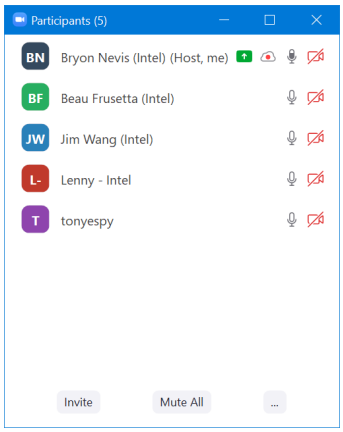
EdgeX Security WG Meeting

https://wiki.edgexfoundry.org/display/FA/Security+Working+Group

July 21, 2021

Attendees



Standing Agenda

- Backlog progress sheet (todo- fixme)
- Review Security Board

Icebox	New	Backlog	WIP	Done
9	1 (+1)	10 (→2)	3 / 0	3

- Securing Consul Board

Ph-3 ToDo	Ph-2 ToDo	WIP	Done
4	1	0 / 0	3

- Review CIS docker scan (will skip unless something changes)
- Review Snyk (will skip unless something changes)

Critical	High	Medium	Low

0	40 (-1)	19 (+1)	6 (unch)

    - Remediated but not yet showing:
        - device-coap(-arm64) -24H -8M
        - Scanning DockerHub -- need to get CLI-based scanning enabled to get early results for next version
    - Next target:
        - device-gpio (10H, 6M) in go.mod
            - No fix currently available
    - To disposition:
        - https://app.snyk.io/org/edgex-jenkins/projects - filter on secretstore-setup
        - Plan to upgrade to `github.com/dgrijalva/jwt-go@4.0.0 once released`

Agenda

- Discussion: ways to make the snap easier to use for Hackathons
    - Ask: dynamically disable security for an EdgeX instance in snap.
    - Background: Snap-based hackathon is targeted at Ireland, but we've now locked down Consul. Previously, it was possible to turn off security by stopping the security services in the snap and restarting the snap. (Secretstore environment variable was dynamically configured by querying status of the secretstore.) This was an unintended consequence if hardening Consul.
    - Would never do this in production, but it would be useful for developers.
    - Is there a way to avoid running the consul bootstrapper that sets up consul security? Idea: maybe turn off acl in consul config based on secretstore service status? Only have "gadget snaps" to feed configuration into a snap.
    - Current workaround: have added two generic service tokens "app-hackathon" and "application-service" that are available for the hackathon. This is secure: tokens are only available if a content interface exists, which requires user to specifically allow.

Action Items

- 7/14: Bryon: Update known security issues with Snyk findings
- 7/14: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.
- 7/21: Tony: File issue to allow configuration.toml setting to change default token TTL. (cmd/security-secretstore-setup/res/filetokenprovider.toml)