SDC Security/Vulnerability Threat Template

SDC should be deployed in an internal network in the service provider eco system to provide an additional layer of security.

SDC is build as a multi tier application where the frontend server is accessible but all the DB and backend servers are positioned in a DMZ, we define all our communication to be proxyed by the fronted server and to be passed from there to the backend server.

no direct communication from the UI to the backend or from UI or frontend server to the db is defined by SDC.

the following recommendations and architecture description mitigates the risk of the identified known vulnerabilities in yellow below.

Repository	Group	Impact Analysis	Action	Notes
sdc-sdc-tosca	com. fasterxml. jackson. core	False positive the lib is part of the sdcTosca parser which is used as a library. the parser only runs on predefined objects and will not attempt to run on an object that was not validated. the parser is protected by the application using it and the information supplied is coming from the using application. There is no non vulnerable version of this component.	No Action in Beijing.	
sdc catalog	org. apache. lucene	False positive the dependency is coming from Elastic search. as such the vulnerability no effecting affecting the application. There is no non vulnerable version of this component.	No Action for Beijing	
sdc catalog + onboarding	org. eclipse. jetty	False positive CVE-2016-4800 exposes a vulnerability when you are running on windows. sdc is dockerized and the container runs on alpine. false positive CVE-2017-9735 expose a vulnerability in using the password class in the lib. this class is not used by sdc. comes with jetty-server we connect update to a newer version because of breaking changes in jetty.	No action Beijing next release we will check the option to upgrade to newer version. Needs more effort and would impact the current state of ONAP.	
sdc - onboarding + catalog	io. springfox	there was a bigapichange that broke backward comparability. will be addressed next release to upgrade to 2.8.0	No action in Beijing. will be upgraded next release	
sdc catalog + onboarding	org. codehaus. jackson	False positive. used as part of the testingframe workinsdc. no actual use as part of the application No version with a fix is currently available.	No action in Beijing	

sdc- catalog	org. codehaus. groovy	Non impacting CVE-2015-3253 expose the application to DOS attack andexecution ofmalicious code by passing serialized objects. came from gremlin-groovy this is part of thetitanproject which is thesdcdriver for communication with our DB.	No action in Beijing. Titan Graph related fixes will be considered depending on the plan for usagepost Beijing. (move to JenoseGraph is being considered)	
sdc catalog + onboarding	com. fasterxml. jackson. core	Not impacting because a user needs to be authenticated CVE-2017-7525 and CVE-2018-7489 expose the application toexecution ofmalicious code byprovideunauthorized java object no version with a fixiscurrently available.	No action in Beijing. integration with AAF will reduce this issue further.	
sdc - catalog	commons - collections	this is a fork of part of thetitanproject. the project is at an end of life. and from common-validators. we are using an API of the titan client and are not in control of the implantation.	no action. move to JenoseGraph is being considered common validators no new versionisavilable	
sdc - onboarding	org. apache. logging. log4j	False positive sdcdoes not send logging events or receives them.	No action for Beijing Fix available - Update the version of the dependency in Casablanca. upgrade to 2.8.2 SDC-1325	open ticket to upgrade to 2.8.2
sdc - onboarding	com. fasterxml. jackson. dataformat	CVE-2016-7051 expose the application toattackedbased on fording the Document Type Definitions inaxmlfile onboarding upgrade to version 2.7.9	No action for Beijing Fix available - Update the version of the dependency to 2.7.9 and 2.8.11	ml open ticket to upgrade to 2.8.9
sdc catalog + onboarding	org. springframework	CVE-2015-5211 CVE-2016-9878 CVE-2018-1271 false positivesdcruns on a docker which is based onalpin upgrade to 4.3.15	Fix available - Update the version of the dependency SDC-1327	**Not found in latest scan** **version 4.3.15.RELEASE and version 4.3.17. RELEASE are labeled as threat level 5** **ml: open a task to catalog and onboarding to upgrade spring to 4.3.18**
sdc - onboarding + **catalog**	org. beanshell	CVE-2016-2510 the vulnerability exposes the application to remote code execution based on serializing objects with exactable code. all versions have vulnerabilities in them. waiting for a fix in future versions.	no action in Beijing. Waiting for a stable release.	used in test ngnotin theaplicationitself
sdc catalog + onboarding	org. hibernate	Non issue sdcdoes not use security manager and as such is not vulnerable	no action in Beijing.	theris aversionavilableneed to understand where it came from
sdc catalog + ~~onboarding~~	io.netty	false positive CVE-2016-4970 expose the application to DOS attacks, this is no exposed external and is only used as part of thedriver forcommunication with thedb. coming from Cassandra driver core	No action in Beijing.	upgradecassndradriver

