mwrlabs / **KernelFuzzer**

Cross Platform Kernel Fuzzer Framework

13 commits | **1** branch | **0** releases | **3** contributors | BSD-3-Clause

Branch: **master** | New pull request | Create new file | Upload files | Find file | Clone or download

NerdKernel2 committed on **GitHub** Merge pull request #3 from 55-AA/master ... Latest commit 9e73157 on 26 Sep 2016

crash_processing	Initial Commit	a year ago
crashes	Initial Commit	a year ago
library_calls	Initial Commit	a year ago
reproducer	Initial Commit	a year ago
worker_setup	Initial Commit	a year ago
LICENSE	Add License	a year ago
README.md	Fixed issues where handle cannot be found for Notepad process, added	a year ago
bughunt.c	Initial Commit	a year ago
bughunt.h	fix a return.	a year ago
bughunt_build_x64_debug.bat	Initial Commit	a year ago
bughunt_build_x64_release.bat	Initial Commit	a year ago
bughunt_build_x86_release.bat	Fix x86 build script	a year ago
bughunt_loop.py	Update script	a year ago
bughunt_syscall.asm	Initial Commit	a year ago
bughunt_syscall_x64.asm	Initial Commit	a year ago
bughunt_syscalls.h	Initial Commit	a year ago
bughunt_thread.h	Initial Commit	a year ago
handles_database.h	Fixed issues where handle cannot be found for Notepad process, added	a year ago
helpers.h	Fixed issues where handle cannot be found for Notepad process, added	a year ago
hooking.h	Initial Commit	a year ago
library_calls.h	Initial Commit	a year ago
logger.h	Initial Commit	a year ago

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).