****

# 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** | **5/18/2023** | **Steve Smith** |  |

## 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

Steve Smith

## Interpreting Client Needs

Having secure communication will be a high value to Artemis Financial’ s software application. By using secure communication, the data will be protected from being compromised and minimize the risk of a data breach. Security is of high importance with the sensitive data transferred through transactions globally. The transactions should be protected with a synchronizer token. There are some government restrictions that need to be followed. We need to be following the 1974 Privacy Act, the Electronic Communication Privacy Act, Computer Fraud and Abuse Act, and Cyber Intelligence Sharing and Protection Act.

## Areas of Security

The application will need input validation. The input validation will authenticate and authorize the control access for the type of user. The Financial Officers, Administrators, and Customers have different levels of permissions. The software will be using RESTful and will need API. The RESTful API will be needed to exchange information securely over the internet. Code quality will be needed for secure coding to be implemented to prevent outside interference to manipulate the code in a unsecure manner. Cryptography will be needed to encrypt account numbers, routing numbers, credit card numbers, and social security numbers.

## Manual Review

* Does not have HTTP which is needed for security over the internet
* No input verification for authentication
* No cryptography for the accounts

## Static Testing

bcprov-jdk15on-1.46.jar – several vulnerabilities on 1.46, update to latest version.

oCVE-2013-1624

oCVE-2015-6644

oCVE-2015-7940

oCVE-2016-1000338

oCVE-2016-1000339

oCVE-2016-1000341

oCVE-2016-1000342

oCVE-2016-1000343

oCVE-2016-1000344

oCVE-2016-1000345

oCVE-2016-1000346

oCVE-2016-1000352

oCVE-2017-13098

oCVE-2018-1000613

oCVE-2018-5382

bcprov-jdk15on-1.46.jar – several vulnerabilities on 1.46, update to latest version.

oCVE-2013-1624

oCVE-2015-6644

oCVE-2015-7940

oCVE-2016-1000338

oCVE-2016-1000339

oCVE-2016-1000341

oCVE-2016-1000342

oCVE-2016-1000343

oCVE-2016-1000344

oCVE-2016-1000345

oCVE-2016-1000346

oCVE-2016-1000352

oCVE-2017-13098

oCVE-2018-1000613

oCVE-2018-5382

bcprov-jdk15on-1.46.jar – several vulnerabilities on 1.46, update to latest version.

oCVE-2013-1624

oCVE-2015-6644

oCVE-2015-7940

oCVE-2016-1000338

oCVE-2016-1000339

oCVE-2016-1000341

oCVE-2016-1000342

oCVE-2016-1000343

oCVE-2016-1000344

oCVE-2016-1000345

oCVE-2016-1000346

oCVE-2016-1000352

oCVE-2017-13098

oCVE-2018-1000613

oCVE-2018-5382

Log4j-api-2.12.2.jar = This has one vulnerability, and the solution would be to update it

to the most recent update 2.13.2

•Bcprov-jdk15on-1.46.jar= A LOT of vulnerabilities, the solution would be to update to

1.60

•Snakeyaml-1.25.jar = one vulnerability, solution is to update to latest system.

•Tomcat-embed-core-9.0.30.jar = Three vulnerabilities, update to Apache Tomcat 10.0.6

•Jackson-databind-2.10.2.jar= One vulnerability, solution is to update to current version.

•Spring-aop-5.2.3.RELEASE.jar= Four vulnerabilities, solution is to update to current

version.

•Hibernate-validator-6.0.18.final.jar= One vulnerability, solution is to update to 6.0.20

## Mitigation Plan

* Implementation of HTTP for internet security.
* Implementation of input verification to authenticate users.
* Implementation of cryptography to encrypt sensitive account data.