Cvjark / Poc Public

Code Issues 1 Pull requests Actions Projects Security ...

main

Poc / swftools / pdf2swf / CVE-2022-35097.md

Cvjark Create CVE-2022-35097.md History

1 contributor

55 lines (45 sloc) 3.13 KB

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034362/id0_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

```
Error: PDF file is damaged - attempting to reconstruct xref table...
AddressSanitizer:DEADLYSIGNAL

==71049==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc
0x0000008293e7 bp 0x7ffe8c3e6990 sp 0x7ffe8c3e6700 T0)
==71049==The signal is caused by a READ memory access.
==71049==Hint: address points to the zero page.
    #0 0x8293e7 in FoFiTrueType::writeTTF(void (*)(void*, char*, int), void*,
char*, unsigned short*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/FoFiTrueType.cc:910:24
    #1 0x8d28a9 in SplashFTFontEngine::loadTrueTypeFont(SplashFontFileID*, char*,
int, unsigned short*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/SplashFTFontEngine.cc:160:7
    #2 0x8c1fa5 in SplashFontEngine::loadTrueTypeFont(SplashFontFileID*, char*,
int, unsigned short*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/SplashFontEngine.cc:255:26
    #3 0x88430a in SplashOutputDev::doUpdateFont(GfxState*)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/SplashOutputDev.cc:1130:36
    #4 0x8060a8 in InfoOutputDev::updateFont(GfxState*)
/home/bupt/Desktop/swftools/lib/pdf/InfoOutputDev.cc:577:13
    #5 0x6f27c5 in Gfx::opShowText(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:3038:10
    #6 0x705f02 in Gfx::execOp(Object*, Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:693:3
    #7 0x7049c1 in Gfx::go(int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:584:7
    #8 0x703ea8 in Gfx::display(Object*, int)
/home/bupt/Desktop/swftools/lib/pdf/xpdf/Gfx.cc:556:3
    #9 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
    #10 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
    #11 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
    #12 0x5fcfff in pdf_open(_gfxsource*, char const*)
/home/bupt/Desktop/swftools/lib/pdf/pdf.cc:542:14
    #13 0x500300 in main /home/bupt/Desktop/swftools/src/pdf2swf.c:738:26
    #14 0x7f971e94dc86 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)

AddressSanitizer can not provide additional info.
```

```
SUMMARY: AddressSanitizer: SEGV
/home/bupt/Desktop/swftools/lib/pdf/xpdf/FoFiTrueType.cc:910:24 in
FoFiTrueType::writeTTF(void (*)(void*, char*, int), void*, char*, unsigned
short*)
==71049==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV
/home/bupt/Desktop/swftools/lib/pdf/xpdf/FoFiTrueType.cc:910:24 in
FoFiTrueType::writeTTF(void (*)(void*, char*, int), void*, char*, unsigned
short*)
```