Logging Beijing - M4 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.

Report in the template below only the vulnerabilities that Nexus-IQ is reporting as **"Critical"** (Level 7 to 10).

This table will be presented to the TSC at Code Freeze milestone (M4).

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.

~~LOG-186~~ - S3P: add cert to Kibana port - coordinate with AAF CLOSED

~~LOG-354~~ - secure kibana - both Logging and CD CLOSED

https://bestpractices.coreinfrastructure.org/projects/1578

blocked URL

Not really applicable - adding an OOM zeroday exploit that is solved by running onap in a private subnet

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
oom	org. kubernetes	see ~~LOG-353~~ - Anti-Crypto: Security RBAC Lockdown of OOM Kubernetes until 1.10 upgrade - port 10249-10255 - specifically 10250 and 8880 oauth CLOSED workaround is private ACL for 10249-10250	~~LOG-353~~ - Anti-Crypto: Security RBAC Lockdown of OOM Kubernetes until 1.10 upgrade - port 10249-10255 - specifically 10250 and 8880 oauth CLOSED In the JIRA ticket, you will explain findings and action plan Add the Label "Security"
		False Positive Add the explanation why you believe it is a false positive	Not applicable

Sample of CLM Report