# VVP R2 Beijing Security/Vulnerability Threat

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:

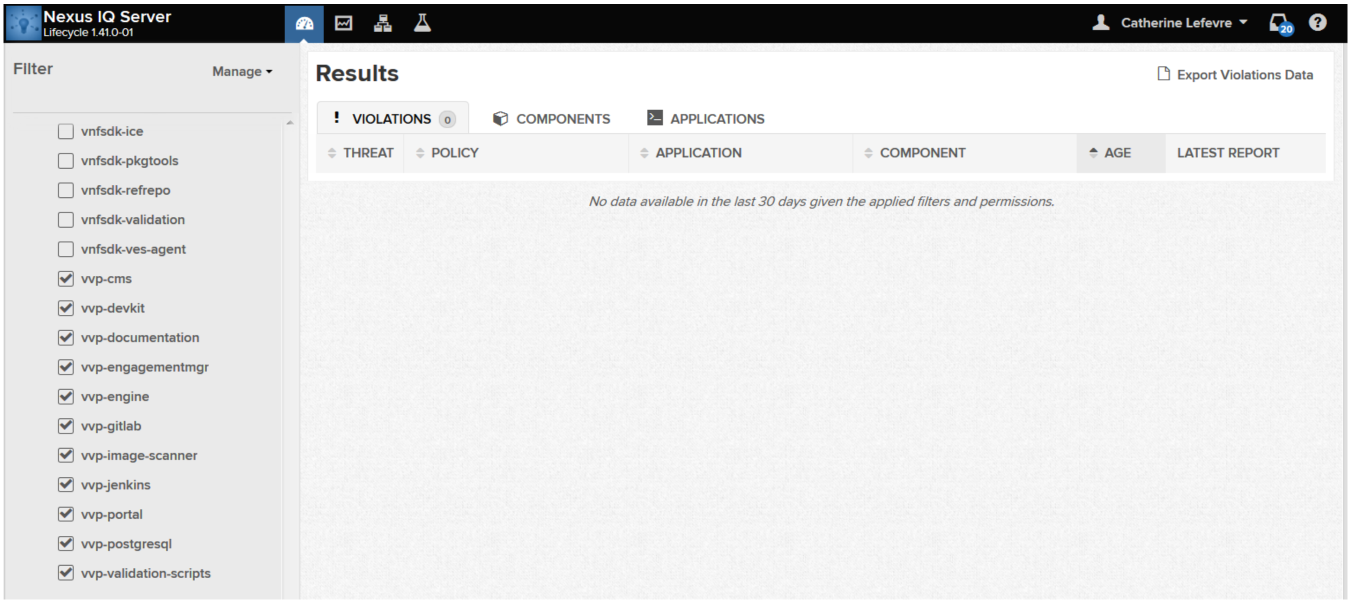
- Confirmation of a vulnerability including an action
- False Positive

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 |
|---|---|---|---|
| | | | |
| | | | |

*__CLM Report :__*

*CLM is setup - VVP repositories mostly contain yaml/Python files. No issue reported till now (4/18/2018).*



- □ vnfsdk-ice
- □ vnfsdk-pkgtools
- □ vnfsdk-refrepo
- □ vnfsdk-validation
- □ vnfsdk-ves-agent
- ☑ vvp-cms
- ☑ vvp-devkit
- ☑ vvp-documentation
- ☑ vvp-engagementmgr
- ☑ vvp-engine
- ☑ vvp-gitlab
- ☑ vvp-image-scanner
- ☑ vvp-jenkins
- ☑ vvp-portal
- ☑ vvp-postgresql
- ☑ vvp-validation-scripts

*No data available in the last 30 days given the applied filters and permissions.*