VNFSDK Security/Vulnerability Threat Analysis

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.

✓ **Usage**

Please make a **Copy** of this template into your project wiki space. Be sure to make a Copy (not a Move) by using the ... on the top right corner of this page

Within the M4 checklist create a link toward your copy of this template

Once this template has been copied into your project wiki space, you can delete this "Tip" section as well as the "Sample of CLM Report" screenshot. This screenshot is just an example.

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
vnfsdk-refrepo	com.fasterxml.jackson.core	False positive Jackson: can be an issue if we leave on default typing ○ In vnfsdk we do not use default typing. We use strict parsing and validation of deserialized data. ○ There is no unknown source data from which marketplace reads the application data (xml/json).	No Action https://jira.onap.org/browse/VNFSDK-212
vnfsdk-refrepo	org.eclipse.jetty	False positive. This vulnerability refers to a potential timing attack on passwords. • in VNFSDK, we don't use this component for passwords. • This is a nested dependency. We upgraded the top level component to the latest version.	No action
vnfsdk-functest	com.fasterxml.jackson.core	False positive. We do not use default typing in vnfsdk-functest.	no action
vnfsdk-functest	com.github.roskart.dropwizard-jaxws	False positive. The code comes in through a 3rd party dependency, but isn't used in VNFSDK.	Helpdesk ticket 54851
vnfsdk-functest	org.webjars.npm bootstrap	False positive. The code comes in through a 3rd party dependency, but isn't used in VNFSDK.	Helpdesk ticket 54851
vnfsdk-functest	jquery	False positive. The code comes in through a 3rd party dependency, but isn't used in VNFSDK.	Helpdesk ticket 54851