DCAE R2 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.

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
dcaegen2/analytics/tca	com.fasterxml.jackson.core	**Vulnerable artifacts:** Dependency com.fasterxml.jackson.core:jackson-databind:jar:2.4.4 *located at* Module org.onap.dcaegen2.analytics.tca:dcae-analytics-aai:jar:2.2.0-SNAPSHOT Dependency com.fasterxml.jackson.core:jackson-databind:jar:2.4.4 *located at* Module org.onap.dcaegen2.analytics.tca:dcae-analytics-cdap-common:jar:2.2.0-SNAPSHOT Dependency com.fasterxml.jackson.core:jackson-databind:jar:2.4.4 *located at* Module org.onap.dcaegen2.analytics.tca:dcae-analytics-cdap-plugins:jar:2.2.0-SNAPSHOT Dependency com.fasterxml.jackson.core:jackson-databind:jar:2.4.4 *located at* Module org.onap.dcaegen2.analytics.tca:dcae-analytics-cdap-tca:jar:2.2.0-SNAPSHOT Dependency com.fasterxml.jackson.core:jackson-databind:jar:2.4.4 *located at* Module org.onap.dcaegen2.analytics.tca:dcae-analytics-common:jar:2.2.0-SNAPSHOT Dependency com.fasterxml.jackson.core:jackson-databind:jar:2.4.4 *located at* Module org.onap.dcaegen2.analytics.tca:dcae-analytics-dmaap:jar:2.2.0-SNAPSHOT Dependency com.fasterxml.jackson.core:jackson-databind:jar:2.4.4 *located at* Module org.onap.dcaegen2.analytics.tca:dcae-analytics-it:jar:2.2.0-SNAPSHOT Dependency com.fasterxml.jackson.core:jackson-databind:jar:2.4.4 *located at* Module org.onap.dcaegen2.analytics.tca:dcae-analytics-model:jar:2.2.0-SNAPSHOT Dependency com.fasterxml.jackson.core:jackson-databind:jar:2.4.4 *located at* Module org.onap.dcaegen2.analytics.tca:dcae-analytics-tca:jar:2.2.0-SNAPSHOT Although the offending dependency appears in all above artifacts, it is only the direct dependent of "dcae-analytics-model". All other uses are transient dependencies through this artifact. Hence the analysis below applies to the "dcae-analytics-model" artifact. **Vulnerability report:** **False Positive Classification Reasoning** There is no use of `BeanDeserializerFactory` class in artifact "dcae-analytics-model". Hence we believe that this vulnerability report is a false positive.	~~DCAEGEN2-412~~ - TCA has dependency on vulnerable com.fasterxml.jackson.core CLOSED
dcaegen2/analytics/tca	com.fasterxml.jackson.core	**Vulnerable artifacts:** <same as jackson-databind 2.4.4 above> **False Positive Classification Reasoning** There is no use of either `UTF8StreamJsonParser` or `ReaderBasedJsonParser` class in artifact "dcae-analytics-model". Hence we believe that this vulnerability report is a false positive.	~~DCAEGEN2-412~~ - TCA has dependency on vulnerable com.fasterxml.jackson.core CLOSED

