****

# 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** | **13 September 2023** | **Clay Nottingham** |  |

## 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

Clay Nottingham

## Interpreting Client Needs

In today’s financial and technological landscape, keeping personal data secure is paramount, with financial security being of the utmost importance. With the worldwide push for a more global economy, and with so many people doing business and financial transactions from all over the world, the concept of international transactions occurring frequently is definitely a possibility. Because of all of the financial and personal information being at stake, and with the current ongoing security risks of foreign groups such as Storm-0558 breaching government information, it’s safe to say these risks certainly pertain to Artemis Financial, so U.S. government regulations pertaining to secure communications will have to be adhered to such as the Computer Fraud and Abuse Act of 1986. External threats that companies live in fear over include, but are not limited to spyware, social engineering, ransomware, and phishing. It is our mission at Global Rain to provide preventative measures to mitigate such risks. Frequent updates and functionality checks will be essential tokens for ensuring security and combating threats.

## Areas of Security

The company software’s APIs are important to consider due to the fact that they are needed for two applications to communicate with one another, which puts a company such as a financial institution at tremendous risk, especially when international transactions are put into consideration, so proper coding and current versions of software must be ensured. Cryptography is paramount in assuring the security of user’s sensitive data, at Global Rain, this is a major concern of ours. Last but not least the company software’s code quality must be inspected is essential because the code must be clear, functional, and properly debugged.

## Manual Review

When doing a manual review of the code, a few issues came to the forefront. In the DocData.java class a local variable isn’t used, keeping clean and bug-free code is vital for security purposes. Also in the pom.xml I would make sure the current version of the spring maven plug-in is being utilized.

## Static Testing

A dependency check report was conducted, and the following vulnerabilities were identified and cross-referenced with the National Vulnerability Database:

bcprov-jdk15on-1.46.jar- The bouncy castle version 1.46 is outdated and should be updated to the current version of 1.56. (National Vulnerability Database, 2018).

hibernate-validator-6.0.18.Final.jar - An error was found Hibernate Validator 6.1.2 and should not only be updated to the current version but debugged as well. (National Vulnerability Database, 2020).

jackson-databind-2.10.2.jar – Previous versions have allowed hackers to commit denial of service attacks and must be updated to the current version of 2.13.1. (National Vulnerability Database, 2023).

log4j-api-2.12.1.jar – Previous versions from the current 2.18.0 are subject to remote code execution attacks and must be updated. (National Vulnerability Database, 2021).

logback-core-1.2.3.jar - Previous versions of the current 1.2.8 are subject to attacks from a user with specific privileges to edit configurations and install malicious ones and must be updated. (National Vulnerability Database, 2021).

snakeyaml-1.25.jar – Using snakeyaml is not recommended due to the risk of denial of service attacks. (National Vulnerability Database, 2022).

spring-boot-2.2.4.RELEASE.jar – Version 2.2.4 as well as other previous versions have been subject to denial of service attacks and must be updated to the current version of 3.1.3. (National Vulnerability Database, 2023).

tomcat-embed-core-9.0.30.jar – URL Redirection to untrusted sites vulnerability found in FORM authentication in previous versions of Apache Tomcat. This must be updated to version 11. (National Vulnerability Database, 2023).

## Mitigation Plan

The issues found in the static testing are typically caused by outdated software which can lead to security threats, so updating to the latest version will serve to be the best solution to this problem. This serves to mitigate performance issues and can also ensure that new features are installed. Another mitigation strategy to keep in mind is secure coding practices as unclear code also leads to security risks. Global Rain is more than happy to help Artemis Financial ensure the security of the company and its users they rely on.

SOURCES:

National Vulnerabilities Database - Search and Statistics. (2019-2023). https://nvd.nist.gov/vuln/search