Policy R2 Beijing 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/drools-pdp	com.fasterxml.jackson.core	False Positive - we are not using the Jackson code in the manner that exposes the vulnerability. In addition, the code for this is disabled. https://gerrit.onap.org/r/gitweb?p=policy/drools-pdp.git;a=blob;f=policy-management/src/main/java/org/onap/policy/drools/protocol/coders/ProtocolCoderToolset.java;h=7ee8b08a3f42c30254afa1764905e267823d8d90;hb=refs/heads/master https://gerrit.onap.org/r/gitweb?p=policy/drools-pdp.git;a=blob;f=feature-pooling-dmaap/src/main/java/org/onap/policy/drools/pooling/Serializer.java;h=63aefb7a2c3ad63da25ab1de8341395188279645;hb=refs/heads/master	Request exception or false positive
policy/drools-applications	com.fasterxml.jackson.core	False Positive - flagged due to inclusion of policy/drools-pdp	Request exception or false positive
policy/engine	org.apache.lucene	Due to inclusion of elasticsearch. We are not using elastic search in this release. But it is noted in the CVE that elastic search is NOT subject to this vulnerability: "Elasticsearch, although it uses Lucene, is NOT vulnerable to this."	False Positive
policy/engine	org.springframework	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. There are too many lines to list here.	Request exception
policy/engine	ch.qos.logback	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	org.beanshell	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	angular org.webjars.npm	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	bouncycastle	Flagged due to inclusion of ONAP Portal SDK	Request exception
policy/engine	org.apache.poi	Flagged due to inclusion of ONAP Portal SDK	
policy/engine	javax.servlet	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	xalan	Flagged due to inclusion of ONAP Portal SDK	Request exception

policy/engine	xerces	Flagged due to inclusion of ONAP Portal SDK	Request exception

Sample of CLM Report