

Artifact Evaluation for "Demystifying the Dependency Challenge in Kernel Fuzzing"

ABSTRACT

This artifact is for the paper "Demystifying the Dependency Challenge in Kernel Fuzzing" in ICSE 2022 Technical Tracks.

Fuzz testing operating system kernels remains a daunting task to date. One known challenge is that much of the kernel code is locked under specific kernel states and current kernel fuzzers are not effective in exploring such an enormous state space. We refer to this problem as the dependency challenge. We undertake a substantial measurement study to systematically understand the

real challenge behind dependencies. In one word, the artifact is to help researchers to understand the dependency challenge in kernel fuzzing.

We want to claim Reusable and Available badges, and more detail is in STATUS.

As for the technology skills assumed by the reviewer evaluating the artifact, we have made almost everything ready in the virtual machine, so it only needs basic familiar of the Linux, and to know a little about Python to configure some numbers in the script.