Dublin DMAAP 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
dmaap-messagerouter-msgrtr	com.fasterxml.jackson.core	There is no non vulnerable version of this component(jackson-databind-2.8.11.1).This vulnerability issue only exists if com.fasterxml.jackson.databind.ObjectMapper.setDefaultTyping() is called before it is used for deserialization. DMaaP MR does not use the default typing. False Positive	No action required. Requesting an exception for all the issues reported due to this component https://jira.onap.org/browse/DMAAP-784
dmaap-messagerouter-msgrtr	javax.mail	Message-Id in the email contains the user name and host name of the java process that triggered the email This component is coming from the Cambria library and all of its versions are vulnerable. As of today non of the Message Router clients use the email generating functionality of the Message Router. False Positive	No action required. Requesting an exception blocked URLDMAAP-785 - Resolve security issues in MessageRouter due to the component javax.mail : mail : 1.4 CLOSED
dmaap-messagerouter-messageservice	com.fasterxml.jackson.core	There is no non vulnerable version of this component(jackson-databind-2.8.11.1).This vulnerability issue only exists if com.fasterxml.jackson.databind.ObjectMapper.setDefaultTyping() is called before it is used for deserialization. DMaaP MR does not use the default typing. False Positive	No action required. Requesting an exception for all the issues reported due to this component https://jira.onap.org/browse/DMAAP-784
dmaap-messagerouter-messageservice	javax.mail	Message-Id in the email contains the user name and host name of the java process that triggered the email This component is coming from the Cambria library and all of its versions are vulnerable. As of today non of the Message Router clients use the email generating functionality of the Message Router. False Positive	No action required. Requesting an exception blocked URLDMAAP-785 - Resolve security issues in MessageRouter due to the component javax.mail : mail : 1.4 CLOSED
dmaap-messagerouter-messageservice	org.springframework.security.oauth	This component is coming from the ajsc libraries. DMaaP does not have the oAuth functionality, so it will not impact	No action required. Requesting an exception
dmaap-messagerouter-messageservice	org.apache.camel	This component is coming from the ajsc libraries. DMaaP does not use the file attachment in email. So this vulnerability don't impact DMaaP.	No action required. Requesting an exception
dmaap-messagerouter-messageservice	org.springframework	This component is coming from the ajsc libraries. DMaaP is a REST project and does not serve any static resources. So this vulnerability does not impact DMaaP.	No action required. Requesting an exception
dmaap-messagerouter-messageservice dmaap-messagerouter-docker	org.springframework	This component is coming from the ajsc libraries. DMaaP is not using the switchUserProcessingFilter functionality identified in these vulnerabilities and thus it does not impact.	No action required. Requesting an exception
dmaap-messagerouter-messageservice dmaap-messagerouter-docker	org.springframework	This component is coming from the ajsc libraries. DMaaP is not using the SecureRandomFactoryBean functionality identified in these vulnerabilities and thus it does not impact.	No action required. Requesting an exception
dmaap-messagerouter-messageservice	commons-fileupload	This component is coming from the ajsc libraries. DMaaP does not have file upload functionality. So DMaaP is not vulnerable	No action required. Requesting an exception
dmaap-messagerouter-messageservice	commons-codec	The Base64 functionality identified in this vulnerability cannot be exploited as the DMaaP components in rare case are using Base64.decode only to decode the Authorization header, which if modified by a malicious user is only going to result in Authorization errors. This vulnerability will not directly impact DMaaP.	No action required. Requesting an exception

dmaap-messagerouter-dmaapclient	com.fasterxml.jackson.core	There is no non vulnerable version of this component(jackson-databind-2.8.11.1).This vulnerability issue only exists if com.fasterxml.jackson.databind.ObjectMapper.setDefaultTyping() is called before it is used for deserialization. DMaaP MR does not use the default typing. False Positive	No action required. Requesting an exception for all the issues reported due to this component https://jira.onap.org/browse/DMAAP-784
dmaap-datarouter-prov	com.h2database : h2	There is no non vulnerable version of this component(com.h2database : h2 : 1.4.197).This is only used to mock the database in unit tests False Positive	No action required. Requesting an exception for all the issues reported due to this component
dmaap-messagerouter-dmaapclient	com.att.nsa : dmaapClient	Component com.att.nsa:dmaapClient was not used in the project dmaap-messagerouter-dmaapclient. these issues are due to issues in CLM Scan False Positive	Created a LF ticket #54030,54268 . LF Help desk updated that they don't know why the scan reported these vulnerabilities
onap-dmaap-messagerouter-msgrtr onap-dmaap-messagerouter-messageservice	org.apache.zookeeper	This will not impact MR project, as we are not using the jar in the way that will cause this issue. We will try to upgrade the jar version to see if the issue is not reported anymore.	No action required. Requesting an exception
onap-dmaap-messagerouter-messageservice	com.att.ajsc	This component is coming from the ajsc libraries. DMaaP does not have the oAuth functionality, so this will not impact	No action required. Requesting an exception
onap-dmaap-messagerouter-messageservice	com.att.ajsc	This vulnerability issue only exists if com.fasterxml.jackson.databind.ObjectMapper.setDefaultTyping() is called before it is used for deserialization. DMaaP MR does not use the default typing. False Positive	No action required. Requesting an exception
dmaap-buscontroller	org.postgresql	The vulnerability is documented as disputed, i.e. this is in fact a documented feature. It becomes vulnerability if the postgresql process allows remote superuser login remotely or for user having pg_execute_server_program role. There are no explicit users defined with that roles or super user capability currently. However, in light of the upcoming shared postgresql instance it would be better for the oom/common/postgresql chart owner to perform a security review for this vulnerability for El Alto. Following Jira opened for OOM team - ~~OOM-1824~~ - Security scan of oom/common/postresql charts for vulnerability CVE-2019-9193 CLOSED	No action required. Requesting an exception