****

# 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)-12

[5. Mitigation Plan 12](#_Toc32574615)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **March 19, 2023** | **Wesston Reed McCollum** |  |

## 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

Wesston Reed Mccollum

## Interpreting Client Needs

The client Artemis Financial is seeking to improve their current RESTful API with new security software. The client deals with very sensitive information on financial plans, so security in information is top priority. This idea is enforced by local and international regulations on this variety of software. There are and always will be numerous persons trying to gain sensitive information that must be denied. This challenge is made harder by the total access to open-source libraries for deconstruction and reverse engineering and ever-evolving web technologies to keep up with and counteract.

## Areas of Security

1. Input Validation: This API needs to ensure that there is no SQL injection happening to prevent intermediary control or DDOS attacks.
2. Secure API Interactions: Ensure that the API is not capable of accessing information outside of its set scope.
3. Cryptography: With such highly sensitive information, it is vital to encrypt as much data as can be reasonably done.
4. Client/Server: Ensure that any connection to a client from a server is secure and that no intermediaries are interacting with the connection whatsoever.

## Manual Review

The code has little to no input validation. It is imperative that any input be validated to prevent injections. There are some minor authentications for the API, but little to no authorization practices. All entries in the code are held with no encryption at all. Also, there is no validation for connections between clients and servers.

## Static Testing

1. Bouncy Castle (bcprov-jdk15on-1.46.jar)

A1. Vulnerability Codes:

1. CVE-2013-1624

CVSSv2: Base Score: MEDIUM (4.0)

Vector: /AV:N/AC:H/Au:N/C:P/I:P/A:N

1. CVE-2015-6644 (OSSINDEX)

CVSSv3: Base Score: LOW (3.3)

Vector: /AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

1. CVE-2015-7940 (OSSINDEX)

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

1. CVE-2016-1000338

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

1. CVE-2016-1000339

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: MEDIUM (5.3)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

1. CVE-2016-1000341

CVSSv2: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: MEDIUM (5.9)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

1. CVE-2016-1000342

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

1. CVE-2016-1000343

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

1. CVE-2016-1000344

CVSSv2: Base Score: MEDIUM (5.8)

Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: HIGH (7.4)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

1. CVE-2016-1000345

CVSSv2: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: MEDIUM (5.9)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

1. CVE-2016-1000346

CVSSv2: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: LOW (3.7)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

1. CVE-2016-1000352

CVSSv2: Base Score: MEDIUM (5.8)

Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: HIGH (7.4)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

1. CVE-2017-13098

CVSSv2: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: MEDIUM (5.9)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

1. CVE-2018-5382

CVSSv2: Base Score: LOW (3.6)

Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: MEDIUM (4.4)

Vector: /AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

1. CVE-2020-0187 (OSSINDEX)

CVSSv2: Base Score: MEDIUM (5.5)

Vector: /AV:L/AC:L/Au:/C:H/I:N/A:N

1. CVE-2020-26939 (OSSINDEX)

CVSSv2: Base Score: MEDIUM (5.3)

Vector: /AV:N/AC:L/Au:/C:L/I:N/A:N

A2. This version of Bouncy Castle was vulnerable to crafted applications, invalid curve attacks, distinguishing and plaintext-recovery attacks through timing data of packet creation, information leaks, signature timing attacks, signature validation, use of weak default private keys, use of ECB mode, padding oracle attacks, unvalidated DH public keys, a weak Bleichenbacher oracle, low integrity BKS keystore, potential for incorrect cryptographic algorithm from an incomplete comparison, and invalid ciphertext attacks.

1. Spring Boot (spring-boot-2.2.4.RELEASE.jar

B1. Vulnerability Codes:

1. CVE-2022-27772

CVSSv2: Base Score: MEDIUM (4.6)

Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

CVSSv3: Base Score: HIGH (7.8)

Vector: /AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

B2. This version of Spring Boot was vulnerable to temporary directory hijacking.

1. Logback-Core Module (logback-core-1.2.3.jar)

C1. Vulnerability Codes

1. CVE-2021-42550

CVSSv2: Base Score: HIGH (8.5)

Vector: /AV:N/AC:M/Au:S/C:C/I:C/A:C

CVSSv3: Base Score: MEDIUM (6.6)

Vector: /AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

C2. Attackers were able to craft malicious configurations given the required privileges.

