****

# Artemis Financial Vulnerability Assessment Report

Table of Contents

[Artemis Financial Vulnerability Assessment Report 1](#_Toc126455093)

[Document Revision History 3](#_Toc126455094)

[Client 3](#_Toc126455095)

[Developer 3](#_Toc126455096)

[Interpreting Client Needs 3](#_Toc126455097)

[Areas of Security 4](#_Toc126455098)

[Manual Review 4](#_Toc126455099)

[Static Testing 5](#_Toc126455100)

[Mitigation Plan 9](#_Toc126455101)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **02/04/2023** | **Michael Reynolds** |  |

## Client



## Developer

Michael Reynolds

## Interpreting Client Needs

The client values their security/secure communications. Wanting to modernize their operation as much as possible, to provide current and effective software security. The client also works in the Financial sector, where money is directly involved and impacted by the security of the software.

There is no evidence nor was it made clear that the client makes international contracts, **It’s crucial we find this out from the client**.

There are governmental restrictions/regulations that must be considered for secure communications, especially when working with financial institutions and their applications. Consider the following regulations:

* Payment Card Industry Data Security Standard (PCI DSS).
* California Consumer Privacy Act (CCPA)
* New York Department of Financial Services (NYDFS)
* Federal Financial Institutions Examination Council (FFIEC)

And for example one that may apply overseas:

* European Union’s General Data Protection Regulation (GDPR)

It’s important to also consider some of the immediate threats our client may deal with after expanding to a digital front. “Phishing Scams” will pose a threat especially if the majority of employees/end-users are susceptible to them, and their user access is not reduced to only what is necessary.

Secure channels of communication and user authentication handling can prevent methods of “Social Engineering”. Creating secure methods of password reset and individual authentication such as 2FA will ensure our client doesn’t find themselves compromising their end-users.

“SQL Injection” and “Man-in-the-middle” attacks are rampant and there are common practice methods for mitigation from our end. Applying certain open-source libraries may help us with ensuring we are up to date and utilizing industry standards, these prove to be very secure methods as they are frequented by developers and industries alike to ensure best practices and secure standards.

## Areas of Security

The following areas of security are paramount with Financial Advising tech:

* Input Validation
* APIs
* Cryptography
* Code Error
* Code Quality
* Secure Data Structures

We’ve excluded “Secure Distributed Computing” as distributed computing will not be required for the financial advising tool we’ll make for our client. Input validation will ensure that the end-user is sending trusted input and will allow them to provide more accurate or errorless input to provide for financial analysis. These inputs will then be sending confidential financial information through the existing APIs, which will need to be encrypted to prevent data breaches on the wire. Code Error handling must be done securely to ensure that nothing could potentially expose the end-users data or lack thereof. Code Quality will ensure the application has best practices for handling financial analysis, accuracy is important when working with financial advising. Secure data structures will be storing client information on the server, so we’ll have to consider that.

## Manual Review

CRUDController.java uses Strings directly from the params of “/read” and “/greeting” endpoints without validating input or parsing for code injection.

Our API endpoints don’t use any form of encryption except SSL.

The connection strings for their mySQL database connection are kept in plain text within the script itself and not accessed via config files.

Error handling on the DocData.java read document method just prints the error stack trace, which applies to our API endpoints as well.

Accessors are not secure or inaccessible in our DocData, Customer, and myDateTime data structures.

