










Casablanca Portal Platform Security/Vulnerability Report



This table represents the known exploitable and non-exploitable vulnerabilities in third party packages used in the project.

High-level mitigation plan:

Regarding known issues like “DOS, Remote Code Execution (RCE), CORS attack, HTTP request smuggling”, the Portal’s code is not exposing these vulnerabilities directly due to many layers of encapsulation by APIs, so these are most likely false positives reported by NexusIQ scan, however to be on safe side the mitigation plan is to deploy Portal platform in a secure environment e.g. in private network inside the company firewall.

Repository	Group	Impact Analysis	Action
portal	com. fasterxml. .jackson. core	<p>False positive.</p> <p>Analysis: This vulnerability is not exposed from the portal's code, because</p> <ol style="list-style-type: none">1. The portal does not pass any untrusted data for deserialization, as there is XSS/XSRF validation enabled in the portal's backend code.2. and the default typing (ObjectMapper.setDefaultTyping()) is not called as we use concrete java types.3. and we use Spring Security 4.2.3 as recommended in the nexus-iq report. <p>Spring version 4.2.3 will take care of this.</p> <p>Comments from Nexus-IQ: Spring Security has provided their own fix for this vulnerability (CVE-2017-4995). If this component is being used as part of Spring Security, then you are not vulnerable if you are running Spring Security 4.2.3. RELEASE or greater for 4.x or Spring Security 5.0.0.M2 or greater for 5.x.</p>	Not vulnerable in ONAP
portal	moments	<p>All available versions of moment.js are vulnerable. Upgrade is not an option.</p> <p>Analysis: Not vulnerable as all our date fields are reformatted and validated before being submitted. See below</p> <p>CVE 185 information: The moment package is vulnerable to Regular Expression Denial of Service (ReDoS). The monthsShortRegex(), monthsRegex(), weekdaysRegex(), weekdaysShortRegex(), and weekdaysMinRegex() functions in the moment.js, moment-with-locales.js, and regex.js files use a vulnerable regular expression while parsing the date input. A remote attacker can exploit this vulnerability by crafting a date input containing a very long sequence of repetitive characters which, when parsed, consumes available CPU resources and results in Denial Of Service.</p>	Not vulnerable in ONAP
portal, portal-sdk	angular	<p>Analysis: Cannot upgrade angular as this will require changes on all the Portal pages.</p> <p>From our analysis the vulnerability cannot be exploited because the portal application follows the below design recommendations provided by nexus-iq report.</p> <p>Recommendation by nexus-iq for this vulnerability (SONATYPE-2016-0064):</p> <p>It's best to design your application in such a way that users cannot change client-side templates.</p> <ul style="list-style-type: none">• Do not mix client and server templates• Do not use user input to generate templates dynamically• Do not run user input through \$scope.\$eval (or any of the other expression parsing functions listed above)• Consider using {@link ng.directive:ngCsp CSP} (but don't rely only on CSP)	Not vulnerable in ONAP
portal	common-s- beanutils	<p>All available versions of common-beanutils are vulnerable. Upgrade is not an option.</p> <p>Analysis: The portal code do not use classloader so it is not vulnerable in ONAP.</p> <p>CVE CWE: 20</p> <p>Description from CVE</p> <p>Apache Commons BeanUtils, as distributed in lib/commons-beanutils-1.8.0.jar in Apache Struts 1.x through 1.3.10 and in other products requiring commons-beanutils through 1.9.2, does not suppress the class property, which allows remote attackers to "manipulate" the ClassLoader and execute arbitrary code via the class parameter, as demonstrated by the passing of this parameter to the getClass method of the ActionForm object in Struts 1.</p>	Not vulnerable in ONAP
portal-sdk	org. apache. poi	<p>Analysis: Not vulnerable as we do not use POI to read documents. We use only to generate XLS from our own data.</p> <p>CVE CWE:399:</p> <p>Apache POI in versions prior to release 3.17 are vulnerable to Denial of Service Attacks: 1) Infinite Loops while parsing crafted WMF, EMF, MSG and macros (POI bugs 61338 and 61294), and 2) Out of Memory Exceptions while parsing crafted DOC, PPT and XLS (POI bugs 52372 and 61295).</p> <p> PORTAL-446 - POI CLOSED</p>	Not vulnerable in ONAP

