Linux Plumbers Conference 2024

Contribution ID: **89**　　Type: **not specified**

Integer Overflow Prevention

Friday 20 September 2024 10:45 (45 minutes)

Integer overflows are a constant source of security problems. Someone needs to do something about it. We'll discuss new approaches using static analysis and runtime sanitizers. These approaches will require creating new rules for writing safe code. Most integer overflows are "harmless". For example, we used to have repeated security issues related to passing negative sizes to copy_from_user() but eventually Kees added a check for that so now passing a negative is "harmless". Under the new rules, many integer overflows which were "harmless" are now considered a bug. We want the new rules to be as effective as possible while balancing that against the burden of dealing with false positives.

Primary authors: CARPENTER, Dan (Oracle); STITT, Justin (Google); COOK, Kees (Google)

Presenters: CARPENTER, Dan (Oracle); STITT, Justin (Google); COOK, Kees (Google)

Session Classification: Birds of a Feather (BoF)

Track Classification: Birds of a Feather (BoF)