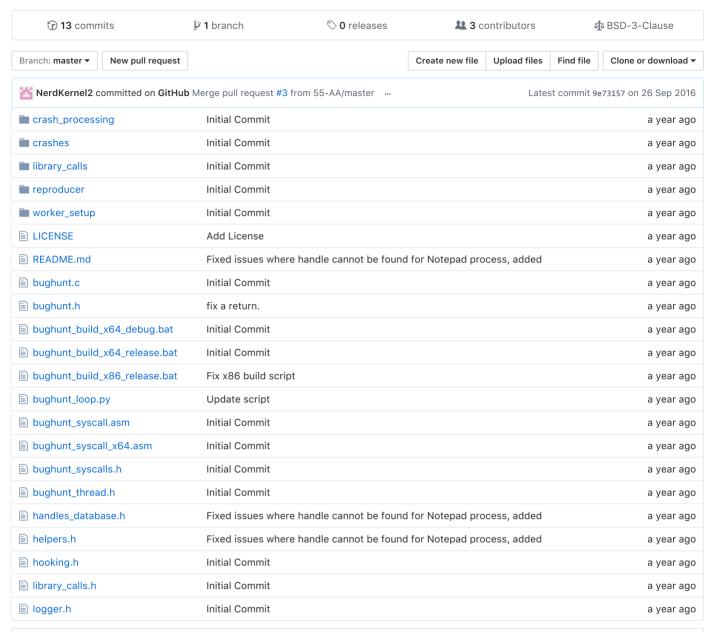
mwrlabs / KernelFuzzer

Cross Platform Kernel Fuzzer Framework



■ README.md

KernelFuzzer

This is the core Kernel Fuzzer, with example library calls and Syscalls to start fuzzing Windows. The fuzzer has been tested on Windows 7 / 10, OS X and QNX.

#Getting started

- Download and install Python 3.5
- Compile binary for your system using the included .bat scripts for the correct architecture (Windows only!). Tested using Visual Studio 2013 if you use a different version of VS, edit the script to point at your copy of 'vcvarsall.bat'.
- Run worker_setup/worker_setup.py

The script should setup the VM as required, reboot and start the fuzzer.

#Writing modules / syscalls

See our Def Con 24 slides over at [MWR Labs] (https://labs.mwrinfosecurity.com/publications/platform-agnostic-kernel-fuzzing/) which give an explanation of the fuzzer and examples of writing library calls and syscalls for the fuzzer. One of each is provided as an example and more examples are provided in the slides.

#Database If you wish to send your crashes to a CouchDB instance, this needs to be setup seperately, then edit the bughunt_loop.py scipt with the required information.

#Contact Feel free to submit issues or ping us on Twitter - [@NerdKernel] (https://twitter.com/NerdKernel) / [@munmap] (https://twitter.com/munmap).