EdgeX Security WG Meeting, 03/18/2020

Attendees: Jim White, Trevor, Diana, Bryon, Eno, Tony, Jim Wang

Agenda

- Security audit: Snyk report & process
- Bound checking issue
- Handling Database credentials

Consul Handling of embedded structures
https://github.com/edgexfoundry/edgex-go/issues/2433
Lenny and Bryon – embedded structure versus a flat dictionary/map. Fix is not to embed structures because Consul package mishandling.
Not Hashicorp handles toml files correctly but not these embedded structures.

Lenny recommends combing through our code base to check for similar patterns and eliminate. He has already fixed authentication.
Bryon on discovering this helped get Blackbox tests unblocked.

A) Secret store info, secret config.
B) In general for the services – review the config structures for embedded structs
AR (action required) for Core Data. Might be fine because we have not run into issues prior to this.
Structure name on the left side and no type associated with
Type on the right side is composing it versus embedding it.

Security Audit: Snyk Reports and Process
No new issues flagged over the last week.
But issue https://github.com/edgexfoundry/edgex-go/issues/2439 reported
Which could manifest as a denial of service attack.

CBOR data handling

https://github.com/edgexfoundry/edgex-go/issues/2439

Jim: Any way to check before going in that the data is malformed?
Tony: need to check the CBOR spec. We could have a similar issue even with JSON.
Jim: this is not just specific to Go. Could be in C too.
Bryon: Something easy to do – http header – content length – if it is too long decline to propose as a bounds checking.
Tony: CBOR is a variant of JSON.
Jim: Is the sender trusted? Or is this an attempt to cause a denial of service
Tony: How did we receive this bad payload? Our SDK? Our client?
Trevor: Looking at the currently used library. Bug in the library? Switch CBOR library.
AR: check on library. Pinged Tobias Mosby – recall him working on CBOR.

Generic Bound Checking issue:

This was brought up Jim, a follow up from last week's architecture meeting, and related to the issue 2439.