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

August 3, 2022

Attendees

<table>
<thead>
<tr>
<th>Participant</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>BN</td>
<td>Bryon Nevis (Intel) (Host, me)</td>
</tr>
<tr>
<td>BM</td>
<td>Brian McGinn (Intel)</td>
</tr>
<tr>
<td>FT</td>
<td>Farshid Tavakolizadeh - Canonical</td>
</tr>
<tr>
<td>JW</td>
<td>Jim Wang (Intel)</td>
</tr>
<tr>
<td>JW</td>
<td>Jim White</td>
</tr>
<tr>
<td>VL</td>
<td>Valina Li (Intel)</td>
</tr>
</tbody>
</table>

Agenda

- CVE-2022-28948 dispositioning results
  - Yaml parsing issue
  - Will save for future
- Consul’s KV organization and security implications / tech-debt
  - Security bootstrapper creates per-service Consul policies
  - Each service is allowed only access to its section of the KV store
  - KV store is divided into buckets
    - Core services
- Security services
- Device services
- App services
  - PROBLEM: each microservices gets to decide independently whether it is part of core, security, device, or app services
    - When we create the policy we know the known service keys
    - But generally don’t know without special logic whether core-data is part of core, or an app service belongs to the app services section
    - As a result, we have to do string parsing on the service key and write custom ACL paths such that “app-” goes into edgex/appsservices/2.0, and “security-” goes into edgex/security/2.0 and “device-” goes into edgex/device/2.0, and everything else into “edgex/core/2.0”
    - Any service that violates the service key naming convention will not have access to consul set up properly
    - Any new types of services such as “wizbang-somename” will get classified as core.
    - UI team has the same problem.
    - **Proposal:** Edgex 3.0 uses edgex/3.0/<service-key> as the path, and eliminate the extra “appservices, security, core, devices” subfolders in the path.
      - This would also remove a parameter to bootstrap.run()
    - Potential snags? Is it possible to have multiple instances of a device service that have the same service key?
      - Answered question about what happens if a service goes offline for more than an hour.

### 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: August 3, 2022 – as expected
- [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?)