1. Apache Log4j API ( log4j-api-2.12.1.jar)

D1. Vulnerability Codes

1. CVE-2020-9488

CVSSv2: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: LOW (3.7)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

1. CVE-2021-44228

CVSSv2: Base Score: HIGH (9.3)

Vector: /AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSSv3: Base Score: CRITICAL (10.0)

Vector: /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

1. CVE-2021-44832

CVSSv2: Base Score: HIGH (8.5)

Vector: /AV:N/AC:M/Au:S/C:C/I:C/A:C

CVSSv3: Base Score: MEDIUM (6.6)

Vector: /AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

1. CVE-2021-45046

CVSSv2: Base Score: MEDIUM (5.1)

Vector: /AV:N/AC:H/Au:N/C:P/I:P/A:P

CVSSv3: Base Score: CRITICAL (9.0)

Vector: /AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

1. CVE-2021-45105

CVSSv2: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSSv3: Base Score: MEDIUM (5.9)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

D2. Apache Log4j was susceptible to man-in-the-middle attacks, deserialization of untrusted data, uncontrolled resource consumption, and uncontrolled recursion.

1. YAML 1.1 (snakeyaml-1.25.jar)

E1. Vulnerability Codes

1. CVE-2017-18640

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1. CVE-2021-4235

CVSSv3: Base Score: MEDIUM (5.5)

Vector: /AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

1. CVE-2022-1471 (OSSINDEX)

CVSSv2: Base Score: HIGH (9.8)

Vector: /AV:N/AC:L/Au:/C:H/I:H/A:H

1. CVE-2022-25857

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1. CVE-2022-3064

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1. CVE-2022-38749

CVSSv3: Base Score: MEDIUM (6.5)

Vector: /AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

1. CVE-2022-38750

CVSSv3: Base Score: MEDIUM (5.5)

Vector: /AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

1. CVE-2022-38751

CVSSv3: Base Score: MEDIUM (6.5)

Vector: /AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

1. CVE-2022-38752

CVSSv3: Base Score: MEDIUM (6.5)

Vector: /AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

1. CVE-2022-41854

CVSSv3: Base Score: MEDIUM (6.5)

Vector: /AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

E2. YAML1.1 was susceptible to XML entity expansion, lack of input validation, deserialization of untrusted data, resource exhaustion, and out-of-bounds writing.

1. Jackson Databinding (jackson-databind-2.10.2.jar)

F1. Vulnerability codes

1. CVE-2020-25649

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

1. CVE-2020-36518

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1. CVE-2022-42003

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1. CVE-2022-42004

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

F2. Jackson data binding was vulnerable to improper restriction of XXE, out-of-bounds writing, and deserialization of untrusted data.

1. Core Tomcat (tomcat-embed-core-9.0.30.jar)

G1. Vulnerability Codes

1. CVE-2019-17569

CVSSv2: Base Score: MEDIUM (5.8)

Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: MEDIUM (4.8)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

1. CVE-2020-11996

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1. CVE-2020-13934

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1. CVE-2020-13935

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1. CVE-2020-13943

CVSSv2: Base Score: MEDIUM (4.0)

Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:N

CVSSv3: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

1. CVE-2020-17527

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

1. CVE-2020-1935

CVSSv2: Base Score: MEDIUM (5.8)

Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: MEDIUM (4.8)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

1. CVE-2020-1938

CVSSv2: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3: Base Score: CRITICAL (9.8)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

1. CVE-2020-8022

CVSSv2: Base Score: HIGH (7.2)

Vector: /AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSSv3: Base Score: HIGH (7.8)

Vector: /AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

1. CVE-2020-9484

CVSSv2: Base Score: MEDIUM (4.4)

Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

CVSSv3: Base Score: HIGH (7.0)

Vector: /AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

1. CVE-2021-24122

CVSSv2: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: MEDIUM (5.9)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

1. CVE-2021-25122

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

1. CVE-2021-25329

CVSSv2: Base Score: MEDIUM (4.4)

Vector: /AV:L/AC:M/Au:N/C:P/I:P/A:P

CVSSv3: Base Score: HIGH (7.0)

