Stack contamination caused by stack overflow

H00K1998

Stack contamination caused by stack overflow

Mon Jun 06, 2022 3:32 pm

Hi, I encountered a stack overflow while testing Fuzz

My system OS: Ubuntu 20.10

mkdir build
export LLVM_CONFIG="llvm-config-11"
export CC=afl-gcc-fast CXX=$HOME/AFLplusplus/afl-clang-fast++
cmake -DCMAKE_BUILD_TYPE=Release -DCMAKE_INSTALL_PREFIX=build/
AFL_USE_ASAN=1 make
sudo AFL_USE_ASAN=1 make install

gdb log:
==70695==ERROR: AddressSanitizer: stack-overflow on address 0x7ffc48e94ee8 (pc 0x00000050b8ec bp 0x7ffc48e95760 sp 0x7ffc48e94ef0 T0)
gdb>>> exploitable
Description: Access violation during branch instruction
Short description: BranchAv (4/22)
Hash: e4e4ba5ba34bd4645f94bf68744ab019.db0147337c4a91cc3427b3c0bf5b5a34
Exploitability Classification: EXPLOITABLE
Explanation: The target crashed on a branch instruction, which may indicate that the control flow is tainted.
Other tags: StackOverflow (11/22), AccessViolation (21/22)

ATTACHMENTS

poc.zip
(907 Bytes) Downloaded 164 times

derekn

Re: Stack contamination caused by stack overflow

Thu Jun 09, 2022 8:07 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.