****

# 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** | **03/24/2024** | **Evan Carter** | **First Draft** |

## Client



## Developer

Evan Carter

## Interpreting Client Needs

Artemis Financials handles highly sensitive customer financial and identification data, both of which could be used for malicious purposes such as theft or impersonation. The security of this information is penultimate to the continued operation of the company.

Servicing international customers requires Artemis Financials to comply with all extra-national security requirements. Government-operated insurance plans may impose security requirements for the data of their patients that are not mandated by private organizations.

Communications hijacking and database cracking or disruption are some of the key threats Artemis Financials may experience. The utilization of open-source libraries is valuable for security purposes, as they are subject to scrutiny and revision by all parties, leading to an overall more secure product.

## Areas of Security

Input Validation

* User input is only controllable to a certain degree. Console input has the potential to cause errors in the application if it does not match what the program is expecting.

APIs

* Interfacing with the services of other companies in order to send, retrieve, or monitor information is subject to threats.

Cryptography

* Customer data encryption is paramount to ensuring that it is not able to be interpreted if released.

Client / Server

* Validation of proper secure communication between client and server, such as during web services, should prevent data from being intercepted.

Code Error

* Errors that do occur must be properly handled to prevent the program from exhibiting unintended behavior or becoming non-functional.

Code Quality

* The code must not be susceptible to errors, malicious or otherwise, that may potentially expose information or allow access to internal functions.

Encapsulation

* Data structures should be properly obfuscated so that they cannot be manipulated outside of expected functions.

## Manual Review

The code shows instances of redundant duplication (CRUD.java), a lack of encapsulation (customer.java) and error catching (CRUD.java, customer.java,DocData.java), and hardcoded sensitive information (DocData.java).

## Static Testing

Dependencies:

* bcprov-jdk15on-1.46.jar
  + The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms.
    - [**CVE-2013-1624**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1624)
    - **CVE-2015-6644** (OSSINDEX)
    - **CVE-2015-7940** (OSSINDEX)
    - [**CVE-2016-1000338**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000338)
    - [**CVE-2016-1000339**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000339)
    - [**CVE-2016-1000341**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000341)
    - [**CVE-2016-1000342**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000342)
    - [**CVE-2016-1000343**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000343)
    - [**CVE-2016-1000344**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000344)
    - [**CVE-2016-1000345**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000345)
    - [**CVE-2016-1000346**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000346)
    - [**CVE-2016-1000352**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000352)
    - [**CVE-2017-13098**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-13098)
    - [**CVE-2018-5382**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5382)
    - **CVE-2020-0187** (OSSINDEX)
    - **CVE-2020-26939** (OSSINDEX)
    - **CVE-2023-33201** (OSSINDEX)
* spring-boot-2.2.4.RELEASE.jar
  + Spring Boot
    - [**CVE-2022-27772**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27772)
    - [**CVE-2023-20873**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20873)
    - [**CVE-2023-20883**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20883)
* logback-core-1.2.3.jar
  + logback-core module
    - [**CVE-2021-42550**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42550)
    - [**CVE-2023-6378**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-6378)
* log4j-api-2.12.1.jar
  + The Apache Log4j API
    - [**CVE-2020-9488**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9488)
    - [**CVE-2021-44228**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-44228)
    - [**CVE-2021-44832**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-44832)
    - [**CVE-2021-45046**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-45046)
    - [**CVE-2021-45105**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-45105)
* snakeyaml-1.25.jar
  + YAML 1.1 parser and emitter for Java
    - [**CVE-2017-18640**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18640)
    - [**CVE-2021-4235**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4235)
    - [**CVE-2022-1471**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1471)
    - [**CVE-2022-25857**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-25857)
    - [**CVE-2022-3064**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-3064)
    - [**CVE-2022-38749**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38749)
    - [**CVE-2022-38750**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38750)
    - [**CVE-2022-38751**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38751)
    - [**CVE-2022-38752**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38752)
    - [**CVE-2022-41854**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-41854)
* jackson-databind-2.10.2.jar
  + General data-binding functionality for Jackson; works on core streaming API
    - [**CVE-2020-25649**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25649)
    - [**CVE-2020-36518**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-36518)
    - [**CVE-2021-46877**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-46877)
    - [**CVE-2022-42003**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-42003)
    - [**CVE-2022-42004**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-42004)
    - [**CVE-2023-35116**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-35116)
* tomcat-embed-core-9.0.30.jar
  + Core Tomcat implementation
    - [**CVE-2019-17569**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-17569)
    - [**CVE-2020-11996**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11996)
    - [**CVE-2020-13934**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13934)
    - [**CVE-2020-13935**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13935)
    - [**CVE-2020-13943**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13943)
    - [**CVE-2020-17527**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17527)
    - [**CVE-2020-1935**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1935)
    - [**CVE-2020-1938**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1938)
    - [**CVE-2020-8022**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8022)
    - [**CVE-2020-9484**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9484)
    - [**CVE-2021-24122**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24122)
    - [**CVE-2021-25122**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25122)
    - [**CVE-2021-25329**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25329)
    - [**CVE-2021-30640**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30640)
    - [**CVE-2021-33037**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33037)
    - [**CVE-2021-41079**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41079)
    - [**CVE-2021-43980**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43980)
    - [**CVE-2022-29885**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29885)
    - [**CVE-2022-34305**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-34305)
    - [**CVE-2022-42252**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-42252)
    - [**CVE-2023-28708**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-28708)
    - [**CVE-2023-41080**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-41080)
    - [**CVE-2023-42795**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-42795)
    - [**CVE-2023-44487**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-44487)
    - [**CVE-2023-45648**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-45648)
    - [**CVE-2023-46589**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-46589)
    - [**CVE-2024-21733**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-21733)
* hibernate-validator-6.0.18.Final.jar
  + Hibernate's Bean Validation (JSR-380) reference implementation.
    - [**CVE-2020-10693**](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-10693)
* spring-web-5.2.3.RELEASE.jar
  + Spring Web
    - **CVE-2016-1000027** (OSSINDEX)
    - **CVE-2020-5421** (OSSINDEX)
    - **CVE-2021-22096** (OSSINDEX)
    - **CVE-2021-22118** (OSSINDEX)
    - **CVE-2024-22243** (OSSINDEX)
* spring-beans-5.2.3.RELEASE.jar
  + Spring Beans
    - **CVE-2022-22965** (OSSINDEX)
* spring-webmvc-5.2.3.RELEASE.jar
  + Spring Web MVC
    - **CVE-2021-22060** (OSSINDEX)
* spring-context-5.2.3.RELEASE.jar
  + Spring Context
    - **CVE-2022-22968** (OSSINDEX)
* spring-expression-5.2.3.RELEASE.jar
  + Spring Expression Language (SpEL)
    - **CVE-2022-22950** (OSSINDEX)
    - **CVE-2023-20861** (OSSINDEX)
    - **CVE-2023-20863** (OSSINDEX)

## Mitigation Plan

Through review of the vulnerabilities identified in the dependency check, the most valuable action to take is simply to ensure that all of these services are updated to their latest versions. Nearly every vulnerability has been patched in newer versions or otherwise removed. The code itself should undergo review to ensure that it is conforming to best practices.