




Casablanca CLAMP 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	Action
clamp	com. fasterxml. jackson. core	<p>From NexusIQ:</p> <p>" jackson-databind is vulnerable to Remote Code Execution (RCE). The <code>createBeanDeserializer()</code> function in the <code>BeanDeserializerFactory</code> class allows untrusted Java objects to be deserialized. A remote attacker can exploit this by uploading a malicious serialized object that will result in RCE if the application attempts to deserialize it."</p>	<ul style="list-style-type: none">▪ We have added a Jackson wrapper that must be used in the code, it disables the incriminated feature. We have also added a unit test to ensure the code is secure.▪ We will change that library and replace it by another one (GSON) <div> CLAMP-236 - Replace Jackson by another JSON library CLOSED</div>
clamp	angular	<p>It impacts our UI as angular is the skeleton technology used in the code.</p> <p>Anyway we have mitigated the issue by setting the angular version to 1.3.2 with the least amount of security issue reported by Nexus IQ (for Release 1.XX)</p>	<p>Analyze how to migrate the UI to a recent angular version (> 4.X)</p> <div> CLAMP-223 - replace "angular.js" and move to "React" for security issues CLOSED</div>
clamp	bootstrap	<p>It impacts our UI as bootstrap (one of the latest version, 4.1.1) is used in clamp code.</p> <p>We could be impacted by the possible Cross-Site Scripting (XSS) reported by Nexus IQ</p>	<p>bootstrap library 4.1.3 CLAMP is using, doesn't present a vulnerability anymore</p> <div> CLAMP-237 - Delete or Replace Bootstrap library in UI CLOSED</div>