

stack_overflow

Post Reply



Search this topic...



2 posts • Page 1 of 1

H00K1998



stack_overflow

Sun Jun 05, 2022 8:16 am

Hello, friend, I have a crash during fuzz test, it seems to be a stack overflow, can you take a look.
thank you 😊

SUMMARY: AddressSanitizer: stack-overflow (/home/jiuge/Desktop/xpdf_NB/New_test/bin/pdftotext+0x4e8659) in
__sanitizer::StackDepotBase<__sanitizer::StackDepotNode, 1, 20>::Put(__sanitizer::StackTrace, bool*)
==17899==ABORTING

See attachment for more:)

ATTACHMENTS

[POC and compile.tar](#)

(7 KiB) Downloaded 146 times

```
Syntax Error (3720): Illegal character '>'
Syntax Error (3801): Dictionary key must be a name object
Syntax Error (4055): Missing 'endstream'
Syntax Error: End of file inside array
Syntax Error: End of file inside dictionary
AddressSanitizer:DEADLYSIGNAL
=====
==17899==ERROR: AddressSanitizer: stack-overflow on address 0x7ffc70016fd8 (pc 0x0000004e8661 bp 0x000000000008 sp 0x7ffc70016fd8 T0)
#0 0x4e8661 in __sanitizer::StackDepotBase<__sanitizer::StackDepotNode, 1, 20>::Put(__sanitizer::StackTrace, bool*) (/home/jiuge/桌面/xpdf_NB/New_test/bin/pdftotext+0x4e8661)
#1 0x4e8636 in __sanitizer::StackDepotPut(__sanitizer::StackTrace) (/home/jiuge/桌面/xpdf_NB/New_test/bin/pdftotext+0x4e8636)
#2 0x44feaa in __asan::Allocator::Allocate(unsigned long, unsigned long, __sanitizer::BufferedStackTrace*, __asan::AllocType, bool) (/home/jiuge/桌面/xpdf_NB/New_test/bin/pdftotext+0x44feaa)
#3 0x450709 in __asan::asan_malloc(unsigned long, unsigned long, __sanitizer::BufferedStackTrace*, __asan::AllocType) (/home/jiuge/桌面/xpdf_NB/New_test/bin/pdftotext+0x450709)
#4 0x4f8132 in operator new[](unsigned long) (/home/jiuge/桌面/xpdf_NB/New_test/bin/pdftotext+0x4f8132)
#5 0x7c4c52 in GString::resize(int) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/goo/GString.cc:119:9
#6 0x7c519c in GString::GString(GString*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/goo/GString.cc:163:3
#7 0x7173bc in GString::copy() /home/jiuge/桌面/xpdf_NB/xpdf-4.04/goo/GString.h:42:32
#8 0x7173bc in Object::copy(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Object.cc:84:27
#9 0x585df0 in Object::arrayGet(int, Object*, int) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Object.h:243:19
#10 0x585df0 in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:566:12
#11 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#12 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#13 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#14 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#15 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#16 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#17 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#18 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#19 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#20 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#21 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#22 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#23 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#24 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#25 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#26 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#27 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#28 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#29 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#30 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#31 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#32 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#33 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#34 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#35 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#36 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#37 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#38 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#39 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
#40 0x585dfc in Catalog::countPageTree(Object*) /home/jiuge/桌面/xpdf_NB/xpdf-4.04/xpdf/Catalog.cc:567:12
```

in __sanitizerStackDepotBase __sanitizerStackDepotNode, 1, 20Put(__sanitizerStackTrace, bool).png
(115.36 KiB) Viewed 4574 times

derekn



Re: stack_overflow

📅 Thu Jun 09, 2022 8:03 pm

That's due to an object loop in the PDF file. I'm planning to implement a more robust loop checker in Xpdf 5.



Post Reply ↩



2 posts • Page **1** of **1**

< [Return to "Xpdf open source"](#)

Jump to ▼

[🏠 Board index](#)

[🗑 Delete cookies](#) All times are UTC

Powered by [phpBB®](#) Forum Software © phpBB Limited

[Privacy](#) | [Terms](#)