Policy R3 Casablanca Security/Vulnerability Threat Template

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.

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
policy/common	com.fasterxml.jackson.core	False Positive - we are not using the Jackson code in the manner that exposes the vulnerability.	Request exception
policy/common	com.fasterxml.jackson.datatype	False Positive - we are not using any DurationDeserializer or InstantDeserializer.	Request exception
policy/drools-pdp policy/drools-applications policy/distribution policy/engine	com.fasterxml.jackson.core	False Positive - flagged due to inheritance of policy/common	Request exception
policy/drools-pdp policy/drools-applications policy/distribution policy/engine	com.fasterxml.jackson.datatype	False Positive - flagged due to inheritance of policy/common	Request exception
policy/drools-pdp	dom4j	This is both a security and a license issue due to Drools v6.5.0.Final including and using this dependency. Upgrading to 7.x version would **not** clear this issue and would result in multiple other license exceptions that are not clearable.	Request exception
policy/drools-pdp	jsoup	This is a security issue due to Drools v6.5.0.Final including this dependency. Upgrading to 7.x version would **not** clear this issue and would result in multiple other new license exceptions that are not clearable.	Request exception
policy/drools-pdp	ant	This is a security issue due to Drools v6.5.0.Final including this dependency. Upgrading to 7.x version **would** clear this issue, but would then consequently result in multiple other new license exceptions that are not clearable.	Request exception
policy/apex-pdp	org.codehaus.jackson.jackson-mapper-asl	This dependency is pulled in by org.apache.avro. We are using the latest version of Avro. We are using Avro to deserialize events. Avro uses jackson-mapper-asl for its Json decoding. The schema for the events we are decoding is controlled in policy models and prevents executable code being specified. Therefore this vulnerability cannot be exploited.	Request exception

policy/apex-pdp	org.python.jython-standalone.2.7.1	This dependency brings in the Jython (Python) interpreter for executing scripts written in Python under the control of Apex. There are two vulnerabilities, both concerning adding extra modules to the Python libraries on a host running Python scripts under Jython. • The setup.py and build_py.py files allow extra python packages to be installed on the host during the startup of Jython. This mechanism uses the setuptools mechanism to install those packages. That mechanism does not enforce path traversal restrictions, allowing malicious packages to access protected areas on the host. • Jython uses packages installed with the python pip utility. Pip is vulnerable to Path Traversal attacks, malicious packages installed with pip can access protected areas on the host The solution is to warn developers not to install malicious extra Python packages.	Request Exception The apex-pdp documentation for the Jython plugin is updated to warn developers that they must ensure that extra python packages they add at install time with PIP or using the setup.py/build_py.py mechanisms must be checked and certified by them as not being malicious.
policy/apex-pdp	dom4j	This dependency is pulled in by hibernate-core. We are using the latest release of Hibernate. The XML schema of incoming events is controlled in Apex and arbitrary code even if it was injected cannot be executed.	Request exception blocked URLPOLICY-1510 - Investigate Apex dom4j OPEN
policy/apex-pdp	org.apache.zookeeper	Liam Fallon - can you take a quick look at the impact?	Request exception
policy/engine	commons-fileupload	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	bootstrap	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	com.fasterxml.jackson.core	False positive The code is not using jackson in the manner described in the vulnerability.	Request exception
policy/engine	org.springframework	One version is flagged due to inclusion of ONAP Portal SDK.	Request exception
policy/engine	org.springframework	We will upgrade other versions not related to ONAP Portal SDK. Possible together, needs investigation.	
policy/engine	bouncycastle	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	com.mchange	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	angularjs angular angular.min.js angular-ui-grid.js angular-sanitize	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	ng-formio-grid	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	wicket-util	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	moment moment	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	xerces	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	commons-beanutils	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	esapi	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	antisamy	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	jquery	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	commons-fileupload	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/distribution	org.springframework	Flagged due to inheritance from policy/engine which has dependency on ONAP Portal SDK	Request exception

Sample of CLM Report