

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 proxied 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
sdsc-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.	
sdsc 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	
sdsc catalog + onboarding	org. eclipse. jetty	False positive CVE-2016-4800 exposes a vulnerability when you are running on windows. sdsc 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 sdsc. 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.	
sdsc - 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	
sdsc catalog + onboarding	org. codehaus. jackson	False positive. used as part of the testingframe workinsdsc. no actual use as part of the application No version with a fix is currently available.	No action in Beijing	

sdscatalog	org. codehaus. groovy	Non impacting CVE-2015-3253 expose the application to DOS attack and execution of malicious code by passing serialized objects. came from gremlin-groovy this is part of the titan project which is the sdc driver for communication with our DB.	No action in Beijing. Titan Graph related fixes will be considered depending on the plan for usage post Beijing. (move to JenoseGraph is being considered)	
sdscatalog + onboarding	com. fasterxml. jackson. core	Not impacting because a user needs to be authenticated CVE-2017-7525 and CVE-2018-7489 expose the application to execution of malicious code by providing unauthorized java object no version with a fix is currently available.	No action in Beijing. integration with AAF will reduce this issue further.	
sdscatalog	commons - collections	this is a fork of part of the titan project. 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 implementation.	no action. move to JenoseGraph is being considered common validators no new version is available	
sdsonboarding	org. apache. logging. log4j	False positive sdc does 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
sdsonboarding	com. fasterxml. jackson. dataformat	CVE-2016-7051 expose the application to attack based on forging the Document Type Definitions in xml file 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
sdscatalog + onboarding	org. springframeword	CVE-2015-5211 CVE-2016-9878 CVE-2018-1271 false positives sdc runs on a docker which is based on alpin 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
sdsonboarding + 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 ng not in the application itself
sdscatalog + onboarding	org. hibernate	Non issue sdc does not use security manager and as such is not vulnerable	no action in Beijing.	there is a version available needed to understand where it came from
sdscatalog + 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 the driver for communication with the db. coming from Cassandra driver core	No action in Beijing.	upgrade cassandra driver

sdscatalog + 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.	
sdsc - 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
sdsc - 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
sdsc - 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 fromsdsc-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
sdsc- 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
sdsc - 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 thedependency blueprints-sail-graph
sdsc- 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.	
sdsc - 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.	
sdsc- catalog	org.apache.poi	Falsepositive Part of thesdctoool used for migration and schema creation and is not part of the be logic	No action in Beijing	
sdsc-titan-cassandra	org.codehaus.jackson	CVE-2017-7525 expose the client toexactionof malice code by a user. sdsc-titan-casndra is the driver used by sdsc 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.	
sdsc-titan-cassandra	com.fasterxml.jackson.core	CVE-2017-7525 expose the client toexactionof malice code by a user. sdsc-titan-casndra is the driver used by sdsc 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	

sd-c-titan-cass andra	org. codehaus. groovy	False positive 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 sd-c-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	
sd-c-titan-cass andra	commons - collections	sd-c-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	
sd-c-titan-cass andra	ch.qos. logback	False positive, CVE-2017-5929 sd-c-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	
sd-c-titan-cass andra	org. hibernate	CVE-2017-7536 we not use security manager and as such is not vulnerable sd-c-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	
sd-c-titan-cass andra	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 sd-c-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	
sd-c-titan-cass andra	org. apache. httpcomp onents	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	
sd-c-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 tobpnm/xml no version with a fix is currently available.	No action in Beijing.	
sd-c - catalog	com. unboundid			comes with shiled need to remove shiled
sd-c- catalog + onboarding	org. eclipse. jetty			consider moving to a newer version of jetty
sd-c-workflow- designer	org. codehaus. jackson			
sd-c-workflow- designer	commons -beanutils			
sd-c-workflow- designer	org. hibernate			
sd-c- onboarding	org. apache. cxf			

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