New issue

Jump to bottom

A stack overflow in analyze.cpp:604:60 causes Segmentation fault #2

Open seviezhou opened this issue on Aug 5, 2020 · 0 comments

seviezhou commented on Aug 5, 2020

System info

Ubuntu x86_64, clang 6.0, pdftools (latest master 7fe388)

Configure

CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" ./configure

Command line

./src/pdftools -o /dev/null @@

Output

```
Segmentation fault
```

AddressSanitizer output

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==76278==ERROR: AddressSanitizer: stack-overflow on address 0x7ffd2f627e38 (pc 0x00000047e3a7 bp 0x7ffd2f6286b0 sp 0x7ffd2f627e40 T0)
    #0 0x47e3a6 in __interceptor_strlen.part.32 /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:332
    #1 0x7fce701843f7 in std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >::basic_string(char const*, std::allocator<char> const&) (/usr/lib/x86_64-
linux-gnu/libstdc++.so.6+0x1413f7)
    #2 0x53062c in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:604:60
    #3 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #4 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #5 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #6 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #7 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #8 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #9 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #10 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #11 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #12 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #13 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #14 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #15 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #16 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #17 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #18 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #19 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #20 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #21 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #22 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #23 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #24 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #25 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #26 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #27 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #28 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #29 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #30 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #31 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #32 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #33 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #34 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #35 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #36 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #37 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #38 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #39 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #40 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #41 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #42 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #43 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #44 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #45 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #46 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #47 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #48 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #49 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #50 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #51 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #52 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #53 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #54 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #55 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #56 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #57 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #58 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #59 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #60 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #61 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
```

```
#62 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#63 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#64 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#65 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#66 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#67 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#68 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#69 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#70 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#71 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#72 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#73 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#74 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#75 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#76 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#77 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#78 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#79 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#80 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#81 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#82 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#83 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#84 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#85 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#86 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#87 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#88 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#89 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#90 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#91 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#92 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#93 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#94 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#95 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#96 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#97 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#98 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#99 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#100 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#101 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#102 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#103 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#104 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#105 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#106 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#107 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#108 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#109 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#110 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#111 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#112 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#113 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#114 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#115 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#116 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#117 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#118 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#119 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#120 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#121 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#122 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#123 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#124 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#125 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#126 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#127 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#128 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#129 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#130 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#131 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#132 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#133 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#134 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#135 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#136 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#137 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#138 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#139 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#140 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#141 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#142 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#143 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#144 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#145 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#146 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#147 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#148 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#149 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#150 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#151 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#152 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#153 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#154 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#155 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#156 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#157 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#158 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#159 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#160 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#161 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#162 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#163 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#164 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#165 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#166 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#167 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#168 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#169 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#170 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#171 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#172 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#173 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
#174 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
```

```
    #175 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #176 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #177 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #178 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #179 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #180 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #181 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #182 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #183 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #184 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #185 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #186 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #187 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #188 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #189 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #190 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #191 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #192 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #193 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #194 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #195 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #196 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #197 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #198 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #199 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #200 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #201 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #202 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #203 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #204 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #205 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #206 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #207 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #208 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #209 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #210 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #211 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #212 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #213 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #214 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #215 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #216 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #217 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #218 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #219 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #220 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #221 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #222 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #223 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #224 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #225 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #226 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #227 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #228 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #229 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #230 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #231 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #232 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #233 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #234 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #235 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #236 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #237 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #238 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #239 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #240 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #241 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #242 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #243 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #244 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #245 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #246 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #247 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #248 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21
    #249 0x530cfe in Analyze::AnalyzePages(node::TreeNode*, node::ArrayNode*) /home/seviezhou/pdftools/src/analyze.cpp:621:21

SUMMARY: AddressSanitizer: stack-overflow /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:332 in
__interceptor_strlen.part.32
==76278==ABORTING
```

POC

stack-overflow-AnalyzePages-analyze-604.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant