdevice*, int, int, int, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:164:14
    #17 0x5f8e64 in pdfpage_rendersection(_gfxpage*, _gfxdevice*, double, double, double, double,
double, double) /home/bupt/Desktop/swftools/lib/pdf/pdf.cc:190:5
    #18 0x501816 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:832:3
    #19 0x7f645bf2ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #20 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

Address 0x62100004fce8 is a wild pointer.
SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2825:14 in
DCTStream::readHuffSym(DCTHuffTable*)
Shadow bytes around the buggy address:
  0x0c4280001f40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280001f50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280001f60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280001f70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280001f80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c4280001f90: fa fa fa fa fa fa fa fa fa fa fa fa fa[fa]fa fa
  0x0c4280001fa0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280001fb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280001fc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280001fd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280001fe0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
```

```
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==71111==ABORTING
```

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id175_heap_buffer_overflow.zip

crash info

```
==50683==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x608000000280 at pc
0x000000751637 bp 0x7ffe2a4712c0 sp 0x7ffe2a4712b8
READ of size 8 at 0x608000000280 thread T0
    #0 0x751636 in GfxICCBasedColorSpace::getDefaultColor(GfxColor*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/GfxState.cc:923:9
    #1 0x6f5e8e in Gfx::opSetFillColorSpace(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:1163:17
    #2 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #3 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #4 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #5 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #6 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int (*)
(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #7 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #8 0x5fcfff in pdf_open(_gfxsource*, char const*)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:542:14
    #9 0x500300 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:738:26
    #10 0x7f363dd8ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #11 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

0x608000000280 is located 0 bytes to the right of 96-byte region [0x608000000220,0x608000000280)
allocated by thread T0 here:
    #0 0x4f8d28 in operator new(unsigned long) /home/bupt/æ¡Œé¢/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_new_delete.cpp:99
    #1 0x7497ce in GfxICCBasedColorSpace::parse(Array*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/GfxState.cc:890:8
    #2 0x745a62 in GfxColorSpace::parse(Object*, StreamColorSpaceMode)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/GfxState.cc:134:12
```

```
    #3 0x6f5da4 in Gfx::opSetFillColorSpace(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc
    #4 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3

SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/lib/pdf/xpdf/GfxState.cc:923:9 in
GfxICCBasedColorSpace::getDefaultColor(GfxColor*)
Shadow bytes around the buggy address:
  0x0c107fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 02 fa
  0x0c107fff8010: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 fa
  0x0c107fff8020: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c107fff8030: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c107fff8040: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c107fff8050:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c107fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==50683==ABORTING
```

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id293_heap_buffer_overflow.zip

crash info

```
==60167==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x604000003080 at pc
0x00000092ceba bp 0x7ffe40762c20 sp 0x7ffe40762c18
WRITE of size 8 at 0x604000003080 thread T0
    #0 0x92ceb9 in draw_stroke /home/bupt/Desktop/swftools/lib/gfxpoly/stroke.c:212:24
    #1 0x92e224 in gfxpoly_from_stroke /home/bupt/Desktop/swftools/lib/gfxpoly/stroke.c:226:5
    #2 0x90989c in polyops_stroke /home/bupt/Desktop/swftools/lib/devices/polyops.c:229:23
    #3 0x7c1563 in VectorGraphicOutputDev::strokeGfxline(GfxState*, _gfxline*, int)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:612:9
    #4 0x7cd69e in VectorGraphicOutputDev::stroke(GfxState*)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1487:5
    #5 0x6eeffa in Gfx::opStroke(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:1415:12
    #6 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #7 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #8 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #9 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #10 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #11 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #12 0x5f87d5 in render2(_gfxpage*, _gfxdevice*, int, int, int, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:164:14
    #13 0x5f8e64 in pdfpage_rendersection(_gfxpage*, _gfxdevice*, double, double, double, double,
double, double) /home/bupt/Desktop/swftools/lib/pdf/pdf.cc:190:5
    #14 0x501816 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:832:3
    #15 0x7f15d7322c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #16 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

