SO 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
so/libs	com.fasterxml.jackson.core	False positive Jackson: can be an issue if we leave on default typing • In SO we do not use default typing. We use strict parsing and validation of deserialized data. • There is no unknown source data from which SO reads the application data (xml/json).	No Action https://jira.onap.org/browse/SO-458
	org.jboss.resteasy	Confirmation of vulnerability came from openstack-java-sdk-client-connector; no non-vulnerable jar	No action for Beijing Wait for new openstack-java-sdk-connector
SO	commons-httpclient	Confirmation of vulnerability can be replaced with httpclient-4.5.5.jar and httpcore-4.4.1.jar	Wait for next build ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	com.fasterxml.jackson.core	False positive Jackson: can be an issue if we leave on default typing • In SO we do not use default typing. We use strict parsing and validation of deserialized data. • There is no unknown source data from which SO reads the application data (xml/json).	No Action ~~SO-457~~ CLOSED
	org.camunda.bpm.webapp	Confirmation of vulnerability Both 7.7.0 and 7.8.0 have security threats. There is non-vulnerable Camunda version yet.	Wait for Camunda 7.9.0, which can happen in Casablanca https://jira.onap.org/browse/SO-457

	com.fasterxml.jackson.core	False positive Jackson: can be an issue if we leave on default typing • In SO we do not use default typing. We use strict parsing and validation of deserialized data. • There is no unknown source data from which SO reads the application data (xml/json).	No Action https://jira.onap.org/browse/SO-457
	com.fasterxml.jackson.core	Confirmation of vulnerability It came with Camunda 7.7.0 and 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	commons-fileupload	Confirmation of vulnerability It came with Camunda 7.7.0 and 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	com.fasterxml.jackson.core	Confirmation of vulnerability It came with Camunda 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	com.fasterxml.jackson.core	Confirmation of vulnerability It came with Camunda 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	org.springframework	Confirmation of vulnerability It can be upgraded to 4.3.14.RELEASE	Wait for next building ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	org.springframework	Confirmation of vulnerability It came with Camunda 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	org.springframework	Confirmation of vulnerability It came with Camunda 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	org.springframework	Confirmation of vulnerability It came with Camunda 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	org.springfamework	Confirmation of vulnerability 4.3.12.RELEASE fixed the vulnerability and licensing issue. It can be upgraded to 4.3.1.2.RELEASE	Wait for next build ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	org.apache.commons	Confirmation of vulnerability 1.5 releae fixed the issues, but this 1.2 jar came with Camunda 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	org.apache.httpcomponents	Confirmation of vulnerability 4.5.5 releae fixed the issues, but this 4.3.3.jar came with Camunda 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	ch.qos.logback	False positive SO does not use RemoteStreamAppenderClient Upgraded it to 1.2.3	merged into next build ~~SO-537~~ - remove SO security vulnerability and licensing CLOSED

	org.springframework	Confirmation of vulnerability 4.3.12 releae fixed the issues, but this 3.1.2.jar came with Camunda 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	com.fasterxml.jackson.core	Confirmation of vulnerability 2.9.4 release fixed the issues, but this 2.6.3.jar came with Camunda 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	org.apache.httpcomponents	Confirmation of vulnerability 4.5.5 release fixed the issues, but this 4.3.3.jar came with Camunda 7.8.0	Wait for Camunda 7.9.0, which can happen in Casablanca ~~SO-457~~ - Resolve the critical vulnerabilities in the third party libraries of SO CLOSED
	org.jboss.resteasy	3.1.0.Fianl.jar fixed the vulnerability issue, but no solution for licensing issue yet	merged into next build ~~SO-537~~ - remove SO security vulnerability and licensing CLOSED
	commons-httpclient	replaced with httpclient-4.5.5.jar and httpcore-4.4.1.jar	Wait for next build