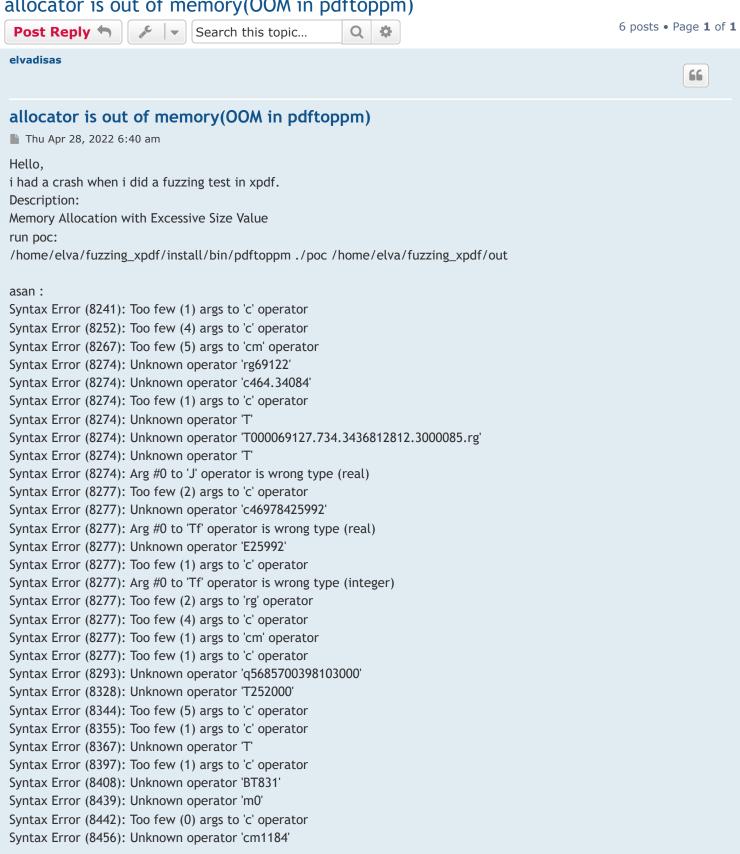


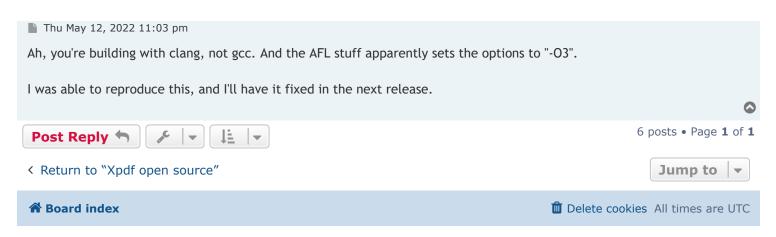
## allocator is out of memory(OOM in pdftoppm)



==486377==ERROR: AddressSanitizer: requested allocation size 0x26bfff68a20 (0x26bfff69a20 after adjustments for alignment, red zones etc.) exceeds maximum supported size of 0x10000000000 (thread T0) #0 0x4ce7cd in malloc (/home/elva/fuzzing\_xpdf/install/bin/pdftoppm+0x4ce7cd) #1 0x7fe487 in gmalloc64(unsigned long) /home/elva/fuzzing\_xpdf/xpdf-4.04/goo/gmem.cc:271:13 #2 0x7fe487 in gmallocn64(int, unsigned long) /home/elva/fuzzing\_xpdf/xpdf-4.04/goo/gmem.cc:288:10 ==486377==HINT: if you don't care about these errors you may set allocator\_may\_return\_null=1 SUMMARY: AddressSanitizer: allocation-size-too-big (/home/elva/fuzzing\_xpdf/install/bin/pdftoppm+0x4ce7cd) in malloc ==486377==ABORTING POC is in ATTACHMENT. Thank you. **ATTACHMENTS** poc.rar (31 KiB) Downloaded 77 times derekn 66 Re: allocator is out of memory(OOM in pdftoppm) Mon May 02, 2022 9:11 pm I can't reproduce this problem. Can you double-check that you attached the correct POC PDF file? Which compiler and version are you using? Thanks. elvadisas 66 Re: allocator is out of memory(OOM in pdftoppm) ■ Thu May 05, 2022 2:01 am hello, thank you for your reply:-) My testing enviorment: --Tested on Ubuntu 20.04.2 LTS x86\_64,AFL++ --gcc version 9.3.0 --xpdf version xpdf 4.04 https://dl.xpdfreader.com/xpdf-4.04.tar.gz POC is in the ATTACHMENT. Screenshot is also in the ATTACHMENT. Pls double-check~~~ Thanks. **ATTACHMENTS** screenshot.rar (76.09 KiB) Downloaded 64 times poc.rar (31 KiB) Downloaded 67 times

## derekn 66 Re: allocator is out of memory(OOM in pdftoppm) ■ Wed May 11, 2022 10:26 pm I've tried with gcc 5.5.0 and gcc 11.2.0 (that's what I have on my dev machines), with asan, and I'm still not seeing a crash. What was your cmake command to configure xpdf before compiling? elvadisas 66 Re: allocator is out of memory(OOM in pdftoppm) h Thu May 12, 2022 2:18 am Hello, derekn you can reproduced the bug by the following steps: mkdir build\_asan cd build\_asan cmake -DCMAKE\_BUILD\_TYPE=Debug \$HOME/fuzzing\_xpdf/xpdf-4.04 -DCMAKE\_INSTALL\_PREFIX=\$HOME/fuzzing\_xpdf/install/ -DCMAKE\_CXX\_COMPILER=afl-clang-fast++ AFL\_USE\_ASAN=1 make sudo AFL\_USE\_ASAN=1 make install \$HOME/fuzzing\_xpdf/install/bin/pdftoppm -f 1 \$HOME/fuzzing\_xpdf/poc \$HOME/fuzzing\_xpdf/output POC file and more screenshots are in the ATTACHMENTS. My Testing Environments: --Tested on Ubuntu 20.04.2 LTS x86\_64,AFL++ --gcc version 9.3.0 --xpdf version xpdf 4.04 https://dl.xpdfreader.com/xpdf-4.04.tar.gz you can try it:-) **ATTACHMENTS** screenshot.rar (76.09 KiB) Downloaded 57 times poc.rar (31 KiB) Downloaded 75 times derekn 66

Re: allocator is out of memory(OOM in pdftoppm)



Powered by phpBB® Forum Software © phpBB Limited Privacy | Terms