0x604000003080 is located 0 bytes to the right of 48-byte region [0x604000003050,0x604000003080)
allocated by thread T0 here:
    #0 0x4b3160 in malloc /home/bupt/æ¡Œé¢/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x92c94f in draw_stroke /home/bupt/Desktop/swftools/lib/gfxpoly/stroke.c:192:26

SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/lib/gfxpoly/stroke.c:212:24 in draw_stroke
Shadow bytes around the buggy address:
  0x0c087fff85c0: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fd
  0x0c087fff85d0: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fd
  0x0c087fff85e0: fa fa fd fd fd fd fd fd fa fa 00 00 00 00 00 00
  0x0c087fff85f0: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
  0x0c087fff8600: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 00
=>0x0c087fff8610:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8620: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8630: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8640: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8650: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff8660: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
```

```
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==60167==ABORTING
```

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id305_heap-buffer-overflow.zip

crash info

```
==8869==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x621000035ae8 at pc
0x00000062399c bp 0x7ffdb53cd5e0 sp 0x7ffdb53cd5d8
WRITE of size 8 at 0x621000035ae8 thread T0
    #0 0x62399b in DCTStream::reset() /home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:1994:15
    #1 0x60dc99 in ImageStream::reset() /home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:337:8
    #2 0x7c82aa in VectorGraphicOutputDev::drawGeneralImage(GfxState*, Object*, Stream*, int, int,
GfxImageColorMap*, int, int, int, int*, Stream*, int, int, int, GfxImageColorMap*)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1183:11
    #3 0x7ccc45 in VectorGraphicOutputDev::drawImage(GfxState*, Object*, Stream*, int, int,
GfxImageColorMap*, int*, int) /home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1430:5
    #4 0x71dc57 in Gfx::doImage(Object*, Stream*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3664:12
    #5 0x6ec5e0 in Gfx::opXObject(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3336:7
    #6 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #7 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #8 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #9 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #10 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int
```

```
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #11 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #12 0x5f87d5 in render2(_gfxpage*, _gfxdevice*, int, int, int, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:164:14
    #13 0x5f8e64 in pdfpage_rendersection(_gfxpage*, _gfxdevice*, double, double, double, double,
double, double) /home/bupt/Desktop/swftools/lib/pdf/pdf.cc:190:5
    #14 0x501816 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:832:3
    #15 0x7f2c3ecc8c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #16 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

0x621000035ae8 is located 0 bytes to the right of 4584-byte region [0x621000034900,0x621000035ae8)
allocated by thread T0 here:
    #0 0x4f8d28 in operator new(unsigned long) /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_new_delete.cpp:99
    #1 0x60ccb7 in Stream::makeFilter(char*, Stream*, Object*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:239:11
    #2 0x60b856 in Stream::addFilters(Object*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:112:11
    #3 0x65fa23 in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Parser.cc:203:14
    #4 0x65d23e in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Parser.cc:94:18
    #5 0x65375a in XRef::fetch(int, int, Object*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/XRef.cc:823:13
    #6 0x6501de in Object::fetch(XRef*, Object*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Object.cc:106:16

SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:1994:15 in DCTStream::reset()
Shadow bytes around the buggy address:
  0x0c427fffeb00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffeb10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffeb20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffeb30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffeb40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c427fffeb50: 00 00 00 00 00 00 00 00 00 00 00 00 00[fa]fa fa
  0x0c427fffeb60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffeb70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffeb80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffeb90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffeba0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
```

```
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==8869==ABORTING
```

stack_buffer_overflow

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id100_stack_buffer_overflow.zip

crash info

