Cvjark Create CVE-2022-35092.md History

1 contributor

54 lines (45 sloc) | 3.07 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034364/id76_SEGV.zip

Command to reproduce

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

Product name & version

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

Problem Type

```
SEGV
```

Crash Detail

```
==41269==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x00000091bf07 bp
0x7fff9910e150 sp 0x7fff9910dfa0 T0)
==41269==The signal is caused by a READ memory access.
==41269==Hint: this fault was caused by a dereference of a high value address
(see register values below).  Disassemble the provided pc to learn which register
was used.
    #0 0x91bf07 in convert_gfxline
/home/bupt/Desktop/swftools/lib/gfxpoly/convert.c:31:18
    #1 0x91bf07 in gfxpoly_from_fill
/home/bupt/Desktop/swftools/lib/gfxpoly/convert.c:250:5
    #2 0x90a161 in polyops_fill
/home/bupt/Desktop/swftools/lib/devices/polyops.c:247:22
    #3 0x7c3e1b in VectorGraphicOutputDev::fillGfxLine(GfxState*, _gfxline*,
char) /home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:627:5
    #4 0x7c3e1b in VectorGraphicOutputDev::endString(GfxState*)
/home/bupt/Desktop/swftools/lib/pdf/VectorGraphicOutputDev.cc:805:6
    #5 0x71bb67 in Gfx::doShowText(GString*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3300:10
    #6 0x6f28e5 in Gfx::opShowText(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3042:3
    #7 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #8 0x7049c1 in Gfx::go(int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #9 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #10 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
    #11 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
    #12 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
    #13 0x5f87d5 in render2(_gfxpage*, _gfxdevice*, int, int, int, int, int, int)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:164:14
    #14 0x5f8e64 in pdfpage_rendersection(_gfxpage*, _gfxdevice*, double, double,
double, double, double, double) /home/bupt/Desktop/swftools/lib/pdf/pdf.cc:190:5
    #15 0x501816 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:832:3
    #16 0x7fa199df7c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #17 0x420b99 in _start
(/home/bupt/Desktop/swftools/build/bin/pdf2swf+0x420b99)

AddressSanitizer can not provide additional info.
```

```
SUMMARY: AddressSanitizer: SEGV
/home/bupt/Desktop/swftools/lib/gfxpoly/convert.c:31:18 in convert_gfxline
==41269==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV
/home/bupt/Desktop/swftools/lib/gfxpoly/convert.c:31:18 in convert_gfxline
```