matthiaskramm / swftools Public

Code Issues 118 Pull requests 5 Actions Projects Wiki ···

New issue

Jump to bottom

A Segmentation fault in xpdf/Stream.cc:598 #98

Open seviezhou opened this issue on Jul 31, 2020 · 0 comments

seviezhou commented on Jul 31, 2020 • edited

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), pdf2swf (latest master fad6c2)

Command line

./pdf2swf -qq -z -o /dev/null ./stack-overflow-Stream-598

Output

```
Segmentation fault (core dumped)
```

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==34903==ERROR: AddressSanitizer: stack-overflow on address 0x7fff90f8fff8 (pc 0x7fbe969a553e bp 0x7fff90f90860 sp 0x7fff90f90000 T0)
    #0 0x7fbe969a553d in operator new(unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x9953d)
    #1 0x5561d4fe12ce in FileStream::makeSubStream(unsigned int, int, unsigned int, Object*) xpdf/Stream.cc:598
    #2 0x5561d50328b6 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:810
    #3 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #4 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #5 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #6 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #7 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #8 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #9 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #10 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #11 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #12 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #13 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #14 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #15 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #16 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #17 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #18 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #19 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #20 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #21 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #22 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #23 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #24 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #25 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #26 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #27 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #28 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #29 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #30 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #31 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #32 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #33 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #34 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #35 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #36 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #37 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #38 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #39 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #40 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #41 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #42 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #43 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #44 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #45 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #46 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #47 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #48 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #49 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #50 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #51 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #52 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #53 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #54 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #55 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #56 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #57 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #58 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #59 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #60 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #61 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #62 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #63 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #64 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #65 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #66 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #67 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
```

```
#68 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#69 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#70 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#71 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#72 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#73 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#74 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#75 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#76 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#77 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#78 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#79 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#80 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#81 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#82 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#83 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#84 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#85 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#86 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#87 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#88 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#89 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#90 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#91 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#92 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#93 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#94 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#95 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#96 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#97 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#98 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#99 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#100 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#101 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#102 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#103 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#104 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#105 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#106 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#107 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#108 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#109 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#110 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#111 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#112 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#113 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#114 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#115 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#116 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#117 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#118 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#119 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#120 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#121 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#122 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#123 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#124 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#125 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#126 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#127 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#128 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#129 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#130 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#131 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#132 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#133 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#134 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#135 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#136 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#137 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#138 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#139 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#140 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#141 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#142 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#143 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#144 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#145 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#146 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#147 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#148 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#149 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#150 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#151 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#152 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#153 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#154 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#155 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#156 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#157 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#158 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#159 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#160 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#161 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#162 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#163 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#164 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#165 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#166 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#167 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#168 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#169 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#170 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#171 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#172 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#173 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#174 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#175 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#176 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#177 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#178 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#179 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#180 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
```

```
#181 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#182 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#183 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#184 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#185 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#186 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#187 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#188 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#189 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#190 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#191 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#192 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#193 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#194 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#195 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#196 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#197 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#198 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#199 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#200 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#201 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#202 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#203 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#204 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#205 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#206 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#207 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#208 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#209 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#210 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#211 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#212 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#213 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#214 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#215 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#216 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#217 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#218 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#219 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#220 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#221 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#222 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#223 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#224 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#225 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#226 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#227 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#228 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#229 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#230 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#231 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#232 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#233 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#234 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#235 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#236 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#237 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#238 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#239 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#240 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#241 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#242 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#243 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#244 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#245 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#246 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#247 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#248 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#249 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#250 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#251 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#252 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#253 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#254 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#255 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#256 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#257 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#258 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#259 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#260 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#261 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#262 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#263 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#264 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#265 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#266 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#267 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#268 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#269 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#270 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#271 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#272 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#273 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#274 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#275 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#276 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#277 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#278 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#279 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#280 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#281 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#282 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#283 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#284 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#285 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#286 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#287 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#288 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#289 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#290 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#291 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#292 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#293 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
```

```
    #294 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #295 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #296 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #297 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #298 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #299 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #300 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #301 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #302 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #303 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #304 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #305 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #306 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #307 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #308 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #309 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #310 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #311 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #312 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #313 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #314 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #315 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #316 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #317 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #318 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #319 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #320 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #321 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #322 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #323 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #324 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #325 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #326 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #327 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #328 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #329 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #330 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #331 0x5561d5039ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #332 0x5561d5039ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #333 0x5561d503bbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #334 0x5561d5032ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824

SUMMARY: AddressSanitizer: stack-overflow ??:0 operator new(unsigned long)
==34903==ABORTING
```

POC

stack-overflow-Stream-598.zip

seviezhou changed the title ~~A stack overflow in xpdf/Stream.cc:598~~ A Segmentation fault in xpdf/Stream.cc:598 on Jul 31, 2020

Cvjark mentioned this issue on Jul 3

bug report swftools-pdf2swf #184

⊙ Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant