GLOBALRAIN

**Artemis Financial Vulnerability Assessment Report**

## Table of Contents

**Document Revision History**

| Version | Date | Author | Comments |
|---|---|---|---|
| 1.0 | 7/13/2023 | Kyle Lund | Changes are made in client needs, security, mitigations, and testing |

**Client**


**Instructions**

Submit this completed vulnerability assessment report. Replace the bracketed text with the relevant information. In the report, identify your findings of security vulnerabilities and provide recommendations for the next steps to remedy the issues you have found.

- Respond to the five steps outlined below and include your findings.
- Respond using your own words. You may also choose to include images or supporting materials. If you include them, make certain to insert them in all the relevant locations in the document.
- Refer to the Project One Guidelines and Rubric for more detailed instructions about each section of the template.

**Developer**
Kyle Lund

## 1. Interpreting Client Needs

The client Artemis Financial has certain needs regarding external threats. Secure communications are important to the client as it ensures the security and integrity of sensitive data moved between the system, users, and external users. It is important to follow security and cross-border regulations as data is moved between international borders. Along with cross border transactions, there is a need to follow any governmental restrictions or regulations that might impose requirements on secure communications. It is a need to secure client data and any sensitive data while following our governments and international government regulations. Current threats now can include malicious hackers looking for potential exploits, vulnerabilities, data breaches, and unauthorized access to the system. These threats will be a constant threat as the system updates and new exposure may occur. As part of the security requirements, it is important to investigate modernization requirements. This will include evaluating open-source libraries and web application technologies. Using outdated and vulnerable libraries can lead to potential security risks, staying up to date with frameworks and technologies is important to keep a safe software application.

## 2. Areas of Security

Areas of security include the following;

Input Validation:
The software should have a form of input validation to prevent common vulnerabilities such as injection attacks.

Cryptography:
The software should have a form of data protection. Encryption is a good safeguard for sensitive data during storage and transmission. It should handle sensitive data securely and ensure only those with proper decryption keys have access to the information.

Code Error:
The system should have secure defaults and error handling. If an error should occur, no sensitive information should be revealed in the error message.

APIs:
The application should have secure communication protocols. When the system is communicating with external services and APIs, it should verify and authenticate the receiving data.

Authorization:
The System should have secure authorization mechanics in place. This is to ensure only users with the proper authorization can access the sensitive data, these authorizations should also be restricted per user roles. Restriction of authorization per user is important to prevent users from accessing data outside of their role and permissions.

## 3. Manual Review

In the DocData class, the read document method accepts key and value as a parameter. This line of code does not set a parameter for the inputs which could potentially lead to injection vulnerabilities. In the DocData class it tries to connect to a database using DriverManager.getConnection, without specifying a secure connection to the database server.

## 4. Static Testing

Below is the dependency checklist

Scan Information (show all):

- *dependency-check version:* 8.3.1
- *Report Generated On:* Thu, 13 Jul 2023 16:58:43 -0700
- *Dependencies Scanned:* 38 (22 unique)
- *Vulnerable Dependencies:* 13
- *Vulnerabilities Found:* 114
- *Vulnerabilities Suppressed:* 0
- ...

**Summary**

Display: Showing Vulnerable Dependencies (click to show all)

