****

# CS 305 Project One

**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** | **22 May 2022** | **Chris Cole** |  |

## Client



## Instructions

Deliver this completed vulnerability assessment report, identifying your findings of security vulnerabilities and articulating recommendations for next steps to remedy the issues you have found.

Respond to the five steps outlined below and include your findings. Replace the bracketed text on all pages with your own words. If you choose to include images or supporting materials, be sure to insert them throughout.

## Developer

Chris Cole

## 1. Interpreting Client Needs

Determine your client’s needs and potential threats and attacks associated with their application and software security requirements. Consider the following regarding how companies protect against external threats based on the scenario information:

* What is the value of secure communications to the company?
* Are there any international transactions that the company produces?
* Are there governmental restrictions about secure communications to consider?
* What external threats might be present now and in the immediate future?
* What are the “modernization” requirements that must be considered, such as the role of open source libraries and evolving web application technologies?

Secure communications are very important for any financial institution. Sensitive data is stored in company databases and can be transmitted from server to client and vice versa. Due to the nature of the business, it is expected that clients may travel or live abroad and expect normal access to their accounts. While the United States does not have federal oversight on secure communications, many US states and foreign governments do have laws and guidelines we must consider. Financial institutions are a popular target for ransomware and attacks on cloud servers. Artemis Financial should consider the importance of keeping software updated and secure while implementing industry standard practices of encryption and staying on top of new innovations in open source libraries.

## 2. Areas of Security

Referring to the Vulnerability Assessment Process Flow Diagram, identify which areas of security are applicable to Artemis Financial’s software application. Justify your reasoning for why each area is relevant to the software application.

* Input Validation – It is extremely important to implement strong input validation to ensure that the threat of SQL injection and other similar attacks is mitigated. Input validation is important for both front facing access to systems and back-end inputs.
* APIs – It is important to develop a strong API to standardize and secure the features of the application. Sharing application logic securely between platforms is a requirement for this project.
* Client / Server – Ensuring the security of client server connections is mandatory for this application. Clients must be able to rely on the security of their interactions with their financial institution.
* Code Quality – High quality code is the only option when developing a project of this magnitude. All code should be clean, properly commented, and modular. This ensures future programmers can easily update and improve software as new threats are detected.

## 3. Manual Review

Continue working through the Vulnerability Assessment Process Flow Diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

No input authentication in CRUDController.

No input authentication in GreetingController.java.

I don’t think HTTPS is utilized.

DocData.java exposes connection.

## 4. Static Testing

Run a dependency check on Artemis Financial’s software application to identify all security vulnerabilities in the code. Record the output from dependency check report. Include the following:

1. The names or vulnerability codes of the known vulnerabilities
2. A brief description and recommended solutions provided by the dependency check report
3. Attribution (if any) that documents how this vulnerability has been identified or documented previously

Dependency: bcprov-jdk15on-1.46.jar

[CVE-2016-1000338](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000338)

[CVE-2016-1000342](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000342)

In Bouncy Castle JCE Provider version 1.55 and earlier the DSA does not fully validate ASN.1 encoding of signature on verification. It is possible to inject extra elements in the sequence making up the signature and still have it validate, which in some cases may allow the introduction of 'invisible' data into a signed structure.

[CVE-2016-1000343](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000343)

In the Bouncy Castle JCE Provider version 1.55 and earlier the DSA key pair generator generates a weak private key if used with default values. If the JCA key pair generator is not explicitly initialized with DSA parameters, 1.55 and earlier generates a private value assuming a 1024 bit key size. In earlier releases this can be dealt with by explicitly passing parameters to the key pair generator.

CVE-2018-1000180 (OSSINDEX)

Bouncy Castle BC 1.54 - 1.59, BC-FJA 1.0.0, BC-FJA 1.0.1 and earlier have a flaw in the Low-level interface to RSA key pair generator, specifically RSA Key Pairs generated in low-level API with added certainty may have less M-R tests than expected. This appears to be fixed in versions BC 1.60 beta 4 and later, BC-FJA 1.0.2 and later.

[CVE-2016-1000344](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000344)

In the Bouncy Castle JCE Provider version 1.55 and earlier the DHIES implementation allowed the use of ECB mode. This mode is regarded as unsafe and support for it has been removed from the provider.

[CVE-2016-1000352](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000352)

In the Bouncy Castle JCE Provider version 1.55 and earlier the ECIES implementation allowed the use of ECB mode. This mode is regarded as unsafe and support for it has been removed from the provider.

[CVE-2016-1000341](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000341)

In the Bouncy Castle JCE Provider version 1.55 and earlier DSA signature generation is vulnerable to timing attack. Where timings can be closely observed for the generation of signatures, the lack of blinding in 1.55, or earlier, may allow an attacker to gain information about the signature's k value and ultimately the private value as well.

