Cvjark Create CVE-2022-35091.md History

1 contributor

53 lines (44 sloc) | 3.19 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034371/id92_FPE.zip

Command to reproduce

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

Product name & version

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

Problem Type

```
FPE
```

Crash Detail

```
==42346==ERROR: AddressSanitizer: FPE on unknown address 0x000000634097 (pc
0x000000634097 bp 0x7fffc9768180 sp 0x7fffc9767b00 T0)
    #0 0x634097 in DCTStream::readMCURow()
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2123:24
    #1 0x632e98 in DCTStream::getChar()
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2040:12
    #2 0x60e023 in ImageStream::getLine()
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:373:25
    #3 0x60dd51 in ImageStream::getPixel(unsigned char*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:344:5
    #4 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
    #5 0x7ccc45 in VectorGraphicOutputDev::drawImage(GfxState*, Object*, Stream*,
int, int, GfxImageColorMap*, int*, int)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:1430:5
    #6 0x71dc57 in Gfx::doImage(Object*, Stream*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3664:12
    #7 0x6ec5e0 in Gfx::opXObject(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3336:7
    #8 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #9 0x7049c1 in Gfx::go(int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #10 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #11 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
    #12 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
    #13 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
    #14 0x5f87d5 in render2(_gfxpage*, _gfxdevice*, int, int, int, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:164:14
    #15 0x5f8e64 in pdfpage_rendersection(_gfxpage*, _gfxdevice*, double, double,
double, double, double, double) /home/bupt/Desktop/swftools/lib/pdf/pdf.cc:190:5
    #16 0x501816 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:832:3
    #17 0x7f4bc52f2c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #18 0x420b99 in _start
(/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)
```

```
AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2123:24 in
DCTStream::readMCURow()
==42346==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: FPE
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Stream.cc:2123:24 in
DCTStream::readMCURow()
```