| Dependency | Vulnerability IDs | Package | Highest Severity | CVE Count | Confidence | Evidence Count |
|---|---|---|---|---|---|---|
| tomcat-embed-websocket-9.0.30.jar | cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:*<br>cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:* | pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30 | CRITICAL* | 21 | Highest | 30 |
| tomcat-embed-core-9.0.30.jar | cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:*<br>cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:* | pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30 | CRITICAL* | 20 | Highest | 30 |
| spring-webmvc-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*<br>cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*<br>cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*<br>cpe:2.3:a:web_project:web:5.2.3:release:*:*:*:*:*:* | pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE | CRITICAL* | 11 | Highest | 36 |
| spring-web-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*<br>cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*<br>cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:*<br>cpe:2.3:a:web_project:web:5.2.3:release:*:*:*:*:*:* | pkg:maven/org.springframework/spring-web@5.2.3.RELEASE | CRITICAL* | 12 | Highest | 34 |
| spring-core-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:*<br>cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*<br>cpe:2.3:a:vmware:spring_framework:5.2.3:release:*:*:*:*:*:* | pkg:maven/org.springframework/spring-core@5.2.3.RELEASE | CRITICAL* | 11 | Highest | 36 |
| snakeyaml-1.25.jar | cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:*:*:*:*:*:*:* | pkg:maven/org.yaml/snakeyaml@1.25 | CRITICAL | 8 | Highest | 44 |
| spring-boot-starter-web-2.2.4.RELEASE.jar | cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:*:*<br>cpe:2.3:a:web_project:web:2.2.4:release:*:*:*:*:*:* | pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE | HIGH | 2 | Highest | 35 |
| spring-boot-2.2.4.RELEASE.jar | cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:*:* | pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE | HIGH | 2 | Highest | 39 |
| jackson-databind-2.10.2.jar | cpe:2.3:a:fasterxml:jackson-databind:2.10.2:*:*:*:*:*:*:*<br>cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:*:*:*:*:*:*:* | pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2 | HIGH | 6 | Highest | 39 |
| bcprov-jdk15on-1.46.jar | cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.46:*:*:*:*:*:*:*<br>cpe:2.3:a:bouncycastle:bouncy_castle_crypto_package:1.46:*:*:*:*:*:*:*<br>cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.46:*:*:*:*:*:*:*<br>cpe:2.3:a:bouncycastle:the_bouncy_castle_crypto_package_for_java:1.46:*:*:*:*:*:*:* | pkg:maven/org.bouncycastle/bcprov-jdk15on@1.46 | HIGH | 18 | Highest | 38 |
| logback-core-1.2.3.jar | cpe:2.3:a:qos:logback:1.2.3:*:*:*:*:*:*:* | pkg:maven/ch.qos.logback/logback-core@1.2.3 | MEDIUM | 1 | Highest | 31 |
| hibernate-validator-6.0.18.Final.jar | cpe:2.3:a:redhat:hibernate_validator:6.0.18:*:*:*:*:*:*:* | pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final | MEDIUM | 1 | Highest | 32 |
| log4j-api-2.12.1.jar | cpe:2.3:a:apache:log4j:2.12.1:*:*:*:*:*:*:* | pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1 | LOW | 1 | Highest | 42 |

There are thirteen dependencies vulnerabilities ranging from critical to low severity.

| | |
|---|---|
| Tomcat embed web socket 9.0.30 | 21 vulnerabilities Critical severity |
| Tomcat embed core 9.0.30 | 20 vulnerabilities Critical severity |
| Spring webmvc 5.2.3 | 11 vulnerabilities Critical severity |
| Spring web 5.2.3 | 12 vulnerabilities Critcal severity |
| Spring core 5.2.3 | 11 vulnerabilities Critical severity |
| Snakeyaml 1.25 | 8 vulnerabilities Critical severity |
| Spring boot starter web 2.2.4 | 2 vulnerabilities High severity |
| Jackson data bind 2.10.2 | 2 vulnerabilities High severity |
| Bcprov jdk15on 1.46 | 18 vulnerabilities High severity |

| | |
|---|---|
| Spring boot 2.2.4 | 2 vulnerabilities High severity |
| Logback core 1.2.3 | 1 vulnerability medium severity |
| Hibernate validator 6.0.18 | 1 vulnerability medium severity |
| Log4j Api 2.12.1 | 1 vulnerabiltiiy Low severity |

**Many of the vulnerabilities include non-secure access via http, outdated and unsafe versions, and leaks in certain versions that allow for denial of service (DOS) attacks. Vulnerabilities in the unsecure access through a reverse proxy via HTTP have been discovered through unprotected transport of credentials. The recommended solutions include keeping versions and libraries up to date, securing HTTPS by protecting any data moving out of the system, and including security systems to stop denial of service attacks.**

## 5. Mitigation Plan

All Tomcat and Spring frameworks should be updated to their latest versions to prevent exploits that lead to DoS (denial of service) attacks. To prevent unwanted leaking of credentials all HTTP related frameworks should be updated to their latest versions and ensure a secure connection to HTTPS. There are unsupported and unsafe versions of frameworks that need to be updated to prevent potential problems. Regardless of the level of severity all frameworks need to be updated to their respective latest versions as most problems occur when older versions lead to vulnerabilities and potential problems the longer outdated frameworks stay in our system.