google / **syzkaller**

syzkaller is an unsupervised, coverage-guided Linux system call fuzzer

#linux #kernel #fuzz-testing #fuzzing #fuzzer #testing #security #security-vulnerability #security-tools

1,452 commits | **3** branches | **0** releases | **28** contributors | Apache-2.0

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

billy-lau committed with **dvyukov** sys/linux: include additional header to ion.txt ... Latest commit `d335103` a day ago

Godeps	vendor: update all packages	2 months ago
dashboard	dashboard/app, syz-ci: upload target OS/arch to dashboard	11 days ago
docs	Update found_bugs.md	a day ago
executor	sys/windows: add more descriptions	2 days ago
pkg	pkg/kd: add KD protocol decoder	2 days ago
prog	all: initial support for fuchsia	9 days ago
sys	sys/linux: include additional header to ion.txt	20 hours ago
syz-ci	dashboard/app, syz-ci: upload target OS/arch to dashboard	11 days ago
syz-fuzzer	syz-fuzzer: port to windows	2 days ago
syz-hub	syz-manager: don't save/send to dashboard repros from hub	2 months ago
syz-manager	vm/gce: windows support	2 days ago
tools	sys/windows: add more descriptions	2 days ago
vendor	vendor/golang.org/x/net/context/: fix fmt with Go 1.8	2 months ago
vm	pkg/kd: add KD protocol decoder	2 days ago
.clang-format	buildbot: add .travis.yml	2 months ago
.gitignore	sys: check in generated files	4 months ago
.travis.yml	travis: another guess at right packages and syntax	10 days ago
AUTHORS	Parse incdir "incdir" in syscall description file to add custom inclu...	3 months ago
CONTRIBUTORS	Add Isolated VM	2 months ago
LICENSE	initial commit	2 years ago
Makefile	sys/windows: add more descriptions	2 days ago
README.md	readme: add travis-ci status	2 months ago

README.md

syzkaller - linux kernel fuzzer

build passing

`syzkaller` is an unsupervised coverage-guided Linux kernel fuzzer.

The project mailing list is syzkaller@googlegroups.com. You can subscribe to it with a google account or by sending an email to syzkaller+subscribe@googlegroups.com.

List of found bugs.

Documentation

- How to install syzkaller

- How to use syzkaller
- How syzkaller works
- How to contribute to syzkaller
- How to report Linux kernel bugs

External Articles

- Kernel QA with syzkaller and qemu (tutorial on how to setup syzkaller with qemu)
- Syzkaller crash DEMO (tutorial on how to extend syzkaller with new syscalls)
- Coverage-guided kernel fuzzing with syzkaller (by David Drysdale)
- ubsan, kasan, syzkaller und co (video) (by Florian Westphal)
- Debugging a kernel crash found by syzkaller (by Quentin Casasnovas)
- Linux Plumbers 2016 talk slides
- syzkaller: the next gen kernel fuzzer (basics of operations, tutorial on how to run syzkaller and how to extend it to fuzz new drivers)

Disclaimer

This is not an official Google product.