Contribution ID: **337**

Type: **not specified**

syzbot ci: continuous patch series fuzzing

For the past 9 years, syzbot has reported more than 13,000 findings to the Linux kernel mailing by continuously fuzzing upstream Linux trees. However, a notable latency often exists between the introduction of a bug and its discovery, complicating and delaying its resolution. Many regressions, including build/boot failures and shallow bugs, can stall the broader fuzzing effort once they land.

To address this, we introduce syzbot ci, a proof-of-concept system engineered to shift fuzzing left in the kernel development cycle. syzbot ci monitors a number of Linux kernel mailing lists, automatically applies incoming patch series to an automatically determined base tree, and initiates a targeted fuzzing campaign specifically on the code paths modified by the patches. The core assumption is that this focused approach can uncover bugs significantly faster than broad, continuous fuzzing.

As of September 2025, the system has already sent reports with findings to over 50 patch series during their review on the mailing lists.

This talk will cover the functionality of syzbot ci and share the preliminary results and insights. The goal is to gather initial feedback from kernel developers and to discuss the future direction and areas of focus for the project.

Primary author: NOGIKH, Aleksandr (Google)

Presenter: NOGIKH, Aleksandr (Google)

Session Classification: Kernel Testing & Dependability MC

Track Classification: Kernel Testing & Dependability MC