

Linux Plumbers Conference 2024



Contribution ID: 394

Type: **not specified**

Lessons from the Buzz

Thursday 19 September 2024 10:30 (30 minutes)

In 2023, we open sourced `buzzer`: A library to construct random, syntactically valid, eBPF programs, with the objective of validating the security assumptions of the verifier. Since then we have also developed new features into `buzzer` like coverage tracking and support for things like function calls and BTF.

The purpose of the talk is to share some of the lessons learned, what did/didn't work when finding the CVEs `buzzer` has discovered and what angles of eBPF could be fuzzed in the future.

Primary author: LOPEZ JAIMEZ, Juan Jose (Google)

Presenter: LOPEZ JAIMEZ, Juan Jose (Google)

Session Classification: eBPF Track

Track Classification: eBPF Track