****

# 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** | **3/18/2024** | **Daniel Schmidt** |  |

## 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

Daniel Schmidt

## Interpreting Client Needs

Artemis Financial is a consulting company that wants to modernize their web application operations. They are seeking out our company to help protect their organization from any external threats.

## Areas of Security

API: Runs internally and externally. This allows certain data to be acceptable and not acceptable.

Input Validation: Provides protection for the client’s users.

Cryptography: This will ensure that the user’s information will not be exposed to anyone else.

## Static Testing

|  |  |  |  |
| --- | --- | --- | --- |
| Dependency | Vulnerability IDs | Package | Summary |
| logback-core-1.2.3.jar | cpe:2.3:a:qos:logback:1.2.3:\*:\*:\*:\*:\*:\*:\* | pkg:maven/ch.qos.logback/logback-core@1.2.3 | A serialization vulnerability in log back receiver component part of log back version 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending poisoned data. |
| jackson-databind-2.10.2.jar | cpe:2.3:a:fasterxml:jackson-databind:2.10.2:\*:\*:\*:\*:\*:\*:\* | pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2 | jackson-databind through 2.15.2 allows attackers to cause a denial of service or other unspecified impact via a crafted object that uses cyclic dependencies. NOTE: the vendor's perspective is that this is not a valid vulnerability report, because the steps of constructing a cyclic data structure and trying to serialize it cannot be achieved by an external attacker. |
| log4j-api-2.12.1.jar | cpe:2.3:a:apache:log4j:2.12.1:\*:\*:\*:\*:\*:\*:\* | pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1 | Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2. |
| tomcat-embed-core-9.0.30.jar | cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\* | pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30 | Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue |
| tomcat-embed-websocket-9.0.30.jar | cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\* | pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30 | Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue. |
| hibernate-validator-6.0.18.Final.jar | cpe:2.3:a:redhat:hibernate\_validator:6.0.18:\*:\*:\*:\*:\*:\*:\* | pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final | A flaw was found in Hibernate Validator version 6.1.2. Final. A bug in the message interpolation processor enables invalid EL expressions to be evaluated as if they were valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages. |
| mongo-java-driver-2.4.jar | cpe:2.3:a:mongodb:java\_driver:2.4:\*:\*:\*:\*:\*:\*:\* | pkg:maven/org.mongodb/mongo-java-driver@2.4 | none |

## Mitigation Plan

After reviewing the summaries of each dependency and reviewing the vulnerabilities, it is safe to say that the main simple solution to clear any errors would be to use the latest updated versions available.