```
==43189==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffe33ffbdc4 at pc
0x00000060df33 bp 0x7ffe33ffbc50 sp 0x7ffe33ffbc48
WRITE of size 1 at 0x7ffe33ffbdc4 thread T0
    #0 0x60df32 in ImageStream::getPixel(unsigned char*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:348:12
    #1 0x7c9dc5 in VectorGraphicOutputDev::drawGeneralImage(GfxState*, Object*, Stream*, int, int,
GfxImageColorMap*, int, int, int, int*, Stream*, int, int, int, GfxImageColorMap*)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1303:12
    #2 0x7ccc45 in VectorGraphicOutputDev::drawImage(GfxState*, Object*, Stream*, int, int,
GfxImageColorMap*, int*, int) /home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1430:5
    #3 0x71dc57 in Gfx::doImage(Object*, Stream*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3664:12
    #4 0x6ec5e0 in Gfx::opXObject(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3336:7
    #5 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #6 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #7 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #8 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #9 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int (*)
(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #10 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #11 0x5f87d5 in render2(_gfxpage*, _gfxdevice*, int, int, int, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:164:14
```

```
    #12 0x5f8e64 in pdfpage_rendersection(_gfxpage*, _gfxdevice*, double, double, double, double,
double, double) /home/bupt/Desktop/swftools/lib/pdf/pdf.cc:190:5
    #13 0x501816 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:832:3
    #14 0x7f6be3d6fc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #15 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

Address 0x7ffe33ffbdc4 is located in stack of thread T0 at offset 292 in frame
    #0 0x7c774f in VectorGraphicOutputDev::drawGeneralImage(GfxState*, Object*, Stream*, int, int,
GfxImageColorMap*, int, int, int, int*, Stream*, int, int, int, GfxImageColorMap*)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1127

  This frame has 19 object(s):
    [32, 40) 'x1' (line 1130)
    [64, 72) 'y1' (line 1130)
    [96, 104) 'x2' (line 1130)
    [128, 136) 'y2' (line 1130)
    [160, 168) 'x3' (line 1130)
    [192, 200) 'y3' (line 1130)
    [224, 232) 'x4' (line 1130)
    [256, 264) 'y4' (line 1130)
    [288, 292) 'pixBuf' (line 1132) <== Memory access at offset 292 overflows this variable
    [304, 316) 'rgb' (line 1133)
    [336, 416) 'color_transform' (line 1137)
    [448, 456) 'buf' (line 1146)
    [480, 736) 'pal' (line 1151)
    [800, 804) 'gray' (line 1155)
    [816, 824) 'buf94' (line 1188)
    [848, 856) 'buf173' (line 1228)
    [880, 1904) 'pal179' (line 1231)
    [2032, 2044) 'rgb180' (line 1232)
    [2064, 3088) 'pal486' (line 1340)
HINT: this may be a false positive if your program uses some custom stack unwind mechanism,
swapcontext or vfork
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:348:12 in ImageStream::getPixel(unsigned char*)
Shadow bytes around the buggy address:
  0x1000467f7760: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000467f7770: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000467f7780: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1000467f7790: 00 00 00 00 f1 f1 f1 f1 00 f2 f2 f2 00 f2 f2 f2
  0x1000467f77a0: 00 f2 f2 f2 00 f2 f2 f2 00 f2 f2 f2 00 f2 f2 f2
=>0x1000467f77b0: 00 f2 f2 f2 00 f2 f2 f2[04]f2 00 04 f2 f2 00 00
  0x1000467f77c0: 00 00 00 00 00 00 00 00 f2 f2 f2 f2 f8 f2 f2 f2
  0x1000467f77d0: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8
  0x1000467f77e0: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8
  0x1000467f77f0: f2 f2 f2 f2 f2 f2 f2 f2 f8 f2 f8 f2 f2 f2 f8 f2
  0x1000467f7800: f2 f2 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
```

```
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==43189==ABORTING
```

global-buffer-overflow

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id7_global_buffer_overflow.zip

crash info

