****

# 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** | **[9/15/23]** | **[Jamei Javis]** | **Completed the document** |

## 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

Jamie Javis

## Interpreting Client Needs

Securing communications is necessary for multiple businesses, as they plan to guarantee that their interactions with clients remain private. The potential of an unknown third-party eavesdropping on their conversations is a worry nobody wants to deal with.

Given Artemis Financials’ role in helping customers with their financial data, it's urgent that they protect internal transactions from outside interference. Furthermore, being a financial organization, they must carefully follow the government guidelines pertaining to these transactions. In this business, there are external threats posed by malicious individuals seeking to compromise client information, such as credit card, debit cards and bank info, which emphasizes the necessity for strict security methods.

## Areas of Security

The implementation of APIs is crucial, and Artemis Financial depend on RESTful APIs for their operations. APIs play a fundamental role in ensuring the protection of all interactions.

Moreover, robust input validation is imperative, especially since APIs accept input from users. In cases where a user harbors malicious intentions, there's a risk of system harm. Thus, rigorous input validation is indispensable.

The two corresponding aspects are code error management and code quality assurance. Code error management relates to how the system manages errors. The system must accurately address errors that may arise if a user accidentally initiates them.

Code quality involves adhering to standard coding practices, including incorporating security procedures. Essentially, programmers must uphold a security-conscious method throughout the system's development to reinforce it against potential hacking efforts

## Manual Review

* The system’s lack of HTTPS develops concerns when handling sensitive information.
* Verification mechanisms are visibly missing throughout the codebase.
* Requests remain unchecked for authorization, posing a substantial liability to potential hacker exploits.
* In the CRUD Controller class, business names are transferred as request parameters, creating a prospective attack vector that exposes the system to security threats.

## Static Testing

A screenshot of a computer

Description automatically generated

* bcprov-jdk15on-1.46.jar - several vulnerabilities on 1.46, update to latest version.
  + CVE-2013-1624
  + CVE-2015-6644
  + CVE-2015-7940
  + CVE-2016-1000338
  + CVE-2016-1000339
  + CVE-2016-1000341
  + CVE-2016-1000342
  + CVE-2016-1000343
  + CVE-2016-1000344
  + CVE-2016-1000345
  + CVE-2016-1000346
  + CVE-2016-1000352
  + CVE-2017-13098
  + CVE-2018-5382
  + CVE-2020-0187
  + CVE-2020-26939
  + CVE-2023-33201
* log4j-api-2.12.1.jar – 5 vulnerabilities, update to latest version.
  + CVE-2020-9488
  + CVE-2021-44228
  + CVE-2021-44832
  + CVE-2021-45046
  + CVE-2021-45105
* snakeyaml-1.25.jar – multiple vulnerability, update to latest version.
  + CVE-2017-18640
  + CVE-2021-4235
  + CVE-2022-1471
  + CVE-2022-25857
  + CVE-2022-3064
  + CVE-2022-38749
  + CVE-2022-38750
  + CVE-2022-38751
  + CVE-2022-38752
  + CVE-2022-41854
* jackson-databind-2.10.2.jar - 6 vulnerability, update to latest version.
  + CVE-2020-25649
  + CVE-2020-36518
  + CVE-2021-46877
  + CVE-2022-42003
  + CVE-2022-42004
  + CVE-2023-35116
* tomcat-embed-core-9.0.30.jar - several vulnerabilities, update to latest tomcat version
  + CVE-2019-17569
  + CVE-2020-11996
  + CVE-2020-13934
  + CVE-2020-13935
  + CVE-2020-13943
  + CVE-2020-17527
  + CVE-2020-1935
  + CVE-2020-1938
  + CVE-2020-8022
  + CVE-2020-9484
  + CVE-2021-24122
  + CVE-2021-25122
  + CVE-2021-25329
  + CVE-2021-30640
  + CVE-2021-33037
  + CVE-2021-41079
  + CVE-2021-43980
  + CVE-2022-29885
  + CVE-2022-34305
  + CVE-2022-42252
  + CVE-2023-28708
  + CVE-2023-41080
* hibernate-validator-6.0.18.Final.jar - one vulnerability, update to latest version.
  + CVE-2020-10693

## Mitigation Plan

After assessing the outcomes from the manual review and static testing, I have identified multiple security vulnerabilities in Artemis Financials’ software application. To address both existing and potential future issues, the following steps are recommended:

* Enhance Data Security – Transition to HTTPS for all of the communication to help prevent unauthorized access. This helps ensure the security of company/client information
* Request Parameter Handling – Move request parameters from the URLs to headers for improved security. This practices enhanced data security and helps prevent potential data leaks
* Dependency Updates – Update all of the project’s dependencies. This helps ensure that the software is up to date with the most recent security updates
* Implement 2FA – Helps strengthen the system by authorizing user authentication. This adds a layer of security and includes access control.
* Secure Database – Remove hard coded database credentials. This helps reduce data leaks and prevent unauthorized users from obtaining access to the system.

By following these suggestions, Artemis Financials’ software application can substantially improve its security strengths, protection of the company’s sensitive information, and greatly reduce the risk of security breaches.