

Linux Plumbers Conference 2025



Contribution ID: 485

Type: **not specified**

ReLaunch Revisited: A Refresher on TrenchBoot Late Launch

Saturday 13 December 2025 11:10 (20 minutes)

As Secure Launch approaches its integration into the kernel, this presentation will revisit the Secure ReLaunch capability. We will conduct a thorough review of D-RTM “late launch” and discuss the various use cases it addresses. Additionally, a brief exploration of the TrenchBoot project’s approach to “late launch” through Secure ReLaunch will be included. The session will conclude with a roadmap discussion and an opportunity for audience questions.

Primary author: SMITH, Daniel (Apertus Solutions, LLC)

Co-author: KIPER, Daniel

Presenters: KIPER, Daniel; SMITH, Daniel (Apertus Solutions, LLC)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC