Beijing CLI Security/Vulnerability Threat Report

This template is intended to be used to document the outcome of the impact analysis related to the known vulnerability reported by Nexus-IQ (CLM tab in Jenkins). Nexus-IQ can identify the known vulnerabilities contained in the components use by onap components.

This table will be presented to TSC at Code Freeze milestone (M4) to the TSC.

It is recommended to **first update to the latest version** of the third party components available. In case the latest third party components still reports some vulnerabilities, you must provide an impact analysis as illustrated in the example below.

In the case where you have nested third party components (a third party component embedding another third party component) and there is **NO CVE** number for the upstream third party component (meaning the third party component you are embedding), it is recommended to open a vulnerability issue on the upstream third party component.

The following table is addressing 2 different scenarios:

- Confirmation of a vulnerability including an action
- False Positive

The information related to Repository, Group, Artifact, Version and Problem Code are extracted from the CLM report (see the below screenshot)

Repository	Group	Impact Analysis	Action
cli [Level: 7 Security]	org.apache. httpcomponents	False Positive ONAP CLI does not allow to access to this libarary, where user can send URL request for malfunction. so there is no impact on the ONAP CLI.	Not applicable
cli [Level: 8 Security]	com.fasterxml.jackson.core	False Positive ONAP CLI does not allow to access to this libarary, where user can malfunction. so there is no impact on the ONAP CLI.	Not applicable
cli [License]	com.github.dreamhead	False Positive. Its MIT licensed	Not applicable
cli [Level: 5 Security]	commons-codec	False Positive Its not direct dependency and is caused via 3rd party lib dependency. And it does not harm anyway to CLI.	Not applicable
cli [Level: 4 Security]	jline	False Positive ONAP CLI does not allow to access to this libarary, where user can malfunction. so there is no impact on the ONAP CLI.	Not applicable

Discussion over ONAP mailing list, pls find here.