ONAP NEXUS IQ MS information

Introduction

Nexus IQ identifies known vulnerabilities in the components that onap components import. These known vulnerabilities are identified all the way down the dependancy chain.

This has been highlighted as from a security perspective it is better release avoid dependencies with known vulnerabilities.

For this the milestone criteria in ONAP has been updated to include

- MS-3 the project should have looked at the known vulnerabilities and have a plan
- MS-4, RC, no known vulnerabilities of more than 60 days old.

Details

The intention is that moving to the latest release of the dependent code will rectify most situations. If not then the project should capture in the MS template:

- Articfact and version, Vulnerability id (CVE-xxxx), impact analysis, rectification plan, if applicable.

Additional information:

- False positives will not be permanently ruled out as while they may not propose a threat to the way ONAP uses it today, they maybe a threat to the way it is used later.
- If the known vulnerability is on a dependencies a few steps down the line, then the project should report a vulnerability towards that component.
- It maybe that the impact of the vulnerability can be alleviated by the way onap uses the imported components. If so, state that in the impact to onap as "no impact due to ONAP does ...".
- it maybe that the community for that component is no longer active. In such a case; a plan must be in place to address this.

This link is a proposed template to fill in (link)