Cvjark Create CVE-2022-35098.md History

1 contributor

87 lines (76 sloc) | 4.41 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034355/id175_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

```
==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
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/lib/pdf/xpdf/GfxState.cc:923:9 in
GfxICCBasedColorSpace::getDefaultColor(GfxColor*)
```