



ZeroSight

ZeroSightで脆弱性発見を自動化

ZeroSightは、ARMのシステムコンポーネント向けファザー。

ARMのプロセッサ支援機能CoreSightを用いたハードウェアモードとソフトウェアモードを開発。

Linux kernel 4.4.0では、9日間でLinuxカーネルのバグを326,681回観測。

ハードウェアモード

ARMのホスト上のCoreSightとVirtualization Extensionを用いて高速にカーネルファジングを可能にする。

ソフトウェアモード

QEMU上で実装されたソフトウェアモードはx86のホストでファジングが可能。

見つかったカーネルクラッシュのリスト
https://github.com/roppinhoppin/kernel_crashes