Cvjark Create CVE-2022-35095.md History

1 contributor

48 lines (39 sloc) | 2.44 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034368/id247_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

```
==55626==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000048 (pc
0x00000080ad10 bp 0x000000e54600 sp 0x7fff3c224a00 T0)
==55626==The signal is caused by a READ memory access.
==55626==Hint: address points to the zero page.
    #0 0x80ad10 in InfoOutputDev::type3D1(GfxState*, double, double, double,
double, double, double)
/home/bupt/Desktop/swftools/lib/pdf/InfoOutputDev.cc:887:12
    #1 0x6f6ca3 in Gfx::opSetCacheDevice(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3968:8
    #2 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #3 0x7049c1 in Gfx::go(int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #4 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #5 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
    #6 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
    #7 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
    #8 0x5fcfff in pdf_open(_gfxsource*, char const*)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:542:14
    #9 0x500300 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:738:26
    #10 0x7f38f630bc86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #11 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/pdf/InfoOutputDev.cc:887:12 in
InfoOutputDev::type3D1(GfxState*, double, double, double, double, double, double)
==55626==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV
/home/bupt/Desktop/swftools/lib/pdf/InfoOutputDev.cc:887:12 in
InfoOutputDev::type3D1(GfxState*, double, double, double, double, double, double)
```