CLAMP R2 - 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.

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

Repository	Group	Impact Analysis	Action
clamp	com.fasterxml. jackson.core	**False Positive** False Positive Explanation: This vulnerability issue only exists if com.fasterxml.jackson.databind.ObjectMapper.setDefaultTyping() is called before it is used for deserialization. https://github.com/FasterXML/jackson-docs/wiki/JacksonPolymorphicDeserialization A centralized custom JacksonUtils class has been developed for CLAMP so that the ObjectMapper created there explicitly disable the default typing feature (the incriminated Jackson Feature) The custom JacksonUtils class is used for Resteasy endpoints and clamp code. A unit test has been added to validate that it's not possible to instantiate a java object based on a JSON in the readValue method call. Concerning the Spring version that CLAMP uses (as it embarks the jackson library too), clamp uses the 4.2.4.RELEASE, which fixes the security problem. Change-id: I1fb11c8fc8e7a53ef832774fa8c06af1c70d3dad Review: https://gerrit.onap.org/r/#/c/38955/1	NA

CLM Report :

You can check the latest CLM report for CLAMP here