****

# Artemis Financial Vulnerability Assessment Report

Table of Contents

[Document Revision History 3](#_Toc32574607)

[Client 3](#_Toc32574608)

[Instructions 3](#_Toc32574609)

[Developer 4](#_Toc32574610)

[1. Interpreting Client Needs 4](#_Toc32574611)

[2. Areas of Security 4](#_Toc32574612)

[3. Manual Review 4](#_Toc32574613)

[4. Static Testing 4](#_Toc32574614)

[5. Mitigation Plan 4](#_Toc32574615)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **1/28/2024** | **Jennifer Allen** |  |

## Client



## Developer

Jennifer Allen

## Interpreting Client Needs

Artemis Financial is looking to update and utilize the latest technology and practices for their company to protect themselves, and their clients’ personal information, from external threats. Since Artemis specializes in an industry that handles sensitive information, they are also looking for secure communications. They do not say whether they are going to be handling international transactions, however it is highly likely that they will. In which case there will be governmental restrictions that need to be considered to protect Artemis from fraud and hijackers. When it comes to open-source libraries, Artemis would need to focus heavily on secure communication and cryptography.

## Areas of Security

Areas of Security that are most applicable are:

* Input Validation – This is to help ensure that all data being received from the users is compatible and up to the standard that Artemis is expecting. Also, it will help to protect from common vulnerabilities such as cross-site scripting.
* APIs – secure APIs are vital in that secure communication between applications is taking place. Whether it is internal communication or external.
* Cryptography – Encryption is going to be very important for both Artemis and the clients. Since information going back and forth will include tax ID numbers, account numbers, etc. all highly sensitive information.
* Code Quality – Utilizing best practices will help protect from unauthorized users to having access to information.

## Manual Review

After reviewing the code provided, I noticed that the code quality overall was decent. However, as for input validation it seemed to be lacking. On line 28 in the Greeting Controller, it accepts a string for input without any steps following for security. I was unable to see any indication of cryptography.

A computer code with text

Description automatically generated with medium confidence

## Static Testing

A screenshot of a service

Description automatically generated

* **bcprov-jdk15on-1.46.jar - The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms.**
* **hibernate-validator-6.0.18.Final.jar - Hibernate's Bean Validation (JSR-380) reference implementation.**
* **jackson-databind-2.10.2.jar - General data-binding functionality for Jackson: works on core streaming API**
* **log4j-api-2.12.1.jar - The Apache Log4j API**
* **logback-core-1.2.3.jar - logback-core module**
* **snakeyaml-1.25.jar -YAML 1.1 parser and emitter for Java**
* **spring-boot-2.2.4.RELEASE.jar - Spring Boot**
* **spring-boot-starter-web-2.2.4.RELEASE.jar - Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container.**
* **spring-core-5.2.3.RELEASE.jar – Spring Core**
* **spring-web-5.2.3.RELEASE.jar – Spring Web**
* **spring-webmvc-5.2.3.RELEASE.jar – Spring Web MVC**
* **tomcat-embed-core-9.0.30.jar – Core tomcat implementation**
* **tomcat-embed-websocket-9.0.30.jar – Core tomcat implementation**

## Mitigation Plan

After manually reviewing the code provided and running a dependency check, multiple vulnerabilities and dependencies came back for cryptography, APIs, and outdated versions of software being utilized. By updating bouncy castle our program would be more secure when it comes to our information being encrypted. Spring is also being used with old versions, by switching to the most recent version it would solve approximately five of the dependencies found. Also, Tomcat is another that needs updated as well to help with Spring running smoothly. With updates to all latest versions made our application should run smoothly with secure connections and communications.