Security SIG Roadmap 2019

There are three areas that the Security SIG wants to focus on for 2019. Those areas are Policies and Procedures, Vulnerabilities, and Role Based Access Controls.

Policies and Procedures

This section is about how the Security SIG handles incoming security vulnerabilities and how we can put up safeguards as to not accidentally introduce dependencies with more vulnerabilities

- Define a process for handling incoming security vulnerabilities to make sure they get patched in a timely fashion
- Define a process for getting CVE numbers
- Have automating scanning of PRs to the spinnaker-dependency project to detect if an update or new library will introduce a new security vulnerability
- Setting up integration tests for Fiat to verify basic functionality

Vulnerabilities

This section is dealing with already known security vulnerabilities

- Upgrade to Spring Boot 2.0 - In Progress by Rob Z from Netflix
- Move to gradle 5.0
- Clouddriver ZipSlip
  - Fix: https://snyk.io/research/zip-slip-vulnerability
  - https://github.com/spinnaker/clouddriver/blob/master/clouddriver-artifacts/src/main/java/com/netflix/spinnaker/clouddriver/artifacts/ArtifactUtils.java#L46
- Work on patching P1 issues in https://docs.google.com/spreadsheets/d/1GxVTKN4nIHX0wjmvX85WNVD6LBKhcKOLy-MEcWNraro/edit#gid=1294484019
  - Some of these will go away once upgrading to Spring Boot 2.0

Role Based Access Control

Having everyone have access to everything in Spinnaker is not something many enterprises will allow. Role Based Access Control (RBAC) is how we can lock down parts of Spinnaker based on what role a given user has. This section covers improving the RBAC experience within Spinnaker.

- Expand RBAC for Pipelines
        - Currently if a user has read permission, they can execute a pipeline
- RBAC for controlling access to:
    - Jenkins/Travis
    - Pub/Sub
- RBAC for MPTv2

Quarter Goals for 2019

The goals that have been identified above have been broken down into the quarter in which they will be worked on. If an above goal is not listed below, we hope to have it completed before the end of 2019 Q1.

2019 Q2 Goals

- Continue - Upgrade to Spring Boot 2.0
- Define a process for getting CVE numbers
- Clouddriver ZipSlip
- Work on patching P1 issues
- Move to gradle 5.0
- Expand RBAC for Pipelines

2019 Q3 Goals

- Continue - Move to gradle 5.0
- Continue - Work on patching P1 issues
- Have automating scanning of PRs to the spinnaker-dependency project to detect if an update or new library will introduce a new security vulnerability
- RBAC for controlling access to:
    - Jenkins/Travis
    - Pub/Sub

2019 Q4 Goals

- Setting up integration tests for Fiat to verify basic functionality
- RBAC for MPTv2
-
- Secure Boot for GCP

    - Controllable in a stage or dynamically