[CVE-2016-1000345](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000345)

In the Bouncy Castle JCE Provider version 1.55 and earlier the DHIES/ECIES CBC mode vulnerable to padding oracle attack. For BC 1.55 and older, in an environment where timings can be easily observed, it is possible with enough observations to identify when the decryption is failing due to padding.

[CVE-2017-13098](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-13098)

BouncyCastle TLS prior to version 1.0.3, when configured to use the JCE (Java Cryptography Extension) for cryptographic functions, provides a weak Bleichenbacher oracle when any TLS cipher suite using RSA key exchange is negotiated. An attacker can recover the private key from a vulnerable application. This vulnerability is referred to as "ROBOT."

[CVE-2020-15522](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-15522)

Bouncy Castle BC Java before 1.66, BC C# .NET before 1.8.7, BC-FJA before 1.0.1.2, 1.0.2.1, and BC-FNA before 1.0.1.1 have a timing issue within the EC math library that can expose information about the private key when an attacker is able to observe timing information for the generation of multiple deterministic ECDSA signatures.

CVE-2020-0187 (OSSINDEX)

In engineSetMode of BaseBlockCipher.java, there is a possible incorrect cryptographic algorithm chosen due to an incomplete comparison. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-148517383

[CVE-2016-1000339](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000339)

In the Bouncy Castle JCE Provider version 1.55 and earlier the primary engine class used for AES was AESFastEngine. Due to the highly table driven approach used in the algorithm it turns out that if the data channel on the CPU can be monitored the lookup table accesses are sufficient to leak information on the AES key being used. There was also a leak in AESEngine although it was substantially less. AESEngine has been modified to remove any signs of leakage (testing carried out on Intel X86-64) and is now the primary AES class for the BC JCE provider from 1.56. Use of AESFastEngine is now only recommended where otherwise deemed appropriate.

CVE-2020-26939 (OSSINDEX)

In Legion of the Bouncy Castle BC before 1.61 and BC-FJA before 1.0.1.2, attackers can obtain sensitive information about a private exponent because of Observable Differences in Behavior to Error Inputs. This occurs in org.bouncycastle.crypto.encodings.OAEPEncoding. Sending invalid ciphertext that decrypts to a short payload in the OAEP Decoder could result in the throwing of an early exception, potentially leaking some information about the private exponent of the RSA private key performing the encryption.

[CVE-2015-7940](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7940)

The Bouncy Castle Java library before 1.51 does not validate a point is withing the elliptic curve, which makes it easier for remote attackers to obtain private keys via a series of crafted elliptic curve Diffie Hellman (ECDH) key exchanges, aka an "invalid curve attack."

[CVE-2018-5382](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5382)

The default BKS keystore use an HMAC that is only 16 bits long, which can allow an attacker to compromise the integrity of a BKS keystore. Bouncy Castle release 1.47 changes the BKS format to a format which uses a 160 bit HMAC instead. This applies to any BKS keystore generated prior to BC 1.47. For situations where people need to create the files for legacy reasons a specific keystore type "BKS-V1" was introduced in 1.49. It should be noted that the use of "BKS-V1" is discouraged by the library authors and should only be used where it is otherwise safe to do so, as in where the use of a 16 bit checksum for the file integrity check is not going to cause a security issue in itself.

[CVE-2013-1624](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1624)

The TLS implementation in the Bouncy Castle Java library before 1.48 and C# library before 1.8 does not properly consider timing side-channel attacks on a noncompliant MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, a related issue to CVE-2013-0169.

[CVE-2016-1000346](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000346)

In the Bouncy Castle JCE Provider version 1.55 and earlier the other party DH public key is not fully validated. This can cause issues as invalid keys can be used to reveal details about the other party's private key where static Diffie-Hellman is in use. As of release 1.56 the key parameters are checked on agreement calculation.

CVE-2015-6644 (OSSINDEX)

Bouncy Castle in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to obtain sensitive information via a crafted application, aka internal bug 24106146.

**Solution:** Upgrade to Release 1.71

Dependency: hibernate-validator-6.0.18.Final.jar

[CVE-2020-10693](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-10693)

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.

**Solution:** Update Hibernate Validator to version 7.0.

Dependency: jackson-databind-2.10.2.jar

[CVE-2020-25649](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25649)

A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.

[CVE-2020-36518](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-36518)

jackson-databind before 2.13.0 allows a Java StackOverflow exception and denial of service via a large depth of nested objects.

**Solution:** Update to version 2.13.3

Dependency: log4j-api-2.12.1.jar

[CVE-2020-9488](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9488)

Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender. Fixed in Apache Log4j 2.12.3 and 2.13.1

**Solution:** Update to Log4j 2.17.2

Dependency: logback-core-1.2.3.jar

[CVE-2021-42550](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42550)

In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers.

