

Casablanca HOLMES 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
holmes-common	com.fasterxml.jackson.core	<p>False Positive</p> <p>Explanation: This vulnerability issue only exists if com.fasterxml.jackson.databind.ObjectMapper.setDefaultTyping() is called before it is used for deserialization.</p> <p>holmes-common does not use ObjectMapper for serialization/deserialization of JSON objects. Instead, Holmes uses GSON to avoid the vulnerability issues. The reason this is detected is that jackson-databind is introduced indirectly by msb-java-sdk. Also, the MSB team has declared this to be a false positive.</p>	
holmes-dsa	com.fasterxml.jackson.core	<p>False Positive</p> <p>Explanation: This vulnerability issue only exists if com.fasterxml.jackson.databind.ObjectMapper.setDefaultTyping() is called before it is used for deserialization.</p> <p>holmes-dsa does not use ObjectMapper for serialization/deserialization of JSON objects. Instead, Holmes uses GSON to avoid the vulnerability issues. The reason this is detected is that jackson-databind is introduced indirectly by msb-java-sdk. Also, the MSB team has declared this to be a false positive.</p>	
holmes-engine-management	com.fasterxml.jackson.core	<p>Explanation: This vulnerability issue only exists if com.fasterxml.jackson.databind.ObjectMapper.setDefaultTyping() is called before it is used for deserialization.</p> <p>holmes-engine-management does not use ObjectMapper for serialization/deserialization of JSON objects. Instead, Holmes uses GSON to avoid the vulnerability issues. The reason this is detected is that jackson-databind is introduced indirectly by dropwizard-core.</p> <p>To solve the problem, we have to replace the framework of Holmes or wait for updates from Dropwizard.</p> <p>From Holmes perspective, we don't use Jackson for JSON data processing. So this is not a big deal for Holmes.</p>	<p>Need to update Dropwizard to check whether its new version has solved this problem. Otherwise, we have to switch to another framework.</p>
holmes-rule-management	com.fasterxml.jackson.core	<p>Explanation: This vulnerability issue only exists if com.fasterxml.jackson.databind.ObjectMapper.setDefaultTyping() is called before it is used for deserialization.</p> <p>holmes-rule-management does not use ObjectMapper for serialization/deserialization of JSON objects. Instead, Holmes uses GSON to avoid the vulnerability issues. The reason this is detected is that jackson-databind is introduced indirectly by dropwizard-core.</p> <p>To solve the problem, we have to replace the framework of Holmes or wait for updates from Dropwizard.</p> <p>From Holmes perspective, we don't use Jackson for JSON data processing. So this is not a big deal for Holmes.</p>	<p>Need to update Dropwizard to check whether its new version has solved this problem. Otherwise, we have to switch to another framework.</p>