New issue

Jump to bottom

Segmentation fault error in xpdf/gmem.cc:101 #97

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-gmalloc-gmem-101

Output

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

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==17568==ERROR: AddressSanitizer: stack-overflow on address 0x7ffd339d4fe8 (pc 0x7f12da79277b bp 0x7ffd339d58f0 sp 0x7ffd339d4fe0 T0)
    #0 0x7f12da79277a  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x2277a)
    #1 0x7f12da8085e2 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x985e2)
    #2 0x55a5e5dc711a in gmalloc(int, bool) xpdf/gmem.cc:101
    #3 0x55a5e5dc79b8 in copyString xpdf/gmem.cc:301
    #4 0x55a5e5e3b0c0 in Object::initCmd(char*) xpdf/Object.h:103
    #5 0x55a5e5e3b0c0 in Lexer::getObj(Object*) xpdf/Lexer.cc:467
    #6 0x55a5e5e376ab in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:108
    #7 0x55a5e5e37d0d in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:85
    #8 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #9 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #10 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #11 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #12 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #13 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #14 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #15 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #16 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #17 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #18 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #19 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #20 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #21 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #22 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #23 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #24 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #25 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #26 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #27 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #28 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #29 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #30 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #31 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #32 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #33 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #34 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #35 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #36 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #37 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #38 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #39 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #40 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #41 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #42 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #43 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #44 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #45 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #46 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #47 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #48 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #49 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #50 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #51 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #52 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #53 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #54 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #55 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #56 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #57 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #58 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #59 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #60 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #61 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #62 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #63 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #64 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #65 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #66 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #67 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
```

```
#68 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#69 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#70 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#71 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#72 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#73 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#74 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#75 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#76 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#77 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#78 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#79 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#80 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#81 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#82 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#83 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#84 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#85 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#86 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#87 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#88 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#89 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#90 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#91 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#92 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#93 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#94 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#95 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#96 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#97 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#98 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#99 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#100 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#101 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#102 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#103 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#104 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#105 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#106 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#107 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#108 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#109 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#110 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#111 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#112 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#113 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#114 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#115 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#116 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#117 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#118 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#119 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#120 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#121 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#122 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#123 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#124 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#125 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#126 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#127 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#128 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#129 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#130 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#131 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#132 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#133 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#134 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#135 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#136 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#137 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#138 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#139 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#140 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#141 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#142 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#143 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#144 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#145 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#146 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#147 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#148 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#149 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#150 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#151 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#152 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#153 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#154 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#155 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#156 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#157 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#158 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#159 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#160 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#161 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#162 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#163 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#164 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#165 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#166 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#167 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#168 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#169 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#170 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#171 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#172 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#173 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#174 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#175 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#176 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#177 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#178 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#179 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#180 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
```

```
#181 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#182 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#183 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#184 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#185 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#186 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#187 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#188 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#189 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#190 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#191 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#192 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#193 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#194 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#195 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#196 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#197 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#198 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#199 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#200 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#201 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#202 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#203 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#204 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#205 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#206 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#207 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#208 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#209 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#210 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#211 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#212 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#213 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#214 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#215 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#216 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#217 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#218 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#219 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#220 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#221 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#222 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#223 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#224 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#225 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#226 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#227 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#228 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#229 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#230 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#231 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#232 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#233 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#234 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#235 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#236 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#237 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#238 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#239 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#240 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#241 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#242 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#243 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#244 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#245 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#246 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#247 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#248 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#249 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#250 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#251 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#252 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#253 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#254 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#255 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#256 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#257 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#258 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#259 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#260 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#261 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#262 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#263 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#264 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#265 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#266 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#267 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#268 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#269 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#270 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#271 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#272 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#273 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#274 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#275 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#276 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#277 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#278 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#279 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#280 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#281 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#282 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#283 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#284 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#285 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#286 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#287 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#288 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#289 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#290 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#291 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#292 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#293 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
```

```
    #294 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #295 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #296 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #297 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #298 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #299 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #300 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #301 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #302 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #303 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #304 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #305 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #306 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #307 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #308 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #309 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #310 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #311 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #312 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #313 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #314 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #315 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #316 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #317 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #318 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #319 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #320 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #321 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #322 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #323 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #324 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #325 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #326 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #327 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #328 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #329 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #330 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #331 0x55a5e5e37bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #332 0x55a5e5e2eee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #333 0x55a5e5e35ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #334 0x55a5e5e35ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156

SUMMARY: AddressSanitizer: stack-overflow ??:0 ??
==17568==ABORTING
```

POC

stack-overflow-gmalloc-gmem-101.zip

seviezhou changed the title ~~Segmentation fault error~~ **Segmentation fault error in xpdf/gmem.cc:301** on Jul 31, 2020

seviezhou changed the title ~~Segmentation fault error in xpdf/gmem.cc:301~~ **Segmentation fault error in xpdf/gmem.cc:101** 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