```
==71185==ERROR: AddressSanitizer: global-buffer-overflow on address 0x000001818502 at pc
0x00000063a7bf bp 0x7ffe36636f40 sp 0x7ffe36636f38
READ of size 1 at 0x000001818502 thread T0
    #0 0x63a7be in DCTStream::transformDataUnit(unsigned short*, int*, unsigned char*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2804:18
    #1 0x634382 in DCTStream::readMCURow()
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2135:4
    #2 0x632e98 in DCTStream::getChar() /home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2040:12
    #3 0x60e023 in ImageStream::getLine()
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:373:25
    #4 0x60dd51 in ImageStream::getPixel(unsigned char*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:344:5
    #5 0x7c9dc5 in VectorGraphicOutputDev::drawGeneralImage(GfxState*, Object*, Stream*, int, int,
GfxImageColorMap*, int, int, int, int*, Stream*, int, int, int, GfxImageColorMap*)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1303:12
    #6 0x7ccc45 in VectorGraphicOutputDev::drawImage(GfxState*, Object*, Stream*, int, int,
GfxImageColorMap*, int*, int) /home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1430:5
    #7 0x71dc57 in Gfx::doImage(Object*, Stream*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3664:12
    #8 0x6ec5e0 in Gfx::opXObject(Object*, int)
```

```
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3336:7
    #9 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #10 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #11 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #12 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #13 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #14 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #15 0x5f87d5 in render2(_gfxpage*, _gfxdevice*, int, int, int, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:164:14
    #16 0x5f8e64 in pdfpage_rendersection(_gfxpage*, _gfxdevice*, double, double, double, double,
double, double) /home/bupt/Desktop/swftools/lib/pdf/pdf.cc:190:5
    #17 0x501816 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:832:3
    #18 0x7f2cb74a3c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #19 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

0x000001818502 is located 30 bytes to the left of global variable 'zoomtowidth' defined in
'pdf.cc:26:12' (0x1818520) of size 4
0x000001818502 is located 30 bytes to the right of global variable 'threadsafe' defined in
'pdf.cc:29:12' (0x18184e0) of size 4
SUMMARY: AddressSanitizer: global-buffer-overflow
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2804:18 in
DCTStream::transformDataUnit(unsigned short*, int*, unsigned char*)
Shadow bytes around the buggy address:
  0x0000802fb050: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000802fb060: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000802fb070: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000802fb080: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 00 f9 f9 f9
  0x0000802fb090: f9 f9 f9 f9 00 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9
=>0x0000802fb0a0:[f9]f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9 01 f9 f9 f9
  0x0000802fb0b0: f9 f9 f9 f9 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000802fb0c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000802fb0d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000802fb0e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000802fb0f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
```

```
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==71185==ABORTING
```

SEGV

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id0_SEGV.zip

crash info

```
Error: PDF file is damaged - attempting to reconstruct xref table...
AddressSanitizer:DEADLYSIGNAL

==71049==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x0000008293e7 bp
0x7ffe8c3e6990 sp 0x7ffe8c3e6700 T0)
==71049==The signal is caused by a READ memory access.
==71049==Hint: address points to the zero page.
    #0 0x8293e7 in FoFiTrueType::writeTTF(void (*)(void*, char*, int), void*, char*, unsigned
short*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/FoFiTrueType.cc:910:24
    #1 0x8d28a9 in SplashFTFontEngine::loadTrueTypeFont(SplashFontFileID*, char*, int, unsigned
short*, int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/SplashFTFontEngine.cc:160:7
    #2 0x8c1fa5 in SplashFontEngine::loadTrueTypeFont(SplashFontFileID*, char*, int, unsigned
short*, int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/SplashFontEngine.cc:255:26
    #3 0x88430a in SplashOutputDev::doUpdateFont(GfxState*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/SplashOutputDev.cc:1130:36
    #4 0x8060a8 in InfoOutputDev::updateFont(GfxState*)
/home/bupt/Desktop/swftools/lib/pdf/InfoOutputDev.cc:577:13
    #5 0x6f27c5 in Gfx::opShowText(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3038:10
    #6 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #7 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #8 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #9 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #10 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #11 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
```

