Cvjark / Poc Public

Code Issues 1 Pull requests Actions Projects Security ...

main ...

Poc / swftools / pdf2swf / CVE-2022-35094.md

Cvjark Create CVE-2022-35094.md History

1 contributor

88 lines (79 sloc) 4.96 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034354/id3_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

```
==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
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2825:14 in
```

```
    DCTStream::readHuffSym(DCTHuffTable*)
```