SIGSEGV Error.cc:85 in xpdf-4.02

b166er_fauxre

SIGSEGV Error.cc:85 in xpdf-4.02

Wed Aug 26, 2020 3:35 pm

Version: xpdf-4.02

OS: Ubuntu 16.04 LTS

cmd: ./pdftohtml -r 300 POC /dev/nul

GDB log:
Program received signal SIGSEGV, Segmentation fault.
0x00007ffff6aee64b in __GI__IO_default_xsputn (f=0x7fffff7ff5b0, data=0x595904, n=12) at genops.c:422
422 genops.c: No such file or directory.
(gdb) backtrace
#0 0x00007ffff6aee64b in __GI__IO_default_xsputn (f=0x7fffff7ff5b0, data=0x595904, n=12) at genops.c:422
#1 0x00007ffff6ac151b in _IO_vfprintf_internal (s=0x7fffff7ff5b0, format=<optimized out>, ap=0x7fffff801c68) at vfprintf.c:1632
#2 0x00007ffff6ac2f01 in buffered_vfprintf (s=0x7ffff6e38540 <_IO_2_1_stderr_>, format=<optimized out>, args=<optimized out>) at vfprintf.c:2320
#3 0x00007ffff6ac033d in _IO_vfprintf_internal (s=0x7ffff6e38540 <_IO_2_1_stderr_>, format=0x595988 "%s: %s\n", ap=ap@entry=0x7fffff801c68) at vfprintf.c:1293
#4 0x00007ffff6ac8807 in __fprintf (stream=<optimized out>, format=<optimized out>) at fprintf.c:32
#5 0x0000000000499bbd in error (category=errSyntaxError, pos=-1, msg=0x593278 "AcroForm field object is wrong type") at /home/b166er/yes/xpdf-4.02/xpdf/Error.cc:85
#6 0x000000000047981d in AcroForm::scanField (this=0x86c880, fieldRef=0x7fffff801f40) at /home/b166er/yes/xpdf-4.02/xpdf/AcroForm.cc:246
#7 0x000000000047997d in AcroForm::scanField (this=0x86c880, fieldRef=0x7fffff801fd0) at /home/b166er/yes/xpdf-4.02/xpdf/AcroForm.cc:271
#8 0x000000000047997d in AcroForm::scanField (this=0x86c880, fieldRef=0x7fffff802060) at /home/b166er/yes/xpdf-4.02/xpdf/AcroForm.cc:271
#9 0x000000000047997d in AcroForm::scanField (this=0x86c880, fieldRef=0x7fffff8020f0) at /home/b166er/yes/xpdf-4.02/xpdf/AcroForm.cc:271
#10 0x000000000047997d in AcroForm::scanField (this=0x86c880, fieldRef=0x7fffff802180) at /home/b166er/yes/xpdf-4.02/xpdf/AcroForm.cc:271
#11 0x000000000047997d in AcroForm::scanField (this=0x86c880, fieldRef=0x7fffff802210) at /home/b166er/yes/xpdf-4.02/xpdf/AcroForm.cc:271
#12 0x000000000047997d in AcroForm::scanField (this=0x86c880, fieldRef=0x7fffff8022a0) at /home/b166er/yes/xpdf-4.02/xpdf/AcroForm.cc:271
#13 0x000000000047997d in AcroForm::scanField (this=0x86c880, fieldRef=0x7fffff802330) at /home/b166er/yes/xpdf-4.02/xpdf/AcroForm.cc:271
#14 0x000000000047997d in AcroForm::scanField (this=0x86c880, fieldRef=0x7fffff8023c0) at /home/b166er/yes/xpdf-4.02/xpdf/AcroForm.cc:271
#15 0x000000000047997d in AcroForm::scanField (this=0x86c880, fieldRef=0x7fffff802450) at /home/b166er/yes/xpdf-4.02/xpdf/AcroForm.cc:271
#16 0x000000000047997d in AcroForm::scanField (this=0x86c880, fieldRef=0x7fffff8024e0) at /home/b166er/yes/xpdf-4.02/xpdf/AcroForm.cc:271l

Backto source code debug:

fprintf(stderr, "%s: %s\n", errorCategoryNames[category], sanitized->getCString());

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff6ac0213 in vfprintf () from target:/lib/x86_64-linux-gnu/libc.so.6
(gdb) p sanitized->getCString()
Cannot access memory at address 0x7fffff7fef7f

Please see testcase sample as attachment.

Thanks.

ATTACHMENTS
SIGSEGV_in_Errorcc.zip
(1.16 KiB) Downloaded 289 times

derekn

Re: SIGSEGV Error.cc:85 in xpdf-4.02

Thu Aug 27, 2020 6:43 pm

That's a stack overflow, caused by a loop in the object tree.

Xpdf 4 has code to catch some object loops, but not all of them. I'm working on a much better loop detector for Xpdf 5.

b166er_fauxre

Re: SIGSEGV Error.cc:85 in xpdf-4.02

Thu Aug 27, 2020 7:23 pm

hi derekn,thanks for your reply and the effort you've made.