sdc catalog + onboarding	commons-beanutils	CVE-2014-0114 expose the application to remote code exaction by manipulating the class loader all versions have vulnerabilities in them. waiting for a fix in future versions.	No action in Beijing. Update the version of the dependency as soon as security issue fixed.	
sdc - onboarding	org.apache.cxf	false positive CVE-2010-2076sdcdoes not use soap messages for communication upgrade to version 2.2.9	No action in Beijing Fix available - Update the version of the dependency	update version to lates
sdc - onboarding	com.fasterxml.jackson.core	false positive	No action in Beijing. Fix available - Update the version of the dependency to 2.8.6	ml update to 2.8.10
sdc - catalog	io.netty	False positive CVE-2015-2156 netty is usedin sidethedbdriver and a testingframe workthat both do not read cookies. CVE-2016-4970 used for testing and as a driver base as such they are not accepting requests and will notbe affectby dos came fromsdc-titan-cassndra this is a fork of part of thetitnaproject. the project is at an end of life.	No action in Beijing. move to JenoseGraph is being considered	exclude from pom in titan
sdc- catalog	org.bouncycastle	False positive came from selenium-server this is included and used in an automation project and does not actually deploy as part of SDC.	No action for Beijing.	**Problem with code CVE-2016-1000341 is now labeled as threat level 5**
sdc - catalog	commons-httpclient	False positive sdcdoes not use the client directly accept in the simulator which is internal use only. the package is at the end of life no none vulnerable version is available.	No action for Beijing.	the uses in catalogbeandtoolmay be removed by removing thedepandency `blueprints-sail-graph`
sdc- catalog	xerces	False positive came from selenium-java this is included and used in an automation project and does not actually deploy as part of SDC.	No action for Beijing.	
sdc - catalog	io.netty	False positive came from selenium-server this is included and used in an automation project and does not actually deploy as part of SDC.	No action for Beijing.	
sdc- catalog	org.apache.poi	Falseposotive Part of thesdctool used for migration and schema creation and is not part of the be logic	No action in Beijing	
sdc-titan-cassandra	org.codehaus.jackson	CVE-2017-7525 expose the client toexactionof malice code by a user. sdc-titan-casndra is the driver used by sdc to communicate with the graph representation stored in Cassandra. the driver used is internal to the application.	No action in Beijing. move to JenoseGraph is being considered.	
sdc-titan-cassandra	com.fasterxml.jackson.core	CVE-2017-7525 expose the client toexactionof malice code by a user. sdc-titan-casndra is the driver used by sdc to communicate with the graph representation stored in Cassandra. the driver used is internal to the application.	No action in Beijing. move to JenoseGraph is being considered	

sdc-titan-cassandra	org.codehaus.groovy	False posotive CVE-2015-3253 expose the application to DOS attack and exaction of malicios code by passing serialized objects. the client receives specific objects for serialization sdc-titan-casndra is the driver used by sdc to communicate with the graph representation stored in Cassandra. the driver used is internal to the application. to support geo-redundancy	No action in Beijing. move to JenoseGraph is being considered	
sdc-titan-cassandra	commons-collections	sdc-titan-casndra is the driver used by sdc to communicate with the graph representation stored in Cassandra. the driver used is internal to the application.	No action in Beijing. move to JenoseGraph is being considered	
sdc-titan-cassandra	ch.qos.logback	False positive, CVE-2017-5929 sdc-titan-casndra is the driver used by sdc to communicate with the graph representation stored in Cassandra. the driver used is internal to the application. t	No action in Beijing. move to JenoseGraph is being considered	
sdc-titan-cassandra	org.hibernate	CVE-2017-7536 we not use security manager and as such is not vulnerable sdc-titan-casndra is the driver used by sdc to communicate with the graph representation stored in Cassandra. the driver used is internal to the application.	No action in Beijing. move to JenoseGraph is being considered	
sdc-titan-cassandra	io.netty	False positive CVE-2015-2156 netty is usedin sidethedbdriver and a testingframe workthat both do not read cookies. CVE-2016-4970 used for testing and as a driver base as such they are not accepting requests and will notbe affectby dos sdc-titan-casndra is the driver used by sdc to communicate with the graph representation stored in Cassandra. the driver used is internal to the application.	No action in Beijing. move to JenoseGraph is being considered	
sdc-titan-cassandra	org.apache.httpcomponents	False positive the client used for communication to the db and the vulnerability is not applicable.	No action in Beijing. move to JenoseGraph is being considered	
sdc-workflow-designer	com.fasterxml.jackson.core	False positive CVE-2018-5968 and CVE-2017-17485 vulnerable to remote code exaction by passing objects. used only for converting specificjsonobjects tobpmn/xml no version with a fix is currently available.	No action in Beijing.	
sdc - catalog	com.unboundid			comes with shiled need to remove shiled
sdc- catalog + onboarding	org.eclipse.jetty			consider moving to a newer version of jetty
sdc-workflow-designer	org.codehaus.jackson			
sdc-workflow-designer	commons-beanutils			
sdc-workflow-designer	org.hibernate			
sdc-onboarding	org.apache.cxf			

sdccatalog	org.eclipse.jetty			
sdccatalog	org.eclipse.jetty			
sdc-titan-cassandra	com.fasterxml.jackson.core			