Cvjark Create CVE-2022-35093.md History

1 contributor

89 lines (79 sloc) | 5.13 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034361/id7_global_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

```
global-buffer-overflow
```

Crash Detail

```
==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
```

Crash summary

```
SUMMARY: AddressSanitizer: global-buffer-overflow
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2804:18 in
DCTStream::transformDataUnit(unsigned short*, int*, unsigned char*)
```