Policy for Fixing Vulnerabilities in the ONAP Code Base

DEPRECATED IN GUILIN: REPLACED BY Remediating Known Vulnerabilities in Third Party Packages

In Scope: All security vulnerabilities in the ONAP code base. This includes vulnerabilities in the code, and vulnerabilities related to the configuration of dependent packages, e.g., using default passwords or enabling debug tools.

Out of Scope: Known vulnerabilities in the dependent packages included in the ONAP code base. Examples of dependent packages in ONAP include ODL, com.fasterxml.jackson.core : jackson-databind : 2.8.11.3, org.eclipse.jetty : jetty-util : 9.4.14.v20181114, and djangoframework.

Reminder: All security vulnerabilities found in the ONAP code base must be fixed within 60days in order for the project to retain its CII Passing badge.

ONAP Policy:

- Any security vulnerability found in the ONAP code base must be removed from the ONAP code base within 60 days.
  - Within the 60 days period, the expectations are that the project team will develop and test a resolution for the CVE.
  - The resolution will immediately be candidate for the next candidate release i.e. early drop, minor or major release.
  - An exception may be raised on extra-ordinary issue, but exceptions must be rare and have a well documented rationale.
  - Inter-dependencies between projects:
    - The project containing the vulnerability must immediately notify the projects that have it as a dependency of:
      - the vulnerability
      - the projected timeline for resolution
      - changes to functionality caused by resolution
    - The projects with dependencies must incorporate the new version within 60 days.
- If a project is unable to remove a security vulnerability within the 60 day window:
  - the project should supply a default configuration that prevents execution of the vulnerable code, and
  - the project must add removal of the vulnerable code to the backlog for the next release.
  - the readthedocs for the project must be updated with the vulnerability and the fix
    - The project must present the following:
      - SECCOM Recommendations, following similar process to the IP Legal issues.
      - The reason they could not meet the deadline.
      - The nature of the risk.Any critical CVE that will not be resolved within the 60 day period must be presented to the TSC for review no later than one week before the expiration period (day 53).
  - The TSC will then decide how to proceed.
    - The TSC allows the project more time to fix the vulnerability without changing the upcoming ONAP release date.
      - The resolution of the vulnerability will become the highest priority of the project.
      - If the next release will contain the vulnerability, the CVE for the vulnerability will be documented in the security section of readthedocs.
      - The project must change the answer to CII badging vulnerabilities_fixed_60_days to UNMET.
    - The TSC allows the project more time to fix the vulnerability and delays the upcoming ONAP release date.
      - The resolution of the vulnerability will become the highest priority of the project.
      - The project must change the answer to CII badging vulnerabilities_fixed_60_days to UNMET.