Cvjark Create CVE-2022-35099.md History

1 contributor

107 lines (97 sloc) | 5.58 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034360/id100_stack_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

```
stack-buffer-overflow
```

Crash Detail

```
==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
```

Crash summary

```
SUMMARY: AddressSanitizer: stack-buffer-overflow
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:348:12 in
ImageStream::getPixel(unsigned char*)
```