```
    #12 0x5fcfff in pdf_open(_gfxsource*, char const*)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:542:14
    #13 0x500300 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:738:26
    #14 0x7f971e94dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #15 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/swftools/lib/pdf/xpdf/FoFiTrueType.cc:910:24 in
FoFiTrueType::writeTTF(void (*)(void*, char*, int), void*, char*, unsigned short*)
==71049==ABORTING
```

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id76_SEGV.zip

crash info

```
==41269==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x00000091bf07 bp 0x7fff9910e150 sp
0x7fff9910dfa0 T0)
==41269==The signal is caused by a READ memory access.
==41269==Hint: this fault was caused by a dereference of a high value address (see register values
below).  Disassemble the provided pc to learn which register was used.
    #0 0x91bf07 in convert_gfxline /home/bupt/Desktop/swftools/lib/gfxpoly/convert.c:31:18
    #1 0x91bf07 in gfxpoly_from_fill /home/bupt/Desktop/swftools/lib/gfxpoly/convert.c:250:5
    #2 0x90a161 in polyops_fill /home/bupt/Desktop/swftools/lib/devices/polyops.c:247:22
    #3 0x7c3e1b in VectorGraphicOutputDev::fillGfxLine(GfxState*, _gfxline*, char)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:627:5
    #4 0x7c3e1b in VectorGraphicOutputDev::endString(GfxState*)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:805:6
    #5 0x71bb67 in Gfx::doShowText(GString*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3300:10
    #6 0x6f28e5 in Gfx::opShowText(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3042:3
    #7 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #8 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #9 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #10 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #11 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #12 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #13 0x5f87d5 in render2(_gfxpage*, _gfxdevice*, int, int, int, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:164:14
```

```
    #14 0x5f8e64 in pdfpage_rendersection(_gfxpage*, _gfxdevice*, double, double, double, double,
double, double) /home/bupt/Desktop/swftools/lib/pdf/pdf.cc:190:5
    #15 0x501816 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:832:3
    #16 0x7fa199df7c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #17 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/swftools/lib/gfxpoly/convert.c:31:18 in
convert_gfxline
==41269==ABORTING
```

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id87_SEGV.zip

crash info

```
==41858==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x0000008e4b57 bp 0x7ffe72186f50 sp
0x7ffe72186e20 T0)
==41858==The signal is caused by a READ memory access.
==41858==Hint: this fault was caused by a dereference of a high value address (see register values
below).  Disassemble the provided pc to learn which register was used.
    #0 0x8e4b57 in gfxline_getbbox /home/bupt/Desktop/swftools/lib/gfxtools.c:765:11
    #1 0x7c200e in VectorGraphicOutputDev::clipToGfxLine(GfxState*, _gfxline*, char)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:636:22
    #2 0x7c439f in VectorGraphicOutputDev::endTextObject(GfxState*)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:829:2
    #3 0x6ed08a in Gfx::opEndText(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:2931:8
    #4 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #5 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #6 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #7 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #8 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int (*)
(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #9 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #10 0x5f87d5 in render2(_gfxpage*, _gfxdevice*, int, int, int, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:164:14
    #11 0x5f8e64 in pdfpage_rendersection(_gfxpage*, _gfxdevice*, double, double, double, double,
double, double) /home/bupt/Desktop/swftools/lib/pdf/pdf.cc:190:5
    #12 0x501816 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:832:3
    #13 0x7fa23073cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
```

```
start.c:310
    #14 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/swftools/lib/gfxtools.c:765:11 in
gfxline_getbbox
==41858==ABORTING
```

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id177_SEGV.zip

crash info

