SIGSEGV in pdftops

blbi

SIGSEGV in pdftops

Tue Dec 01, 2020 5:23 am

There is an stack-overflow in getOp function.

Version : Xpdf 4.02
OS : Ubuntu 16.04

This is an AddressSanitizer log.

CODE: SELECT ALL

```
$ ./pdftops poc
Syntax Error: Couldn't read xref table
Syntax Warning: PDF file is damaged - attempting to reconstruct xref table...
ASAN:SIGSEGV
=================================================================
==20483==ERROR: AddressSanitizer: stack-overflow on address 0x7ffdcc40aff8 (pc 0x000000548617 bp 0x7ffdcc40b0b0 sp 0x7ffdcc40b000 T0)
    #0 0x548616 in FoFiType1C::getOp(int, int, int*) (/home/circuit/xpdf/xpdf-4.02/build/xpdf/pdftops+0x548616)
    #1 0x540a5d in FoFiType1C::cvtGlyph(int, int, GString*, Type1CIndex*, Type1CPrivateDict*, int) (/home/circuit/xpdf/xpdf-4.02/build/xpdf/pdftops+0x540a5d)
    #2 0x542edc in FoFiType1C::cvtGlyph(int, int, GString*, Type1CIndex*, Type1CPrivateDict*, int) (/home/circuit/xpdf/xpdf-4.02/build/xpdf/pdftops+0x542edc)
    .... repeat 250 times
    #251 0x542edc in FoFiType1C::cvtGlyph(int, int, GString*, Type1CIndex*, Type1CPrivateDict*, int) (/home/circuit/xpdf/xpdf-4.02/build/xpdf/pdftops+0x542edc)

SUMMARY: AddressSanitizer: stack-overflow ??:0 FoFiType1C::getOp(int, int, int*)
==20483==ABORTING
```

Thank you

derekn

Re: SIGSEGV in pdftops

Tue Dec 01, 2020 9:49 pm

Can you email the POC PDF file to xpdf@xpdfreader.com?

blbi

Re: SIGSEGV in pdftops

Sat Dec 05, 2020 4:41 am

Yes! I sent the POC file by email

derekn

Re: SIGSEGV in pdftops

Mon Dec 07, 2020 6:29 pm

That turned out to be an infinite loop caused by a bad subroutine reference in a Type 1C font charstring.

I'm going to add a recursion check in FoFiType1C::cvtGlyph().

Thanks for the bug report.