****

# 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** | **September 15, 2022** | **Juan Pablo Izquierdo** | **Initial assessment** |

## Client



## Developer

Juan Pablo Izquierdo

## Interpreting Client Needs

*What is the value of secure communications to the company?*

Global Rain’s mission states that “Security is everyone’s responsibility”. Therefore, the implementation of a secure RESTful web application must be accomplished in close partnership with Artemis Financial to protect the organization and its clients.

*Does the company make any international transactions?*

Yes, Global Rain specializes in secure software utilized by entrepreneurs, businesses, and governments around the world. A web application is vulnerable to attacks from international sources and precautions must be taken to mitigate any breaches, locally or internationally.

*Are there governmental restrictions about secure communications to consider?*

Yes, client’s personal information and records of financial transactions must be kept secure in accordance with the law. For example, personal identifiable information must be secured, or hefty fines can be incurred.

*What external threats might be present now and in the immediate future?*

Denial of service (DoS), injection, improper input validation, man in the middle, are just some of the potential threats that are commonly used to exploit vulnerabilities in unsecure software today.

What are the modernization requirements that you must consider?

Open-source libraries are a great option for software developers because they are continuously improving and reviewed by many developers, and operating costs are much lower than the alternatives. However, open-source libraries are still vulnerable to logic, syntax errors, and new threats that evolve to bypass mitigation techniques.

## Areas of Security

Input validation and APIs:

Dependencies are indispensable tools that facilitate the creation and maintenance of software applications. However, they are also a major vulnerability because these source libraries are utilized without the need for in-depth knowledge of the code within them. It is our job to perform a vulnerability assessment and static tests of known threats, and manually analyze the application for any other unknown threats as well.

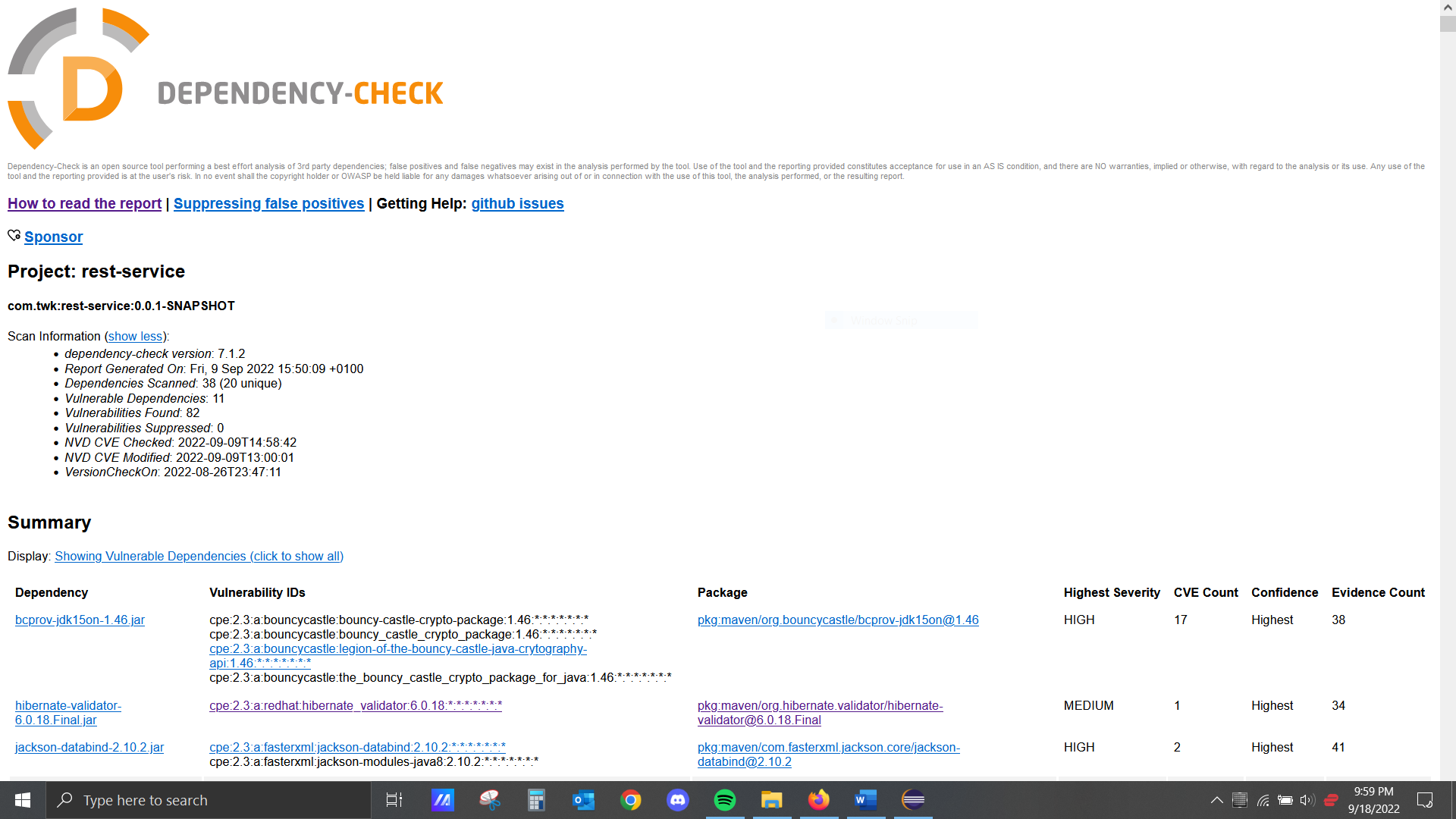
Cryptography and client/server:

The interaction between clients and servers must be secured, specially because of the sensitive nature of the financial information being transmitted.

## Manual Review

The versions of Maven and Spring Framework in the pom file are accessing outdated versions. These versions must be updated to patch known security threats.

## Static Testing



Graphical user interface, text, application, email

Description automatically generated

## Mitigation Plan

The primary defense against threats is to have the most up to date definitions and versions of software being utilized. Many of the vulnerabilities have been found and resolved in the latest iterations of Spring and Maven. Therefore, the best way to mitigate security vulnerabilities is to update.

Additionally, there are other threats that must be addressed individually such as configuration errors and injection prevention by parameterization.

The static test revealed many vulnerabilities but the most severe and their descriptions are depicted below:

