Security/Vulnerability Threat - AAF

Security Vulnerabilities are reported for aaf/authz were from old repo. We are working on latest code that committed to the aaf repo.

Repository	Group	Impact Analysis	Action
aaf-authz	io.netty:netty-handler	Instrumental: This has been **RESOLVED** by updating the Version netty handler is not longer on the report, 4/25: https://nexus-iq.wl.linuxfoundation.org/assets/index.html#/reports/aaf-authz/8a3ac7244a394bd892545012abd27864	N
aaf-authz	org.apache.httpcomponents also "commons-beans-utils1.8.3", "org.apache.shiro:shiro-core:1.3.2"	httpcomponents resolved, but "common-beans-utils" and "shire-core" remain. HOWEVER: These are ONLY used by Shiro Adapter. This Shiro Adapter is NOT used in any running AAF components or any part of CADI. 04/27/2018 The Adapter is ONLY used by OTHER apps which are using Shiro (and thus the vulnerability is on those apps, not AAF) **THEREFORE, this is a false positive for AAF as a Service or Clients.**	N
aaf-authz	org.bouncycastle	org.bouncycastle updated to latest version, There are **NO LONGER any Security issues r**elated to Bouncy Castle. The License is MIT, which is listed as a Policy violation, however. Impact: Replacement of Bouncy Castle is not trivial. Cannot simply replace in short timeframe. Is the License from MIT an unacceptable risk going forward?	N