


















# Dublin Policy 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	A c t i o n
policy/common  These repos inherit from policy /common:  policy/models  policy/api  policy/pap  policy/drools-pdp  policy/xacml-pdp  policy/apex-pdp  policy/drools-applications  policy /distribution	com. fasterxml. jackson. core	<p>Request Exception - false positive</p> <p>Inherit from Dmaap 1.1.9 Project artifacts - we are not using Jackson in this repo anymore.</p> <div><input checked="" type="checkbox"/> <del>POLICY-1668</del> - Investigate exclusion or upgrade dmaap client when they remove jackson vulnerabilities <span>CLOSED</span></div> <p>19 Apr 2019 The dmaap team indicated they are not vulnerable to the jackson security issue.</p>	
policy/common  These repos inherit from policy /common:  policy/models  policy/api  policy/pap  policy/drools-pdp  policy/xacml-pdp  policy/apex-pdp  policy/drools-applications  policy /distribution	commons-codec	<p>Request Exception</p> <p>This dependency is used by org.apache.httpcomponents HttpClient - which is a popular library heavily used in open source. The codec does the Base64 decoding for authentication. There is no alternate commons-codec, nor a fix in HttpClient that excludes it.</p> <p>Replacing this code would be a significant effort - possible the apache codec team is recently looking to fix this.</p> <div><input checked="" type="checkbox"/> <del>POLICY-1658</del> - Upgrade httpclient when available or find alternative to HttpClient apache component <span>CLOSED</span></div>	

policy/drools-pdp	dom4j	<p>Request Exception - False Positive</p> <p>This is both a security and a license issue due to Drools v6.5.0.Final including and using this dependency.</p> <p>Upgrading to 7.x version would <b>not</b> clear this issue and would result in multiple other license exceptions that are not clearable.</p> <p>Our Drools PDP does not utilize XML documents.</p> <p>We are trying to determine an appropriate time to upgrade Drools:</p> <p> <a href="#">POLICY-1487</a> - Upgrade PDP-D to drools 7.28.0.Final <span>CLOSED</span></p>
policy/drools-pdp	org.apache.ant	<p>Request Exception</p> <p>This is a security issue due to Drools v6.5.0.Final including this dependency.</p> <p>Upgrading to 7.x version <b>would</b> clear this issue, but would then consequently result in multiple other new license exceptions that are not clearable.</p> <p>It does not look like the Drools v6.5.0 calls any of the methods identified in the sonatype or the CVE.</p> <p>We are trying to determine an appropriate time to upgrade Drools:</p> <p> <a href="#">POLICY-1487</a> - Upgrade PDP-D to drools 7.28.0.Final <span>CLOSED</span></p>
policy/drools-pdp	org.jsoup	<p>Request Exception - false positive</p> <p>This is a security issue due to Drools v6.5.0.Final including this dependency.</p> <p>Upgrading to 7.x version would <b>not</b> clear this issue and would result in multiple other new license exceptions that are not clearable.</p> <p>It does not look like the Drools v6.5.0 uses the class identified in the CVE.</p> <p>We are trying to determine an appropriate time to upgrade Drools:</p> <p> <a href="#">POLICY-1487</a> - Upgrade PDP-D to drools 7.28.0.Final <span>CLOSED</span></p>
policy/xacml-pdp policy/drools-applications	com.fasterxml.jackson.core	<p>Request Exception - false positive</p> <p>Inherited from a dependency which does not use jackson in the manner subject to vulnerability.</p> <p>NOTE: This dependency is in github and is managed by <a href="#">Pamela Dragosh</a> - removal of jackson from that dependency is in progress. We will upgrade it in EI Alto.</p> <p> <a href="#">POLICY-1666</a> - Upgrade XACML github PDP when jackson is removed <span>CLOSED</span></p>
policy/apex-pdp	org.codehaus.jackson	<p>Request Exception - false positive</p> <p>This dependency is pulled in by org.apache.avro. We are using the latest version of Avro.</p> <p>We are using Avro to deserialize events. Avro uses jackson-mapper-asl for its Json decoding. The schema for the events we are decoding is controlled in policy models and prevents executable code being specified. Therefore this vulnerability cannot be exploited.</p> <p> <a href="#">POLICY-1508</a> - Investigate Apex org.codehaus.jackson.jackson-mapper-asl security false positive <span>CLOSED</span></p>