Vector: /AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

1. CVE-2021-30640

CVSSv2: Base Score: MEDIUM (5.8)

Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3: Base Score: MEDIUM (6.5)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N

1. CVE-2021-33037

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSSv3: Base Score: MEDIUM (5.3)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

1. CVE-2021-41079

CVSSv2: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1. CVE-2021-43980

CVSSv3: Base Score: LOW (3.7)

Vector: /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

1. CVE-2022-29885

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1. CVE-2022-34305

CVSSv2: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:N

CVSSv3: Base Score: MEDIUM (6.1)

Vector: /AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

1. CVE-2022-42252

CVSSv3: Base Score: HIGH (7.5)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

G2. Core Tomcat was vulnerable to HTTP request smuggling, memory leaks, NULL pointer dereferences, infinite loops, information exposures, incorrect default permissions, deserialization of untrusted data, use of incorrectly resolved name or reference, improper encoding or escaping of output, race conditions, resource exhaustion, and cross-site scripting.

1. Hibernate’s Bean Validation (hibernate-validator-6.0.18.Final.jar)

H1. Vulnerability Codes

1. CVE-2020-10693

CVSSv2: Base Score: MEDIUM (5.0)

Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSSv3: Base Score: MEDIUM (5.3)

Vector: /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

H2. Hibernate’s Bean Validation was vulnerable to improper input validation.

1. Spring Web (spring-web-5.2.3.RELEASE.jar

I1. Vulnerability Codes

1. CVE-2016-1000027 (OSSINDEX)

CVSSv2: Base Score: HIGH (9.8)

Vector: /AV:N/AC:L/Au:/C:H/I:H/A:H

1. CVE-2020-5421 (OSSINDEX)

CVSSv2: Base Score: MEDIUM (6.5)

Vector: /AV:N/AC:H/Au:/C:L/I:H/A:N

1. CVE-2021-22096 (OSSINDEX)

CVSSv2: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:L/Au:/C:N/I:L/A:N

1. CVE-2021-22118 (OSSINDEX)

CVSSv2: Base Score: HIGH (7.8)

Vector: /AV:L/AC:L/Au:/C:H/I:H/A:H

I2. Spring Web was vulnerable to deserialization of untrusted data, improper output neutralization for logs, and exposure of resources to wrong spheres.

1. Spring Beans (spring-beans-5.2.3.RELEASE.jar)

J1. Vulnerability Codes

1. CVE-2022-22965 (OSSINDEX)

CVSSv2: Base Score: HIGH (9.8)

Vector: /AV:N/AC:L/Au:/C:H/I:H/A:H

J2. Spring Beans was vulnerable to code injection.

1. Spring Web MVC (spring-webmvc-5.2.3.RELEASE.jar)

K1. Vulnerability Codes

1. CVE-2021-22060 (OSSINDEX)

CVSSv2: Base Score: MEDIUM (4.3)

Vector: /AV:N/AC:L/Au:/C:N/I:L/A:N

K2. Spring Web MVC was vulnerable to improper neutralization for logs.

1. Spring Context (spring-context-5.2.3.RELEASE.jar)

L1. Vulnerability Codes

1. CVE-2022-22968 (OSSINDEX)

CVSSv2: Base Score: MEDIUM (5.3)

Vector: /AV:N/AC:L/Au:/C:N/I:L/A:N

L2. Spring Context was vulnerable to improper handling of case sensitivity.

1. Spring Expression Language (spring-expression-5.2.3.RELEASE.jar)

M1. Vulnerability Codes

1. CVE-2022-22950 (OSSINDEX)

CVSSv2: Base Score: MEDIUM (6.5)

Vector: /AV:N/AC:L/Au:/C:N/I:N/A:H

M2. Spring Expression Language was vulnerable to throttling.

## Mitigation Plan

The largest part of the mitigation plan would be to use more up-to-date APIs and validate inputs. Most vulnerabilities listed fall under these two categories. Also, server-to-client authentication and authorization will need to be instated to a much higher degree as deserialized data from an untrusted user was very common. With just these three changes a large portion of vulnerabilities can be nullified. The next step would be to encrypt data such as user information and keys so that it cannot be taken from logs and intermediary services.