stack_overflow

Post Reply Search this topic... 2 posts • Page 1 of 1

H00K1998

stack_overflow

Sun Jun 05, 2022 8:16 am

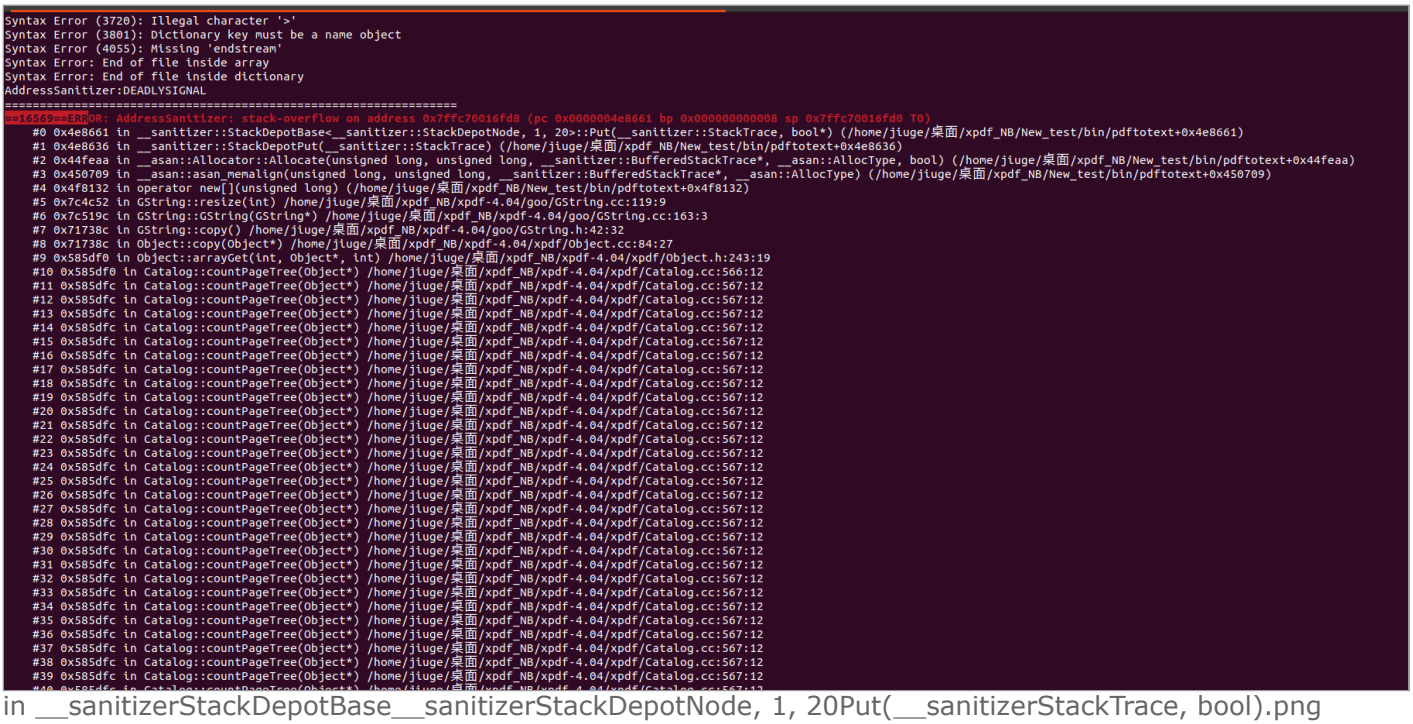
Hello, friend, I have a crash during fuzz test, it seems to be a stack overflow, can you take a look.
thank you

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 amd compile.tar
(7 KiB) Downloaded 146 times



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.

Powered by phpBB® Forum Software © phpBB Limited

Privacy | Terms