policy/apex-pdp	org.python	<p>This dependency brings in the Jython (Python) interpreter for executing scripts written in Python under the control of Apex.</p> <p>There are two vulnerabilities, both concerning adding extra modules to the Python libraries on a host running Python scripts under Jython.</p> <ul style="list-style-type: none"> <li>The setup.py and build_py.py files allow extra python packages to be installed on the host during the startup of Jython. This mechanism uses the setuptools mechanism to install those packages. That mechanism does not enforce path traversal restrictions, allowing malicious packages to access protected areas on the host.</li> <li>Jython uses packages installed with the python pip utility. Pip is vulnerable to Path Traversal attacks, malicious packages installed with pip can access protected areas on the host</li> </ul> <p>The solution is to warn developers not to install malicious extra Python packages.</p> <p><input checked="" type="checkbox"/> <a href="#">POLICY-1599</a> - Investigate Apex org.python.jython-standalone.2.7.1 <span>CLOSED</span></p>	
policy/engine	bouncycastle	<p>Flagged due to inclusion of ONAP Portal SDK</p> <p><input checked="" type="checkbox"/> <a href="#">POLICY-1604</a> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span></p>	
policy/engine	com.fasterxml.jackson.core	<p>Request Exception - false positive</p> <p>The repo does not use the dependency in the manner exposing the vulnerability. We will finish removal of Jackson from this repo when possible, it is a large effort.</p> <p><input checked="" type="checkbox"/> <a href="#">POLICY-1644</a> - Finish removal of Jackson from Policy Framework repositories <span>CLOSED</span></p>	
policy/engine	com.mchange	<p>Flagged due to inclusion of ONAP Portal SDK</p> <p><input checked="" type="checkbox"/> <a href="#">POLICY-1604</a> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span></p>	
policy/engine	org.springframework	<p>Flagged due to inclusion of ONAP Portal SDK</p> <p><input checked="" type="checkbox"/> <a href="#">POLICY-1604</a> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span></p>	
policy/engine	angular  angularjs angular.min.js	<p>Flagged due to inclusion of ONAP Portal SDK</p> <p><input checked="" type="checkbox"/> <a href="#">POLICY-1604</a> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span></p>	
policy/engine	angular-sanitize	<p>Flagged due to inclusion of ONAP Portal SDK</p> <p><input checked="" type="checkbox"/> <a href="#">POLICY-1604</a> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span></p>	
policy/engine	angular-ui-grid	<p>Flagged due to inclusion of ONAP Portal SDK</p> <p><input checked="" type="checkbox"/> <a href="#">POLICY-1604</a> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span></p>	
policy/engine	commons-beanutils	<p>Flagged due to inclusion of ONAP Portal SDK</p> <p><input checked="" type="checkbox"/> <a href="#">POLICY-1604</a> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span></p>	
policy/engine	dom4j	<p>Request Exception</p> <p>dom4j is a dependency of org.hibernate:hibernate-core:jar:4.3.10</p> <p><input checked="" type="checkbox"/> <a href="#">POLICY-1664</a> - Investigate upgrade of hibernate to 5.x <span>CLOSED</span></p> <p>Upgrading hibernate or moving to eclipselink is a large effort in this repo.</p>	

policy/engine	org. springfram ework	<p>May need an exception - will investigate upgrade</p> <div>  <b>POLICY-1539</b> - Investigate upgrade of org.springframework 4.3.24-RELEASE <span>CLOSED</span> </div>
policy/engine	org. apache. tomcat	<p>Request Exception - false positive</p> <div>  <b>POLICY-1675</b> - Upgrade tomcat 9.0.16 when security vulnerabilities fixed <span>CLOSED</span> </div> <p>We upgraded to remove a vulnerability from 8.5.34, now we have a new one due to 9.0.16</p> <div>  <b>POLICY-1662</b> - Upgrade tomcat to 9.0.16 to remove security DoS issue <span>CLOSED</span> </div> <p>The application is vulnerable by using this component when running on Windows with the CGI Servlet initialization parameter enableCmdLineArguments option of the component set to true.</p> <p>Since we do not run this in windows, ONAP Policy Engine is not vulnerable.</p>
policy/engine	moment	<p>Flagged due to inclusion of ONAP Portal SDK</p> <div>  <b>POLICY-1694</b> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span> </div>
policy/engine	org. apache. wicket	<p>Flagged due to inclusion of ONAP Portal SDK</p> <div>  <b>POLICY-1694</b> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span> </div>
policy/engine	org. owasp. antisamy	<p>Flagged due to inclusion of ONAP Portal SDK</p> <div>  <b>POLICY-1694</b> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span> </div>
policy/engine	org. webjars  bootstrap	<p>Flagged due to inclusion of ONAP Portal SDK</p> <div>  <b>POLICY-1694</b> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span> </div>
policy/engine	org. webjars  jquery	<p>Flagged due to inclusion of ONAP Portal SDK</p> <div>  <b>POLICY-1694</b> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span> </div>
	jQuery	
policy/engine	org. owasp. esapi	<p>Flagged due to inclusion of ONAP Portal SDK</p> <div>  <b>POLICY-1694</b> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span> </div>
policy/engine	commons- fileupload	<p>Flagged due to inclusion of ONAP Portal SDK</p> <div>  <b>POLICY-1694</b> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span> </div>
policy/engine	org.exist- db. thirdparty. xerces	<p>Flagged due to inclusion of ONAP Portal SDK</p> <div>  <b>POLICY-1694</b> - Upgrade Portal SDK when they fix vulnerabilities <span>CLOSED</span> </div>
policy /distribution	com. fasterxml. jackson. core	<p>Request Exception - false positive</p> <p>Inherited from policy/engine, does not use this dependency directly. Could exclude it when time permits.</p> <div>  <b>POLICY-1597</b> - Investigate exclusion of jackson-databind in policy/distribution <span>CLOSED</span> </div>

