****

# 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** | **21 May 2023** | **Keith Spraglin** |  |

## 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

Keith Spraglin

## Interpreting Client Needs

Artemis Financial is an international company that works with clients worldwide and international transactions. Artemis help individuals with different financial plans from opening savings accounts to auto and home insurance, with all the financial needs in between. The security of the company is vital to its success, they handle personal and classified information of their clients and mutual business partners. The data going in and out of Artemis should be heavily encrypted because the threat of their clients personal being target is always high. Having regularly bug fixes and updates on the security of data will limited the exposure of leaked data.

## Areas of Security

After looking at the Vulnerability Assessment Process Flow Diagram, I identified areas of security that will benefit Artemis Financials software.

* Input Validation – this is required by the financial company to validate information being inputted into the software. This extra step will provide more protection for users.
* APIs – having API would be necessary for the financial company because it would filter what data is accepted.
* Cryptography – having the company software encrypted, will have a significant impact because banks deal with different currencies so user information will be secure from people around the world.
* Code Error – having code error, will back up the APIs work. This applies another barrier for helping keep user information being exposed.

## Manual Review

The first vulnerability I seen was in the CRUDController.java file. The application shoes exposure for internal objects. When the value “business\_name” is passed through it will expose the DOCData database. That lead me to the DocData.java file. The username and password might show vulnerabilities. This might show an issue because username and passwords might be easily guessed by random people.

## Static Testing

* Bcprov-jdk15on-1.46.jar, has 14 vulnerabilities that need to be updated to the latest software.
* Log4j-api-2.12.jar, has one vulnerability that needs to be update to the latest version.
* Tomcat-embed-core-9.0.31.jar, shows multiple vulnerabilities that need to be updates to latest version.

## Mitigation Plan

To help ensure all future issues with the identified security vulnerabilities, Artemis will need to ensure their customers and clients information is secure. Remove any hard coded credentials in the database like business names, or customers personal information. Adding an extra layer of protection with two factor authentication. Protecting the shared information between customer/client and

Artemis Financial from outside threat is crucial for a successful company.