Casablanca Maintenance ExtAPI Security/Vulnerability Report

This table represents the known exploitable and non-exploitable vulnerabilities in third party packages used in the project.

Repository	Group	Impact Analysis	Action
externalapi/nbi	com.fasterxml.jackson.core	False Positive. The exploit primarily is about enabling polymorphic type handling with the object mapper and writing class specifics into the JSON object. There are two ways of doing this: 1. ObjectMapper.enableDefaultTyping() 2. @JsonTypeInfo for marshalling / unmarshalling an object By default the ObjectMapper does not enableDefaultTyping, the code base is not using either approach, so the possibility of the exploit vector does not apply.	N/A
externalapi/nbi	com.fasterxml.jackson.core	False positive axis2-transport-jms is not used	Update to >= 2.9.8
externalapi/nbi	com.fasterxml.jackson.core	False positive Open JPA is not used	Update to >= 2.9.8
externalapi/nbi	com.fasterxml.jackson.core	False positive jboss-common-core is not used	Update to >= 2.9.8
externalapi/nbi	commons-beanutils	No impact: Beanutils is ONLY manipulated for outgoing serialization purpose, to filter json node to populate http response with json. Beanutils is not used on input data or exposed as is to external client	N/A Note: 1.9.3 is the latest released but still not fix the listed vulnerability. We tried to use some other frameworks but only beanutils has some key features we can not miss, to filter json response data. Avoiding commonsbenanutils means an important re write of the code with other opened risk for sure.
externalapi/nbi	dom4j	No impact: Dom4j is manipulated internaly by hibernate 5.0.2 wich is used by spring-boot-starter-data-jpa	N/A Note: The threat level moved from 6 to 7 between 09/19 and 11/05 Try to force dom4j 2.x, or plan an upgrade of externalapi to a more recent version of springboot
externalapi/nbi	org.apache.tomcat.embed	No impact: Tomcat-embed-websocket is coming with spring-boot-starter-web 1.5.12 but websocket are not active on externalapi	N/A Note: The threat level moved from 6 to 7 between 09/19 and 11/05 Try to exclude tomcat-embed-websocket from import. Try to force tomcat 9.0.12 or plan an upgrade of externalapi to a more recent version of springboot compatible with tomcat 9.0.12
externalapi/nbi	com.google.guava	No impact Guava is coming with org.onap.msb.java-sdk:msb-java-sdk, used internaly for externalapi registration on msb.	N/A Note: Update to msb-java-sdk from 1.1.0 to 1.2.0 should remove the alert as 1.2.0 does not have any alert on this.

externalapi/nbi	org.apache.tomcat.embed	No impact tomcat-embed-core is coming with spring-boot-starter-web 1.5.12, but externalapi doesn't use any directory redirection.	N/A Note: Try to force tomcat 9.0.12 or plan an upgrade of externalapi to a more recent version of springboot compatible with tomcat 9.0.12
externalapi/nbi	org.springframework	No impact: Stomp is not active on externalapi	N/A See https://pivotal.io/security/cve-2018-1257
externalapi/nbi	org.springframework	No impact; application doesn't serve static resources or use `org.springframework.core.io.Resource`	N/A See https://pivotal.io/security/cve-2018-15756
externalapi/nbi	org.springframework	No impact: HiddenHttpMethodFilter is not used	N/A See https://pivotal.io/security/cve-2018-11040
externalapi/nbi	org.springframework	No impact: MappingJackson2JsonView is not used	N/A See https://pivotal.io/security/cve-2018-11040
externalapi/nbi	org.springframework	No impact: MappingJackson2JsonView is not used	N/A See https://pivotal.io/security/cve-2018-11040