


New issue

[Jump to bottom](#)

A Segmentation fault in xpdf/Lexer.cc:53 #100

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

seviezhou commented on Jul 31, 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-Lexer-Lexer-53

Output

Segmentation fault (core dumped)

AddressSanitizer output

```
ASAN: SIGSEGV
=====
==78316==ERROR: AddressSanitizer: stack-overflow on address 0x7ffc6fc29ff8 (pc 0x7f8314fc71ff bp 0x000000000020 sp 0x7ffc6fc2a000 T0)
#0 0x7f8314fc71fe (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xb01fe)
#1 0x7f8314fc6d47 (/usr/lib/x86_64-linux-gnu/libasan.so.2+0xafd47)
#2 0x7f8314f39ebf (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x22ebf)
#3 0x7f8314fb050e in operator new(unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x9950e)
#4 0x560f6b08ed0e in Lexer::Lexer(XRef*, Stream*) xpdf/Lexer.cc:53
#5 0x560f6b0848da in XRef::fetch(int, int, Object*) xpdf/XRef.cc:809
#6 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#7 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#8 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#9 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#10 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#11 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#12 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#13 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#14 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#15 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#16 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#17 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#18 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#19 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#20 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#21 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#22 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#23 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#24 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#25 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#26 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#27 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#28 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#29 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#30 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#31 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#32 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#33 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#34 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#35 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#36 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#37 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#38 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#39 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#40 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#41 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#42 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#43 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#44 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#45 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#46 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#47 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#48 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#49 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#50 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#51 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#52 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#53 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#54 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#55 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#56 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#57 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#58 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#59 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#60 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#61 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#62 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#63 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#64 0x560f6b08bdd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#65 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#66 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#67 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
```

[illegible]

[illegible]

```
#294 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#295 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#296 0x560f6b08dbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#297 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#298 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#299 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#300 0x560f6b08dbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#301 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#302 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#303 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#304 0x560f6b08dbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#305 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#306 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#307 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#308 0x560f6b08dbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#309 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#310 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#311 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#312 0x560f6b08dbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#313 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#314 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#315 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#316 0x560f6b08dbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#317 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#318 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#319 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#320 0x560f6b08dbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#321 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#322 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#323 0x560f6b08dbd5 in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#324 0x560f6b08dbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#325 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#326 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#327 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#328 0x560f6b08dbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#329 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
#330 0x560f6b08bddf in Object::dictLookup(char*, Object*) xpdf/Object.h:253
#331 0x560f6b08bddf in Parser::makeStream(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:156
#332 0x560f6b08dbd5 in Parser::getObj(Object*, unsigned char*, CryptAlgorithm, int, int, int) xpdf/Parser.cc:94
#333 0x560f6b084ee0 in XRef::fetch(int, int, Object*) xpdf/XRef.cc:824
```

SUMMARY: AddressSanitizer: stack-overflow ??:0 ??
==78316==ABORTING

POC

[stack-overflow-Stream-598.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