portal, portal-sdk	org. springfra mework	<p>The impact of the springframework library is all over the project. So have to be very careful in upgrading the versions.</p> <p>At least trying to resolve the multiple version use in Dublin -</p> <div>  PORTAL-423 - Align springframework version among all poms CLOSED </div>	Request exception
portal-sdk	io.netty	<p>Not clear what is the issue based on the Nexus IQ report information.</p>	Request exception
portal, portal- sdk	common s- fileupload	<p>If not false positive, can be handled with the new version upgrade which do not have vulnerability.</p> <div>  PORTAL-443 - commons-fileupload CLOSED </div> <p>Explanation</p> <p>Apache Commons FileUpload contains a resource leak which may lead to a Denial of Service (DoS) attack.</p>	Target fix in Dublin release
portal-sdk	xerces	<p>There is no non vulnerable version of this package.</p> <div>  PORTAL-445 - xerces CLOSED </div> <p>Explanation</p> <p>Apache Xerces2 is vulnerable to a Denial of Service (DoS) attack.</p>	Request exception
portal-sdk	bootstrap	<p>There is no non vulnerable version of this package.</p>	Request exception
portal, portal-sdk	org. bouncycas tle	<p>If not false positive, can be handled with the new version upgrade which do not have vulnerability.</p> <div>  PORTAL-444 - bouncy castle CLOSED </div> <p>Explanation</p> <p>Bouncy Castle is vulnerable to Remote Code Execution (RCE).</p>	we will try to handle them in Dublin release based on the resource availability and priority
portal	org. codehaus s.groovy	<p>If not false positive, can be handled with the new version upgrade which do not have vulnerability.</p> <div>  PORTAL-447 - codehaus.groovy CLOSED </div> <p>Explanation</p> <p>Groovy is vulnerable to insecure deserialization leading to Remote Code Execution (RCE).</p>	we will try to handle them in Dublin release based on the resource availability and priority
portal	org. eclipse. jetty	<p>If not false positive, can be handled with the new version upgrade which do not have vulnerability.</p> <div>  PORTAL-448 - jetty CLOSED </div> <p>Explanation</p> <p>Eclipse Jetty Server is vulnerable to HTTP request smuggling.</p>	we will try to handle them in Dublin release based on the resource availability and priority
portal, portal-sdk	org. apache. lucene	<p>Not used, this will be removed.</p> <div>  PORTAL-440 - Lucene libraries CLOSED </div>	we will try to handle them in Dublin release
portal	org. apache. tomcat. embed	<p>There is no non vulnerable version of this component/package.</p> <div>  PORTAL-449 - tomcat.embedded CLOSED </div> <p>Explanation</p> <p>Apache Tomcat is vulnerable to a Cross-Origin attack due to the insecure default configuration of the CORS filter.</p>	Request exception

portal	org. apache. cxf	<p>False positive</p> <p>We do not use the below code, which is vulnerable.</p> <pre>System.setProperty("java.protocol.handler.pkgs", "com.sun.net.ssl.internal.www.protocol");</pre> <div>  PORTAL-450 - cxf CLOSED </div>	Not Vulnerable
portal	org. hibernate	<p>If not false positive, can be handled with the new version upgrade which do not have vulnerability.</p> <div>  PORTAL-444 - Hibernate validator CLOSED </div> <p>Explanation</p> <p>The Hibernate Validator (HV) package is vulnerable to a privilege escalation vulnerability.</p>	we will try to handle them in Dublin release based on the resource availability and priority