## Static Testing

Text

Description automatically generated

| Dependency | Severity |  |
| --- | --- | --- |
| [bcprov-jdk15on-1.46.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l2_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) | HIGH | CVE-2013-1624  https://nvd.nist.gov/vuln/detail/CVE-2013-1624  CWE-310REDHAT - RHSA-2014:0371REDHAT - RHSA-2014:0372SECUNIA - 57716SECUNIA - 57719  CWE-200: Information Exposure  CWE-347: Improper Verification of Cryptographic SignatureREDHAT - RHSA-2018:2669REDHAT - RHSA-2018:2927UBUNTU - USN-3727-1  CWE-361REDHAT - RHSA-2018:2669REDHAT - RHSA-2018:2927UBUNTU - USN-3727-1  CWE-347: Improper Verification of Cryptographic SignatureREDHAT - RHSA-2018:2669REDHAT - RHSA-2018:2927UBUNTU - USN-3727-1  CWE-310REDHAT - RHSA-2018:2669REDHAT - RHSA-2018:2927UBUNTU - USN-3727-1  CWE-361REDHAT - RHSA-2018:2669REDHAT - RHSA-2018:2927UBUNTU - USN-3727-1  CWE-320REDHAT - RHSA-2018:2669REDHAT - RHSA-2018:2927UBUNTU - USN-3727-1  CWE-354: Improper Validation of Integrity Check ValueREDHAT - RHSA-2018:2927  CWE-310  CWE-203: Information Exposure Through Discrepancy  Patch: No Patch Available |
| [spring-boot-2.2.4.RELEASE.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l3_225a4fd31156c254e3bb92adb42ee8c6de812714) | HIGH | CVE-2022-27772  https://nvd.nist.gov/vuln/detail/CVE-2022-27772  CWE-668: Exposure of Resource to Wrong Sphere    Patch: https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85 |
| [logback-core-1.2.3.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l4_864344400c3d4d92dfeb0a305dc87d953677c03c) | MEDIUM | CVE-2021-42550  https://nvd.nist.gov/vuln/detail/CVE-2021-42550  CWE-502: Deserialization of Untrusted DataOSSINDEX - [sonatype-2021-4517] CWE-502: Deserialization of Untrusted Data    Patch: https://jira.qos.ch/browse/LOGBACK-1591 |
| [log4j-api-2.12.1.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l5_a55e6d987f50a515c9260b0451b4fa217dc539cb) | CRITICAL | CVE-2020-9488  https://nvd.nist.gov/vuln/detail/CVE-2020-9488  Patch: https://issues.apache.org/jira/browse/LOG4J2-2819 |
| [snakeyaml-1.25.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l8_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) | HIGH | CVE-2017-18640  https://nvd.nist.gov/vuln/detail/CVE-2017-18640  CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')  CWE-502: Deserialization of Untrusted Data  CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')  CWE-787: Out-of-bounds Write    Patch: https://bitbucket.org/asomov/snakeyaml/issues/377/allow-configuration-for-preventing-billion |
| [jackson-databind-2.10.2.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l9_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) | HIGH | CVE-2020-25649  https://nvd.nist.gov/vuln/detail/CVE-2020-25649  CWE-611: Improper Restriction of XML External Entity Reference ('XXE')  CWE-787: Out-of-bounds Write  CWE-502: Deserialization of Untrusted Data    Patch: https://github.com/FasterXML/jackson-databind/issues/2589 |
| [tomcat-embed-core-9.0.30.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l13_ad32909314fe2ba02cec036434c0addd19bcc580) | CRITICAL | CVE-2019-17569  https://nvd.nist.gov/vuln/detail/CVE-2019-17569    Patch: https://www.oracle.com/security-alerts/cpujan2021.html |
| [hibernate-validator-6.0.18.Final.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l16_7fd00bcd87e14b6ba66279282ef15efa30dd2492) | MEDIUM | CVE-2020-10693  https://nvd.nist.gov/vuln/detail/CVE-2020-10693  CWE-20: Improper Input Validation    Patch: https://lists.apache.org/thread.html/rb8dca19a4e52b60dab0ab21e2ff9968d78f4b84e4033824db1dd24b4@%3Cpluto-scm.portals.apache.org%3E |
| [spring-web-5.2.3.RELEASE.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l19_dd386a02e40b915ab400a3bf9f586d2dc4c0852c) | HIGH | CVE-2016-1000027  https://nvd.nist.gov/vuln/detail/CVE-2016-1000027  CWE-502: Deserialization of Untrusted Data  CWE-noinfo  CWE-117: Improper Output Neutralization for Logs  CWE-668: Exposure of Resource to Wrong Sphere    Patch: No Patch Available |
| [spring-beans-5.2.3.RELEASE.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l20_0250c8c641433dc06b1b44e4563fa08a2fbf8954) | HIGH | CVE-2022-22965  https://nvd.nist.gov/vuln/detail/CVE-2022-22965  CWE-94: Improper Control of Generation of Code ('Code Injection')OSSINDEX - [sonatype-2022-1764] CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')    Patch: No Patch Available |
| [spring-webmvc-5.2.3.RELEASE.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l21_745a62502023d2496b565b7fe102bb1ee229d6b7) | MEDIUM | CVE-2021-22060  https://nvd.nist.gov/vuln/detail/CVE-2021-22060  CWE-117: Improper Output Neutralization for Logs    Patch: No Patch Available |
| [spring-context-5.2.3.RELEASE.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l22_7750c95c96c7a1885c8b1b503ba915bc33ca579a) | MEDIUM | CVE-2022-22968  https://nvd.nist.gov/vuln/detail/CVE-2022-22968  CWE-178: Improper Handling of Case Sensitivity    Patch: No Patch Available |
| [spring-expression-5.2.3.RELEASE.jar](file:///C:\Users\kmedr\OneDrive\Desktop\School\2023\CS-305%20Software%20Security\Projects\Project%20One\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l23_d0c6bb10758805b2153c589686b8045554bfac2d) | MEDIUM | CVE-2022-22950  https://nvd.nist.gov/vuln/detail/CVE-2022-22950  CWE-770: Allocation of Resources Without Limits or Throttling    Patch: No Patch Available |

