New issue

Jump to bottom

A Segmentation fault in xpdf/gmem.cc:156 #103

Open **seviezhou** opened this issue on Aug 1, 2020 · 0 comments

seviezhou commented on Aug 1, 2020

System info

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

Command line

./pdf2swf -qq -z -o /dev/null ./stack-overflow-grealloc-gmem-156

Output

```
Error: PDF file is damaged - attempting to reconstruct xref table...
Error: Wrong type in font encoding resource differences (cmd)
Segmentation fault (core dumped)
```

AddressSanitizer output

```
Error: PDF file is damaged - attempting to reconstruct xref table...
Error: Wrong type in font encoding resource differences (cmd)
ASAN:SIGSEGV
=================================================================
==68956==ERROR: AddressSanitizer: stack-overflow on address 0x7ffeeba07ff0 (pc 0x7fd321caa24e bp 0x000000000080 sp 0x7ffeeba07fe0 T0)
    #0 0x7fd321caa24d  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xb024d)
    #1 0x7fd321ca9d47  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xafd47)
    #2 0x7fd321c1cebf  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x22ebf)
    #3 0x7fd321c925e2 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x985e2)
    #4 0x557ed05733d7 in grealloc(void*, int, bool) xpdf/gmem.cc:156
    #5 0x557ed05d1f69 in Array::add(Object*) xpdf/Array.cc:47
    #6 0x557ed05e4d64 in Lexer::Lexer(XRef*, Stream*) xpdf/Lexer.cc:54
    #7 0x557ed05da8da in XRef::fetch(int, int, Object*) xpdf/XRef.cc:809
    #8 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #9 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #10 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #11 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #12 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #13 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #14 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #15 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #16 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #17 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #18 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #19 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #20 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #21 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #22 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #23 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #24 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #25 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #26 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #27 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #28 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #29 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #30 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #31 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #32 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #33 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #34 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #35 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #36 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #37 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #38 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #39 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #40 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #41 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #42 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #43 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #44 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #45 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #46 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #47 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #48 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #49 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #50 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #51 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #52 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #53 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #54 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #55 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #56 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #57 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #58 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #59 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #60 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #61 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #62 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #63 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
```

```
#64 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#65 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#66 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#67 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#68 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#69 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#70 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#71 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#72 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#73 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#74 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#75 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#76 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#77 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#78 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#79 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#80 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#81 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#82 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#83 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#84 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#85 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#86 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#87 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#88 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#89 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#90 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#91 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#92 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#93 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#94 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#95 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#96 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#97 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#98 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#99 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#100 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#101 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#102 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#103 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#104 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#105 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#106 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#107 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#108 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#109 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#110 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#111 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#112 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#113 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#114 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#115 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#116 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#117 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#118 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#119 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#120 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#121 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#122 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#123 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#124 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#125 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#126 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#127 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#128 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#129 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#130 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#131 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#132 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#133 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#134 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#135 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#136 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#137 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#138 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#139 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#140 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#141 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#142 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#143 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#144 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#145 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#146 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#147 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#148 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#149 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#150 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#151 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#152 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#153 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#154 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#155 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#156 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#157 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#158 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#159 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#160 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#161 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#162 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#163 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#164 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#165 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#166 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#167 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#168 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#169 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#170 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#171 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#172 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#173 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#174 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#175 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#176 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
```

```
#177 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#178 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#179 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#180 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#181 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#182 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#183 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#184 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#185 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#186 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#187 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#188 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#189 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#190 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#191 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#192 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#193 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#194 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#195 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#196 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#197 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#198 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#199 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#200 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#201 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#202 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#203 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#204 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#205 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#206 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#207 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#208 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#209 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#210 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#211 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#212 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#213 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#214 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#215 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#216 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#217 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#218 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#219 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#220 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#221 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#222 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#223 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#224 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#225 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#226 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#227 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#228 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#229 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#230 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#231 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#232 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#233 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#234 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#235 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#236 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#237 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#238 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#239 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#240 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#241 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#242 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#243 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#244 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#245 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#246 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#247 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#248 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#249 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#250 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#251 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#252 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#253 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#254 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#255 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#256 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#257 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#258 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#259 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#260 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#261 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#262 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#263 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#264 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#265 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#266 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#267 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#268 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#269 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#270 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#271 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#272 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#273 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#274 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#275 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#276 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#277 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#278 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#279 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#280 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#281 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#282 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#283 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#284 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#285 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#286 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#287 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#288 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#289 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
```

```
    #290 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #291 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #292 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #293 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #294 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #295 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #296 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #297 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #298 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #299 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #300 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #301 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #302 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #303 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #304 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #305 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #306 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #307 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #308 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #309 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #310 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #311 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #312 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #313 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #314 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #315 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #316 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #317 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #318 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #319 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #320 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #321 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #322 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #323 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #324 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #325 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #326 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #327 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #328 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #329 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
    #330 0x557ed05e3bd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
    #331 0x557ed05daee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
    #332 0x557ed05e1ddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
    #333 0x557ed05e1ddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156

SUMMARY: AddressSanitizer: stack-overflow ??:0 ??
==68956==ABORTING
```

POC

stack-overflow-grealloc-gmem-156.zip

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