Dublin OOF 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
optf/cmso	com.fasterxml.jackson.core	False positive `jackson-databind` is vulnerable to Remote Code Execution (RCE). The `createBeanDeserializer()`function in the `BeanDeserializerFactory` 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. A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x before 2.9.9. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint, the service has the mysql-connector-java jar (8.0.14 or earlier) in the classpath, and an attacker can host a crafted MySQL server reachable by the victim, an attacker can send a crafted JSON message that allows them to read arbitrary local files on the server. This occurs because of missing com.mysql.cj.jdbc.admin.MiniAdmin validation. 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.	1. CMSO only configures Spring Security for Unit testing purposes (CSIT_ enabled via a Spring Profile. OOM testing is configured to use AAF. 2. When configured for Unit testing CMSO is running Spring Security 5.1.4. RELEASE blocked URLOPTFRA-397 - CMSO Update to Spring Boot 2.1.3-RELEASE CLOSED blocked URLOPTFRA-390 - Add AAF AUthentication to CMSO CLOSED
optf/cmso	org.apache.tomcat.embed	False positive When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows.	Since we do not run this in windows, CMSO is not vulnerable. blocked URLOPTFRA-480 - Fix tomcat-embed-core vulnerability SUBMITTED
optf/cmso	org.springframework.security	False positive The spring-security-core package has a cryptographic weakness. The `getObject` method in `SecureRandomFactoryBean.class` uses a seed to create a cryptographically sensitive value in a reversible manner. An attacker with access to the random material produced by a vulnerable application's seed can exploit this behavior to decrypt values that would not normally be accessible.	1. CMSO only configures Spring Security for Unit testing purposes (CSIT) enabled via a Spring Profile. OOM testing is configured to use AAF and HTTPS 2. There are no references to SecureRandomFactoryBean in CMSO blocked URLOPTFRA-478 - Fix Vulnerability with spring-security-core package SUBMITTED
optf/cmso	org.springframework.security	The `spring-security-web` package is vulnerable to Cross-Site Request Forgery (CSRF). The application is vulnerable by using this component if the Switch User Processing Filter is configured.	There is no non vulnerable version of this component/package. We need to investigate alternative components. blocked URLOPTFRA-431 - Fix Vulnerability with spring-security-web package REOPENED
optf/cmso	org.springframework.data	This affects Spring Data JPA in versions up to and including 2.1.5, 2.0.13 and 1.11.19. Derived queries using any of the predicates ?startingWith?, ?endingWith? or ?containing? could return more results than anticipated when a maliciously crafted query parameter value is supplied. This affects Spring Data JPA in versions up to and including 2.1.6, 2.0.14 and 1.11.20. ExampleMatcher using ExampleMatcher.StringMatcher.STARTING, ExampleMatcher.StringMatcher.ENDING or ExampleMatcher.StringMatcher.CONTAINING could return more results than anticipated when a maliciously crafted example value is supplied.	OPTFRA-481 - Fix Vulnerability with spring-data-jpa package OPEN