Cvjark / Poc Public

<> Code ⊙ Issues 1 Pull requests Actions Projects Security ···

main ▾ ···

Poc / swftools / pdf2swf / CVE-2022-35096.md

Cvjark Create CVE-2022-35096.md History

1 contributor

88 lines (78 sloc) 4.54 KB ···

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034357/id293_heap_buffer_overflow.zip

Command to reproduce

```
./pdf2swf -G -f -t [sample file] -o /dev/null
```

Product name & version

```
last github commit code : 772e55a
```

Problem Type

```
heap-buffer-overflow
```

Crash Detail

```
==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
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/lib/gfxpoly/stroke.c:212:24 in draw_stroke
```