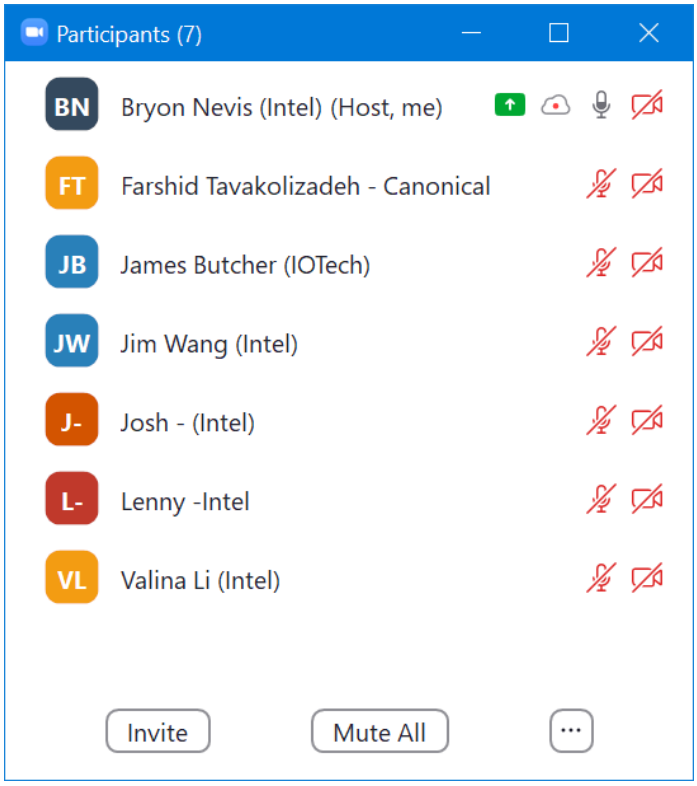
EdgeX Security WG Meeting

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

July 13, 2022

Attendees



Agenda

- New attendee - Joshua Silverio
    - One of IOTG's scrum teams working on EdgeX work. Previously a solutions engineer working on retail use cases.

- From TSC update today
    - Starting to make some progress working through the backlog; expecting to accelerate in the coming weeks. (Thank you Valina)
    - Interesting email discussion with Snyk–they expect CVE fixes to be identical across branches; security engineers actually look into the code for the fix before posting it. (Thank you Jim and Valina)

- Snyk update - added scanning of LTS release - issues to be dispositioned - volunteers?
    - On or after 21 July we need to go and edit the scan interval for jakarta synk tests to monthly (currently locked right now)
    - AR: Submit PR against github.com/canonical/edgex-snap-hooks to update testify to non-CVE version.and notify Farshid. (go-mod-outdated, and update)
    - AR: Bryon: edgexfoundry/app-service-configurable:jakarta:go.mod - need to disposition in snyk and update security wiki regarding AES encryption
    - https://www.cve.org/CVERecord?id=CVE-2021-38561 needs to be dispositioned as to whether we are affected.
    - Dispositioning jakarta issues is priority

- Farshid: determine CVE fixing priority for testing tools?
    - Do we need to patch vulnerabilities in testing tools? e.g. testify library
    - For a unit test support library, would not patch an LTS because of it because doesn't have a runtime impact. But would patch opportunistically if had to re-release LTS for another reasons.
    - Have existing policy for non-test code.

- Proposed list of metrics from two weeks ago (would be implemented in go-mod-bootstrap for most)
    - Will have chicken and egg problem for some of these (metrics would be collected but not reported until message bus is up; and what about services that don't ever use a message bus? Implementation TBD)
    - **Counter - secret requested from the store**
    - Counter - consul token requested
    - Counter - put secret
    - **Timer - how long to obtain secret token**
    - Timer - how long to obtain consul token
    - (stretch - spiffe-token-provider metrics)
        - Counter - every token requested
        - Timer - how long does it take go return a new token
        - Counter - known secret requested (tag by secret name)
- TODO: Add two bold ones to the backlog

Standing Agenda

- Review Security Board
- Securing Consul Board (skip)
- Review CIS docker scan (will skip unless something changes) (click latest run, go to classic, view console output).
    - Last checked: Tue Nov 16 05:36:01 UTC 2021

- Review Snyk (Jenkins) (will skip unless something changes) (Imagelist)
- Review action items from previous week

Action Items

- 7/14/21: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.
- 6/22/22: Bryon: Update known security issue wiki (add GHSA?)