# **EdgeX Security WG Meeting, 03/11/2020**

**Attendees:** Trevor, Anthony, Bron, Colin, Diana, Jim Wang, Jim White, Lenny, Mike, Tony, Tingyu, Malini

## **Agenda**

## Blackbox Tests:

## Security audit: Snyk report & process

## Proxy awareness of new App & Device services

* Configuration consistency across the Fuji/Geneva
* Follow up from last week – how often do we need to update/patch the product based on Synk/Clair report?

**Blackbox Tests broken:**

 Jim White has initiated email chain to bring together all relevant parties to get this back on track. Trevor, Lenny, Bryon have all provided input.

 **App & Device Services can be added dynamically, how do we thread into Proxy**

Lenny

Just putting the base route is adequate for all the known services. But App and Device services are dynamic. How do these get added to Kong. The SDK allows developers to add these dynamic services.

The proxy has a config file for all the standard services.

Similar to the issue of per-service vault tokens. Bryon had an environment variable proposal.

Tony: could we use self-seeding.

Lenny: how do we protect it

Tingyu: you need to have access to the admin port to do so.

Also Proxy config can be passed through the command line.

Lenny: if you point it to a different config file, still need to mount it.

Malini: do we need to check that the port is not used before.

Lenny: Need a map <service> to <port>

**Environment variable: key-value pair like the above. A comma**  **separate list of these. Additional routes. (decision)Tingyu**

Bryon: automatic is not possible at this stage because there is an initialization order. We trust docker-compose today.

We do not trust clients to contact consul.

Same approach nice.

Lenny: slightly different, because here value pair, the secrets is just the service key.

Internally translate the config file secretservice to secretstore that go-mod-secrets expects. Basically leave the inconsistency for now 1.2 and we change it for 2.0 release.

**Bryon, Trevor (& QA), Jim : we have no upgrade path for the configuration files. Need to look at this now. Jim will add this to arch review**

Tony: Snaps have epochs to prevent someone updating from one version to another.

**Jim White: Please consider adding a comment/annotation saying that something may. be deprecated. Toml also supports comments. Whereever we plan to introduce breaking changes. TODOs**

**Configuration consistency across Fuji/Geneva**

Tingyu showed the current config.

Tony: nice to not keep changing config file formats with each release

Lenny: secret store has expanded from Fuji. An App Service added in Fuji – additive. Things like retries, retry period etc will be default values since the old config would not have specified for them.

Trevor: additive changes OK, use and document default settings

Tony: if just name change, **support both of them in our code**. Might even want to change the paths to things like cert paths. It is configurable so we should expect people to modify it. Pick one as the naming convention going forward and keep using it going forward, but support both.

**Security Audit: Snyk report & process**

Week ofMarch 11, no new issues.

* What strategy should we take if there is another high priority security issue coming right after a security update? Need DevOp’s input as well. A guidance is needed.
* Need balance between addressing urgency vs. frequency.

How often do we need to update the product ?

James Gregg: I would suggest waiting until we have full continuous delivery automated so that release artifacts can be remediated and published after successful validation.
In terms of our "INTEL" policy - we have remediation guidelines that require both high / med CVEs to be fixed within the following timelines
High = 30 days
Medium = 60 DAYS
To Trevor's point, it makes sense to only install the suggested fixes if the fix is a formal release, not a rc - release candidate

Should we bump up the version number of all containers or just the patched one .. Malini – would not bumping up all the versions result in more network traffic during updates on real IoT/Edge devices? \*\*\*

Release Frequency – should be decided by Security WG based on severity of the issue.

**On version bump – Conclusion Trevor/DevOps WG: : only bump the affected container \*\*\* Good!**

**Incremental patch number <major>.<minor>.<patch>**

**Jim: Lets re-visit this in arch meeting .. when we are patching our EdgeX code due to a CVE in our own code.**

Trevor: Do we release at some cadence. JQ is a command line tool, any number of CVEs is possible.

**Jim White: Case by case basis, working with James Gregg/SIR team.** Jim cautions that while the granularity is just High, Medium, Low, sometimes its theoretical, we do not use it, and sometimes it really affects. So document each and in the last case fix. Also when did this surface in the context of when our regularly scheduled release coming out, to avoid churn.

Tony says above practice in Ubuntu. Tingyu, we need to acknowledge.

Trevor: Workflow

1) Create a PR

2) James runs Snyk tool to be sure new container does not have the H, M, L that was supposed to be fixed

3) James then runs the full blackbox test suite using the updated container to be sure nothing is broken

4) All good? Then PR merged.