```
==51127==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000018 (pc 0x7f36c6dc2eeb bp
0x7ffe41030f10 sp 0x7ffe410306a8 T0)
==51127==The signal is caused by a WRITE memory access.
==51127==Hint: address points to the zero page.
    #0 0x7f36c6dc2eeb  /build/glibc-CVJwZb/glibc-2.27/string/../sysdeps/x86_64/multiarch/memset-
vec-unaligned-erms.S:253
    #1 0x4b226b in __asan_memset /home/bupt/æ¡Œé¢/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_interceptors_memintrinsics.cpp:26
    #2 0x80ac4a in InfoOutputDev::type3D0(GfxState*, double, double)
/home/bupt/Desktop/swftools/lib/pdf/InfoOutputDev.cc:880:21
    #3 0x6f686b in Gfx::opSetCharWidth(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3964:8
    #4 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #5 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #6 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #7 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #8 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int (*)
(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #9 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #10 0x5fcfff in pdf_open(_gfxsource*, char const*)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:542:14
    #11 0x500300 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:738:26
    #12 0x7f36c6c55c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #13 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /build/glibc-CVJwZb/glibc-
```

```
2.27/string/../sysdeps/x86_64/multiarch/memset-vec-unaligned-erms.S:253
==51127==ABORTING
```

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id247_SEGV.zip

crash info

```
==55626==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000048 (pc 0x00000080ad10 bp
0x000000e54600 sp 0x7fff3c224a00 T0)
==55626==The signal is caused by a READ memory access.
==55626==Hint: address points to the zero page.
    #0 0x80ad10 in InfoOutputDev::type3D1(GfxState*, double, double, double, double, double,
double) /home/bupt/Desktop/swftools/lib/pdf/InfoOutputDev.cc:887:12
    #1 0x6f6ca3 in Gfx::opSetCacheDevice(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3968:8
    #2 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #3 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #4 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #5 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #6 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int (*)
(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #7 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #8 0x5fcfff in pdf_open(_gfxsource*, char const*)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:542:14
    #9 0x500300 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:738:26
    #10 0x7f38f630bc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #11 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/swftools/lib/pdf/InfoOutputDev.cc:887:12 in
InfoOutputDev::type3D1(GfxState*, double, double, double, double, double, double)
==55626==ABORTING
```

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id299_SEGV.zip

crash info

```
==102977==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000048 (pc 0x00000080ad10 bp
0x000000e54600 sp 0x7ffde73e8d00 T0)
==102977==The signal is caused by a READ memory access.
==102977==Hint: address points to the zero page.
    #0 0x80ad10 in InfoOutputDev::type3D1(GfxState*, double, double, double, double, double,
double) /home/bupt/Desktop/swftools/lib/pdf/InfoOutputDev.cc:887:12
    #1 0x6f6ca3 in Gfx::opSetCacheDevice(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3968:8
    #2 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #3 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #4 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #5 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #6 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int (*)
(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #7 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #8 0x5fcfff in pdf_open(_gfxsource*, char const*)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:542:14
    #9 0x500300 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:738:26
    #10 0x7f93e149ec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #11 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/swftools/lib/pdf/InfoOutputDev.cc:887:12 in
InfoOutputDev::type3D1(GfxState*, double, double, double, double, double, double)
==102977==ABORTING
```

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id359_SEGV.zip

crash info

```
==64656==ERROR: AddressSanitizer: SEGV on unknown address 0x62703a2bdf6f (pc 0x00000082c60e bp
0x7fff6931f990 sp 0x7fff6931f700 T0)
```

