CVE Upgrades

- Requirements
  - StarlingX shall continually monitor the open source components used and update them as needed for CVE issues
  - StarlingX shall continually monitor CVE reports against its own unique components and address them
- Primary / First Responder responsibility belongs to the Security team
  - Question: Do we have CVE monitoring scripts in place and reporting?
  - Security processes are well defined: https://wiki.openstack.org/wiki/StarlingX/Security
- In general we rely on upstream component providers (e.g. CentOS, OpenStack) to address CVEs in their software and will incorporate fixes during the rebasing cycle.
- The Security team may request a update for a higher priority CVE as needed

CVE Upgrade Plan / Resourcing

- Scanning of upstream repos for CVES is in place (RPM based)
- Distro.* teams to address Med/Low CVE issues during their rebase cycles
- Distro.* teams need to allow for resolving High CVE issues at any time
- Flock service teams should handle incoming CVE reports urgently in the unlikely event that we receive any