****

# 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** | **11/10/23** | **Davi Nen** |  |

## Client



## Developer

Davi Nen

## Interpreting Client Needs

* What is the value of secure communications to the company?
  + When a company uses secure protocols and secure data communication techniques to send and receive data between the server and client, it is said to be using secure communication. This ensures that no data is lost and that only trusted users receive the data during the communication. For these reasons, having secure connections should be very important.
* Does the company make any international transactions?
  + If someone accesses the data internationally, the corporation may generate an international transaction.
* Are there governmental restrictions about secure communications to consider?
  + There are no laws against encrypted communication; in fact, the government encourages businesses to employ private communication methods to safeguard customer privacy and data.
* What external threats might be present now and in the immediate future?
  + Any existing or future risks would be the pursuit of financial data about the client and the business, as well as personal information on behalf of a client.
* What are the modernization requirements that you must consider?
  + Modernization includes things like the development of security web applications that operate in sandboxed environments to guarantee high security. The business can enhance the functionality of their software by using open-source libraries.

## Areas of Security

In order to write organized code with a degree of security that will assist in avoiding outside invasions, secure coding is required. Code errors are necessary because, in order to ensure that everything is secure, the organization must manage problems such as repeated login attempts. The usage of RESTful API by the web services necessitates a certain level of safe communication, which makes APIs necessary as well. The final one is input validation; because the RESTful API requires user input, it needs to be cleared and verified securely.

## Manual Review

* Since the service does not employ HTTPS, sharing sensitive information via HTTPS is advised.
* There isn't a mechanism in place for authentication purposes.
* Because requests are not verified, the system is open to outside interference.
* Business names are supplied in the CRUD Controller class as request parameters. This demonstrates its vulnerability by allowing information to be leaked to outside parties.

## Static Testing

* bcprov-jdk15on-1.46.jar – several vulnerabilities on 1.46. Needs update
* Log4j-api-2.12.1.jar – one vulnerability. Needs update
* Snakeyalm-1.25.jar – one vulnerability. Needs update
* Jackson-databind-2.10.2.jar – one vulnerability. Needs update
* Tomcat-embed-core-9.0.30.jar – several vulnerabilities. Needs update
* Hibernate-validator-6.0.18.Final.jar – one vulnerability. Needs update
* Spring-core-5.2.3.RELEASE.jar – one vulnerability. Needs update

## Mitigation Plan

Prior to addressing any upcoming problems or present ones, it is advised to make sure that client and corporate information is secure. All direct communication must switch to HTTPS in order to guard against outside eavesdropping. Second, assign headers to request parameters. Third, take out any mention of company names in the hard-coded database logins. Fourth, put two-factor/general authentication solutions into place and turn them on. This will make it far more difficult for an outsider to obtain important information by protecting user data and identification as well as company identity. Update each and every dependent found in the dependency check mentioned above.