```
==64656==The signal is caused by a READ memory access.
    #0 0x82c60e in FoFiTrueType::computeTableChecksum(unsigned char*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/FoFiTrueType.cc:1776:14
    #1 0x82c60e in FoFiTrueType::writeTTF(void (*)(void*, char*, int), void*, char*, unsigned
short*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/FoFiTrueType.cc:1146:6
    #2 0x8d28a9 in SplashFTFontEngine::loadTrueTypeFont(SplashFontFileID*, char*, int, unsigned
short*, int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/SplashFTFontEngine.cc:160:7
    #3 0x8c1fa5 in SplashFontEngine::loadTrueTypeFont(SplashFontFileID*, char*, int, unsigned
short*, int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/SplashFontEngine.cc:255:26
    #4 0x88430a in SplashOutputDev::doUpdateFont(GfxState*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/SplashOutputDev.cc:1130:36
    #5 0x8060a8 in InfoOutputDev::updateFont(GfxState*)
/home/bupt/Desktop/swftools/lib/pdf/InfoOutputDev.cc:577:13
    #6 0x6f27c5 in Gfx::opShowText(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3038:10
    #7 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #8 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #9 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #10 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #11 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #12 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #13 0x5fcfff in pdf_open(_gfxsource*, char const*)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:542:14
    #14 0x500300 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:738:26
    #15 0x7f36eef4ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #16 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/swftools/lib/pdf/xpdf/FoFiTrueType.cc:1776:14
in FoFiTrueType::computeTableChecksum(unsigned char*, int)
==64656==ABORTING
```

FPE

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id92_FPE.zip

crash info

```
==42346==ERROR: AddressSanitizer: FPE on unknown address 0x000000634097 (pc 0x000000634097 bp
0x7fffc9768180 sp 0x7fffc9767b00 T0)
    #0 0x634097 in DCTStream::readMCURow()
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2123:24
    #1 0x632e98 in DCTStream::getChar() /home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2040:12
    #2 0x60e023 in ImageStream::getLine()
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:373:25
    #3 0x60dd51 in ImageStream::getPixel(unsigned char*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:344:5
    #4 0x7c9dc5 in VectorGraphicOutputDev::drawGeneralImage(GfxState*, Object*, Stream*, int, int,
GfxImageColorMap*, int, int, int, int*, Stream*, int, int, int, GfxImageColorMap*)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1303:12
    #5 0x7ccc45 in VectorGraphicOutputDev::drawImage(GfxState*, Object*, Stream*, int, int,
GfxImageColorMap*, int*, int) /home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1430:5
    #6 0x71dc57 in Gfx::doImage(Object*, Stream*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3664:12
    #7 0x6ec5e0 in Gfx::opXObject(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3336:7
    #8 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #9 0x7049c1 in Gfx::go(int) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #10 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #11 0x6b9401 in Page::displaySlice(OutputDev*, double, double, int, int, int, int, int, int,
int, int, Catalog*, int (*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:317:10
    #12 0x6b8cee in Page::display(OutputDev*, double, double, int, int, int, int, Catalog*, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/Page.cc:264:3
    #13 0x6099b0 in PDFDoc::displayPage(OutputDev*, int, double, double, int, int, int, int, int
(*)(void*), void*) /home/bupt/Desktop/swftools/lib/pdf/xpdf/PDFDoc.cc:317:27
    #14 0x5f87d5 in render2(_gfxpage*, _gfxdevice*, int, int, int, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:164:14
    #15 0x5f8e64 in pdfpage_rendersection(_gfxpage*, _gfxdevice*, double, double, double, double,
double, double) /home/bupt/Desktop/swftools/lib/pdf/pdf.cc:190:5
    #16 0x501816 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:832:3
    #17 0x7f4bc52f2c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #18 0x420b99 in _start (/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2123:24 in
DCTStream::readMCURow()
==42346==ABORTING
```

out of memory

reproduce

command to reproduce: ./pdf2swf -G -f -t [sample file] -o /dev/null

sample file

id298_out_of_memory.zip

crash info

```
==102601==ERROR: AddressSanitizer: allocator is out of memory trying to allocate 0x2e03f3250 bytes
    #0 0x4b3160 in malloc /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-rt/lib/asan/asa
    #1 0x92c94f in draw_stroke /home/bupt/Desktop/swftools/lib/gfxpoly/stroke.c:192:26

==102601==HINT: if you don't care about these errors you may set allocator_may_return_null=1
SUMMARY: AddressSanitizer: out-of-memory /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
==102601==ABORTING
```


Cvjark mentioned this issue on Jul 3

bug report swftools-pdf2swf #184

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant