Contribution ID: **71** Type: **not specified**

What's Left After openat2?

Monday 24 August 2020 07:05 (20 minutes)

openat2 landed in Linux 5.6, but unfortunately (though it does make it easier to implement safer container runtimes) there are still quite a few remaining tricks that attackers can use to attack container runtimes. This talk will give a quick overview of the remaining issues, some proposals for how we might fix them, and how libpathrs will make use of them. In addition, a brief update on libpathrs will be given.

Examples of attacks include:

- Fake /proc mounts.
- Bind-mounting on top of magic-links (such as /proc/$pid/attr/exec).

I agree to abide by the anti-harassment policy

I agree

Primary author: Mr SARAI, Aleksa (SUSE LLC)

Presenter: Mr SARAI, Aleksa (SUSE LLC)

Session Classification: Containers and Checkpoint/Restore MC

Track Classification: Containers and Checkpoint/Restore MC