VF-C 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.

The following table is addressing 2 different scenarios:

- Confirmation of a vulnerability including an action
- False Positive

Repository	Group	Impact Analysis	Action
vfc-nfvo-driver-svnfm-nokia	com.fasterxml.jackson.core	False positive Explaination: This vulnerability issue only exists if com.fasterxml.jackson.databind.ObjectMapper.setDefaultTyping() is called before it is used for deserialization. nokia driver doesn't invoke this method	
~~vfc-nfvo-driver-svnfm-nokia~~	~~commons-httpclient~~	~~Version 3.1 is already newest.~~ ~~There is no non-vulnerable version of this component.~~	~~We are trying to replace this jar with other jars~~
vfc/nfvo/resmanagement	commons-collections	net.sf.json-lib:json-lib:2.4 depend on this This vulnerability issue is an indirect dependency introduced by vfc/nfvo/resmanagement	
vfc/nfvo/resmanagement	commons-beanutils	net.sf.json-lib:json-lib:2.4 depend on this This vulnerability issue is an indirect dependency introduced by vfc/nfvo/resmanagement	
vfc/nfvo/resmanagement	org.codehaus.jackson	Version 1.9.13 is already newest. There is no non vulnerable version of this component. We don't use Jackson directly and don't use createBeanDeserializer() function which has the vulnerability. We were unable to find any reference to this Vulnerability	
vfc/nfvo/driver/vnfm/svnfm/huawei	commons-collections	net.sf.json-lib:json-lib:2.4 depend on this This vulnerability issue is an indirect dependency introduced by vfc/nfvo/driver/vnfm/svnfm/huawei	
vfc/nfvo/driver/vnfm/svnfm/huawei	commons-beanutils	net.sf.json-lib:json-lib:2.4 depend on this This vulnerability issue is an indirect dependency introduced by vfc/nfvo/driver/vnfm/svnfm/huawei	
vfc/nfvo/driver/vnfm/svnfm/huawei	commons-httpclient	Version 3.1 is already newest. There is no non vulnerable version of this component. VF-C code don't use the readRawLine() method in commons-httpclient directly. We plan to replace this jar with Apache HttpComponents, but need some time to update the code and test.	We are trying to replace this jar with other jars
vfc/nfvo/driver/vnfm/svnfm/huawei	org.codehaus.jackson	Version 1.9.13 is already newest. There is no non vulnerable version of this component. We don't use Jackson directly and don't use createBeanDeserializer() function which has the vulnerability. We were unable to find any reference to this Vulnerability	
vfc/nfvo/driver/vnfm/gvnfm/juju	commons-collections	net.sf.json-lib:json-lib:2.4 depend on this This vulnerability issue is an indirect dependency introduced by vfc/nfvo/driver/vnfm/gvnfm/juju	
vfc/nfvo/driver/vnfm/gvnfm/juju	commons-beanutils	net.sf.json-lib:json-lib:2.4 depend on this This vulnerability issue is an indirect dependency introduced by vfc/nfvo/driver/vnfm/gvnfm/juju	

vfc/nfvo/driver /vnfm/gvnfm/juju	org.codehaus. jackson	Version 1.9.13 is already newest. There is no non vulnerable version of this component. We don’t use Jackson directly and don’t use createBeanDeserializer() function which has the vulnerability. We were unable to find any reference to this Vulnerability	
vfc-nfvo-driver-ems	com. fasterxml. jackson.core	False positive Explaination: This vulnerability issue only exists if com.fasterxml.jackson.databind.ObjectMapper. setDefaultTyping() is called before it is used for deserialization. ems driver doesn't invoke this method	
~~vfc-nfvo-driver-ems~~	~~xerces~~	~~Version 1.9.13 is already newest.~~ ~~There is no non vulnerable version of this component.~~	