dcaegen2 /platform /inventory-api	com. fasterxml .jackson. core	**Vulnerable artifact:** **False Positive Classification Reasoning** According to these description, and the fact that the org. onap.dcaegen2.platform:inventory-api code does not enable use of global type information, using Class name as the type id, we believe that this report is a false positive.	~~DCAEGEN2-423~~ - Inventory has dependency on vulnerable com.fasterxml. jackson.core CLOSED
dcaegen2 /collectors/ves	com. fasterxml .jackson. core	**Vulnerable artifact:** Dependency com.fasterxml.jackson.core:jackson-databind:jar:2.8.11 *located at* Module org.onap.dcaegen2.collectors.ves:VESCollector:jar **Vulnerability report:** CVE-2017-7525 originally reports that the application is vulnerable by using this component, when default typing is enabled. More details about the vulnerability is provided by https://github.com/FasterXML/jackson-docs/wiki/JacksonPolymorphicDeserialization. **False Positive Classification Reasoning:** The org.onap.dcaegen2.collectors.ves:VESCollector code does not enable use of global type information, using Class name as the type id. More over, VESCollector invokes json-schema-validator, which is where jackson-databind is used, post event serialization primarily for schema validation. Thus, we believe that the reported vulnerability is a false positive.	~~DCAEGEN2-446~~ - VEScollector security issues identified in CLM CLOSED
dcaegen2 /services /mapper	com. fasterxml .jackson. core	**Vulnerable artifact:** **Vulnerability report:** incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the c3p0 libraries are available in the classpath. **False Positive Classification Reasoning:** In mapper, Jackson is only used for converting between POJO to JSON, not the other direction which is reported as vunerable by CVE-2018-7489. The member call used is ObjectMapper.writeValueAsString. not the risky readValue method. Thus we believe the reporting is a false positive.	~~DCAEGEN2-467~~ - Security issue to be addressed for fasterxml.jackson CLOSED
dcaegen2 /services /mapper	org. springframework	**Vulnerable artifact:** Dependency org.springframework:spring-expression:jar:5.0.4.RELEASE *located at* Module org.onap.dcaegen2.services.mapper.vesadapter:snmpmapper:jar:0.0.1 **Vulnerability report:** older unsupported versions, allow applications to expose STOMP over WebSocket endpoints with a simple, in-memory STOMP broker through the spring-messaging module. A malicious user (or attacker) can craft a message to the broker that can lead to a remote code execution attack. **False Positive Classification Reasoning:** In mapper, there is no use of STOMP over websocket. There fore we believe that this is a false positive.	~~DCAEGEN2-467~~ - Security issue to be addressed for fasterxml.jackson CLOSED
dcaegen2 /services /mapper	com. fasterxml .jackson. core	**Vulnerable artifact:** Dependency com.fasterxml.jackson.core:jackson-databind:jar:2.9.5 *located at* Module org. onap.dcaegen2.services.mapper.vesadapter:UniversalVesAdapter:jar:0.0.1 **Vulnerability report:** `jackson-databind` is vulnerable to Remote Code Execution (RCE). A remote attacker can exploit this by uploading a malicious serialized object that will result in RCE if the application attempts to deserialize it. **False Positive Classification Reasoning:** In mapper, Jackson is only used for converting between POJO to JSON, not the other direction which is reported as vunerable by CVE-2018-7489. The member call used is ObjectMapper.writeValueAsString. not the risky readValue method. Thus we believe the reporting is a false positive.	~~DCAEGEN2-467~~ - Security issue to be addressed for fasterxml.jackson CLOSED

dcaegen2 /services /mapper	org. springframework	**Vulnerable artifact:** Dependency org.springframework:spring-webmvc:jar:5.0.4.RELEASE *located at* Module org. onap.dcaegen2.services.mapper.vesadapter:snmpmapper:jar:0.0.1 **Vulnerability report:** older unsupported versions, allow applications to configure Spring MVC to serve static resources (e.g. CSS, JS, images). When static resources are served from a file system on Windows (as opposed to the classpath, or the ServletContext), a malicious user can send a request using a specially crafted URL that can lead a directory traversal attack. **False Positive Classification Reasoning:** The identified vulnerability exists when serving static artifact from Windows host. Our use is neither from a Windows host, or serving static file. Therefore we believe this is afalse positive.	~~DCAEGEN2-467~~ - Security issue to be addressed for fasterxml.jackson CLOSED
~~dcaegen2 /services/prh~~	~~com. fasterxml .jackson. core~~	~~incomplete fix for the CVE-2017-7525 deserialization flaw~~ ~~FasterXML 2.9.5 released March 2018, supposed to correct this behavior (in tests currently).~~ ~~After FasterXML upgrade to 2.9.5, we still have negative CLM scan results, we will be constantly looking at newer FasterXML version, providing permanent correction of bugs found in 2.9.x.~~	~~DCAEGEN2-426~~ - Security issues to be addressed for PRH CLOSED All vulnerabilities addressed, according to CLM scan on 04/21. https://nexus-iq.wl.linuxfoundation.org/assets/index.html#/reports/dcaegen2-services-prh/a66b0ace9ec046c18cda082800e0fddc

Sample of CLM Report