****

# 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** | **07/15/23** | **Cassidy Kemmerer** |  |

## 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

Cassidy Kemmerer

## Interpreting Client Needs

Artemis Financial is a financial institution that deals with financial transactions and having this information secure has the utmost importance for the organization. Having the client’s information secure and their transactions being secure is this company’s top priority. Artemis Financial data should be safe and secure not only while the information is being stored but also while this information is in transit. To keep the information secure, we should be proactive for cases of any kind of intrusions and should be detecting early signs of the intrusions while logging the signs. When looking at how the information needs to be secure, there are government restrictions that deal with encryption. The information being encrypted will mean that only users that have be granted access to the information are able to access it and this will help prevent unauthorized users from accessing information that they should not be. Through researching, it appears that 3D protocol is a common way that agencies have a secure way to conduct transactions to keep all parties protected. There are regulations that state that certain types of financial information can be stored on the system and certain information be transferred over a network, this is regulated by PCI-DSS. Also, the Gramm-Leach-Bliley Act requires that financial institutions that are conducting any financial transactions to inform their clients on any information sharing practices along with safeguarding sensitive data.

There are some common threats that can seriously harm the organization. These threats to the organization would include hacking and phishing. If the company were to be hacked this can pose a threat to the entire organization’s reputation, along with client and employee sensitive data being exposed. The financial records could become destroyed or altered due to a hacking incident. The other security threat phishing can be just as damaging as a hacking incident. A phishing incident works on tricking a user into giving someone unauthorized access. Implementing more security measures can help keep more of the company’s information secure.

## Areas of Security

API- Having authentication and verification are crucial to keep access confined to select individuals who have been granted access to sensitive information. There are ways to have authentication which are through password validation and 2-way authentication.

Input Validation – The input needs to be validated to ensure that the input received is validated to ensure that it does not contain any harmful information to trick the output and cause the application to crash.

Cryptography – Financial information is being dealt with therefore all sensitive information needs to be coded and de-coded to ensure that if the information becomes comprised that it is not easy to be deciphered.

## Manual Review

When inspecting the code there is not any code that appears to be out of the ordinary. There is the REST, along with no test values, test cases, entry criteria, and exit criteria. When examining there is one thing that was noticeable which is that the 2.2.4 spring maven plugin should be upgraded to version 2.4.0.

## Static Testing

* Dependency: bcprov-jdk15on-1.46.jar
  + Vulnerability:
    - CVE-2013-1624 & CVE-2016-1000341 : The TLS implementation in the Bouncy Castle Java library before 1.48 along with the C# library before 1.8 and does not properly consider timing the side channel attacks on a noncompliant MAC. It is recommended to upgrade to version 1.5 or 1.7.
    - CVE-2015-6644 : This vulnerability allows for the local manipulation in the code to be able to get access to the confidential data and poses as a major threat. It is recommended that Bouncy Castle is upgraded in Android to 5.1.1.
* Dependency: Log4j.api.2.12.1.jar
  + Vulnerability:
    - CVE-2020-9488 : This is a vulnerability due to there being a new version available and this poses a low severity. It is recommended that is needs to be upgraded to log4j2.
* Dependency: snakeyaml-1.25.jar
  + Vulnerability:
    - CVE-2017-18640 : This vulnerability is high and this is due to the occurrence of a set of untrust data that is parsed and the denial of service code is the output. It is recommended that there should be using a filter and that there needs to be an implementation of load configurations in the code.
* Dependency: tomcat-embed-core-9.0.30.jar
  + Vulnerability:
    - CVE-2019-17569 : This vulnerability affects Tomcats Apache versions 9.0.28 to 9.0.30 and 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 and this is a medium severity. The solution to resolve the vulnerability is to upgrade to tomcat 9.0.31.
    - CVE-2020-10934 : This vulnerability has a high severity because if a number of requests are made a denial of service outcome can occur. The solution would be to download YaST online\_update
    - CVE-2020-8022 : This has a medium severity because there is incorrect default permissions that is within the packaging of tomcat. The solution would be to upgrade to tomcat 9.0.35.
* Dependency: spring-core-5.2.3.RELEASE.jat
  + Vulnerability:
    - CVE-2020-5421: This vulnerability leaves it to be susceptible to RFD attacks and can result in the vulnerability to range from medium to high. The solution would be to upgrade springframe.

## Mitigation Plan

After looking over the vulnerabilities, it appears that there are a few vulnerabilities that stem from the usage of outdated plugins. The security risks are going to target the outdated plugins and exploit those. The developer has the responsibility to ensure that any of the dependencies do not have any negative impact on the quality of the code. Along with identifying the vulnerabilities above, there are some solutions listed on how to resolve the vulnerability. Through the static testing, it became apparent of what the vulnerabilities were and with some research appropriated recommendations were given based on the posed vulnerabilities.