## Mitigation Plan

https://nvd.nist.gov/vuln/detail/CVE-2022-27772

Patch: <https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85>

A screenshot of a computer

Description automatically generated

Text

Description automatically generated

Fix: Update to LTS.

https://nvd.nist.gov/vuln/detail/CVE-2021-42550

Patch: <https://jira.qos.ch/browse/LOGBACK-1591>

A picture containing application

Description automatically generated



Fix: Update to LTS.

https://nvd.nist.gov/vuln/detail/CVE-2020-9488

Patch: <https://issues.apache.org/jira/browse/LOG4J2-2819>

Graphical user interface, text, application

Description automatically generated

Fix: Update to LTS.

https://nvd.nist.gov/vuln/detail/CVE-2017-18640

Patch: <https://bitbucket.org/asomov/snakeyaml/issues/377/allow-configuration-for-preventing-billion>

Graphical user interface, text

Description automatically generated

Path Inaccessible, assuming Update to LTS.

https://nvd.nist.gov/vuln/detail/CVE-2020-25649

Patch: <https://github.com/FasterXML/jackson-databind/issues/2589>

A screenshot of a computer

Description automatically generated with medium confidence

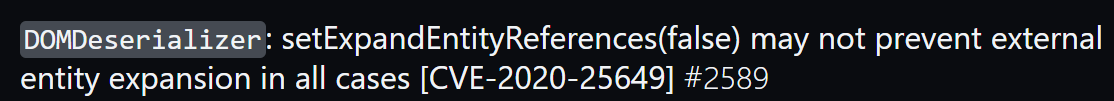
Text

Description automatically generated

Fix: Update to LTS.

https://nvd.nist.gov/vuln/detail/CVE-2019-17569

Patch: <https://www.oracle.com/security-alerts/cpujan2021.html>



Text

Description automatically generated

Fix: Update to LTS.

https://nvd.nist.gov/vuln/detail/CVE-2020-10693

Patch: <https://lists.apache.org/thread.html/rb8dca19a4e52b60dab0ab21e2ff9968d78f4b84e4033824db1dd24b4@%3Cpluto-scm.portals.apache.org%3E>



Graphical user interface, text, application

Description automatically generated

Fix: Update to LTS.