# CS 305 Module Two Coding Assignment Template

Abdulrahman Al-Nachar

CS305 / 2-2

## Run Dependency Check

A screenshot of a computer

Description automatically generated

## Document Results

Dependency Vulnerability ID PackageSeverity

|  |  |  |  |
| --- | --- | --- | --- |
| hibernate-validator-6.0.18.Final.jar | cpe:2.3:a:redhat:hibernate\_validator:6.0.18 | /org.hibernate.validator/hibernate-validator@6.0.18.Final | MEDIUM |
| jackson-databind-2.10.2.jar | cpe:2.3:a:fasterxml:jackson-databind:2.10.2 | /com.fasterxml.jackson.core/jackson-databind@2.10.2 | HIGH |
| log4j-api-2.12.1.jar | cpe:2.3:a:apache:log4j:2.12.1 | /org.apache.logging.log4j/log4j-api@2.12.1 | LOW |
| logback-core-1.2.3.jar | cpe:2.3:a:qos:logback:1.2.3 | /ch.qos.logback/logback-core@1.2.3 | HIGH |
| mongo-java-driver-2.4.jar | cpe:2.3:a:mongodb:java\_driver:2.4 | /org.mongodb/mongo-java-driver@2.4 | MEDIUM |
| snakeyaml-1.25.jar | cpe:2.3:a:snakeyaml\_project:snakeyaml:1.25 | /org.yaml/snakeyaml@1.25 | CRITICAL |
| spring-boot-2.2.4.RELEASE.jar | cpe:2.3:a:vmware:spring\_boot:2.2.4 | /org.springframework.boot/spring-boot@2.2.4.RELEASE | CRITICAL |
| spring-boot-starter-web-2.2.4.RELEASE.jar | cpe:2.3:a:vmware:spring\_boot:2.2.4 | /org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE | CRITICAL |
| spring-core-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3 | /org.springframework/spring-core@5.2.3.RELEASE | CRITICAL\* |
| spring-expression-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3 | /org.springframework/spring-expression@5.2.3.RELEASE | CRITICAL\* |
| spring-web-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3 | /org.springframework/spring-web@5.2.3.RELEASE | CRITICAL\* |
| spring-webmvc-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3 | /org.springframework/spring-webmvc@5.2.3.RELEASE | CRITICAL\* |
| tomcat-embed-core-9.0.30.jar | cpe:2.3:a:apache:tomcat:9.0.30 | /org.apache.tomcat.embed/tomcat-embed-core@9.0.30 | CRITICAL\* |
| tomcat-embed-websocket-9.0.30.jar | cpe:2.3:a:apache:tomcat:9.0.30 | /org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30 | CRITICAL\* |

## Analyze Results

**hibernate-validator-6.0.18.Final.jar:**

**Problem:** A flaw was found in Hibernate Validator version 6.1.2.Final. A bug in the message interpolation processor enables invalid EL expressions to be evaluated as if they were valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages.

**Fix:** update Hibernate Validator to the newest version.

**jackson-databind-2.10.2.jar:**

**Problem:** A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.

**Fix:** Upgrade com.fasterxml.jackson.core:jackson-databind to version 2.6.7.4 or higher.

**log4j-api-2.12.1.jar:**

**Problem:** Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender. Fixed in Apache Log4j 2.12.3 and 2.13.1

**Fix:** update log4j-api-2.12.1. to 2.12.3 .

**logback-core-1.2.3.jar:**

**Problem:** A serialization vulnerability in logback receiver component part of logback version 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending poisoned data.

**Fix:** update logback-core-1.2.3. to 1.2.13.

**mongo-java-driver-2.4.jar:**

**Problem:** Specific versions of the Java driver that support client-side field level encryption (CSFLE) fail to perform correct host name verification on the KMS server’s certificate. This vulnerability in combination with a privileged network position active MITM attack could result in interception of traffic between the Java driver and the KMS service rendering Field Level Encryption ineffective. This issue was discovered during internal testing and affects all versions of the Java driver that support CSFLE. The Java async, Scala, and reactive streams drivers are not impacted. This vulnerability does not impact driver traffic payloads with CSFLE-supported key services originating from applications residing inside the AWS, GCP, and Azure network fabrics due to compensating controls in these environments. This issue does not impact driver workloads that don’t use Field Level Encryption.

**Fix:** this issue has been patched in newer versions like 3.11.3.

**snakeyaml-1.25.jar:**

**Problem:** SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization. We recommend upgrading to version 2.0 and beyond.

**Fix:** this issue has been fixed in the SnakeYAML 2.0 version

**spring-boot-2.2.4.RELEASE.jar:**

**Problem:** In Spring Boot versions 3.0.0 - 3.0.5, 2.7.0 - 2.7.10, and older unsupported versions, an application that is deployed to Cloud Foundry could be susceptible to a security bypass. Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+. Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+.

**Fix:** update spring-boot-2.2.4. to the newest supported 3.0.6 version.

**spring-boot-starter-web-2.2.4.RELEASE.jar:**

**Problem:** In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache.

**Fix: :** update spring-boot-2.2.4. to the newest supported 3.0.6 version.

**spring-core-5.2.3.RELEASE.jar:**

**Problem:** A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

**Fix:** upgrade spring framework to the newest version.

**spring-expression-5.2.3.RELEASE.jar:**

**Problem:** In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

**Fix:** upgrade spring framework to the newest version.

**spring-web-5.2.3.RELEASE.jar:**

**Problem:** In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

**Fix:** upgrade spring framework to the newest version.

**spring-webmvc-5.2.3.RELEASE.jar:**

**Problem:** In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, application with a STOMP over WebSocket endpoint is vulnerable to a denial of service attack by an authenticated user.

**Fix:** upgrade spring framework to the newest version.

**tomcat-embed-core-9.0.30.jar:**

**Problem:** When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

**Fix:** Apache released this version that fixes this 9.0.31.

**tomcat-embed-websocket-9.0.30.jar:**

**Problem:** Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.

**Fix:** update apache tomcat to the latest supported version.

**Summary:**

Almost all of the flaws, bugs, vulnerabilities, issue found in this check today is because the frameworks and dependencies used in the program needs to be updated the their latest supported versions , almost all of the problems found today has been solved by these dependency developers and released in later versions.