**Solution:** Update to LOGBack 1.2.11

Dependency: snakeyaml-1.25.jar

[CVE-2017-18640](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18640)

The Alias feature in SnakeYAML 1.18 allows entity expansion during a load operation, a related issue to CVE-2003-1564.

CWE-776 Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')

**Solution:** Update to SnakeYAML version 1.30

Dependency: spring-aop-5.2.3.RELEASE.jar

[CVE-2016-1000027](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000027)

Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required. NOTE: the vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data.

[CVE-2022-22965](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965)

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

[CVE-2021-22118](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118)

In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.

[CVE-2022-22970](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22970)

In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.

CWE-770 Allocation of Resources Without Limits or Throttling

[CVE-2020-5421](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421)

In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

[CVE-2022-22950](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950)

In Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.

[CVE-2022-22971](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22971)

In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, application with a STOMP over WebSocket endpoint is vulnerable to a denial of service attack by an authenticated user.

[CVE-2022-22968](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968)

In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.

CWE-178 Improper Handling of Case Sensitivity

[CVE-2021-22060](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060)

In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.

[CVE-2021-22096](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096)

In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.

NVD-CWE-Other

**Solution:** Update to Spring Framework Version 5.3.19

Dependency: spring-boot-2.2.4.RELEASE.jar

[CVE-2022-27772](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27772)

\*\* UNSUPPORTED WHEN ASSIGNED \*\* spring-boot versions prior to version v2.2.11.RELEASE was vulnerable to temporary directory hijacking. This vulnerability impacted the org.springframework.boot.web.server.AbstractConfigurableWebServerFactory.createTempDir method. NOTE: This vulnerability only affects products and/or versions that are no longer supported by the maintainer.

CWE-668 Exposure of Resource to Wrong Sphere

**Solution:** Update to Spring Boot 2.6.6.

Dependency: spring-core-5.2.3.RELEASE.jar

[CVE-2016-1000027](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000027)

Pivotal Spring Framework through 5.3.16 suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Depending on how the library is implemented within a product, this issue may or not occur, and authentication may be required. NOTE: the vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data.

CWE-502 Deserialization of Untrusted Data

[CVE-2022-22965](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965)

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

CWE-94 Improper Control of Generation of Code ('Code Injection')

[CVE-2021-22118](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118)

In Spring Framework, versions 5.2.x prior to 5.2.15 and versions 5.3.x prior to 5.3.7, a WebFlux application is vulnerable to a privilege escalation: by (re)creating the temporary storage directory, a locally authenticated malicious user can read or modify files that have been uploaded to the WebFlux application, or overwrite arbitrary files with multipart request data.

CWE-269 Improper Privilege Management

[CVE-2022-22970](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22970)

In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, applications that handle file uploads are vulnerable to DoS attack if they rely on data binding to set a MultipartFile or javax.servlet.Part to a field in a model object.

CWE-770 Allocation of Resources Without Limits or Throttling

[CVE-2020-5421](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421)

In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

NVD-CWE-noinfo

[CVE-2022-22950](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950)

In Spring Framework versions 5.3.0 - 5.3.16 and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial of service condition.

CWE-770 Allocation of Resources Without Limits or Throttling

[CVE-2022-22971](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22971)

In spring framework versions prior to 5.3.20+ , 5.2.22+ and old unsupported versions, application with a STOMP over WebSocket endpoint is vulnerable to a denial of service attack by an authenticated user.

CWE-770 Allocation of Resources Without Limits or Throttling

[CVE-2022-22968](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968)

In Spring Framework versions 5.3.0 - 5.3.18, 5.2.0 - 5.2.20, and older unsupported versions, the patterns for disallowedFields on a DataBinder are case sensitive which means a field is not effectively protected unless it is listed with both upper and lower case for the first character of the field, including upper and lower case for the first character of all nested fields within the property path.

CWE-178 Improper Handling of Case Sensitivity

[CVE-2021-22060](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060)

In Spring Framework versions 5.3.0 - 5.3.13, 5.2.0 - 5.2.18, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries. This is a follow-up to CVE-2021-22096 that protects against additional types of input and in more places of the Spring Framework codebase.

[CVE-2021-22096](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096)

In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.

NVD-CWE-Other

**Solution:** Update to Spring Framework Version 5.3.19

Dependency: tomcat-embed-core-9.0.30.jar

[CVE-2020-1938](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1938)

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

CWE-269 Improper Privilege Management

[CVE-2020-11996](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11996)

A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat 10.0.0-M1 to 10.0.0-M5, 9.0.0.M1 to 9.0.35 and 8.5.0 to 8.5.55 could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive.

[CVE-2020-13934](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13934)

An h2c direct connection to Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M5 to 9.0.36 and 8.5.1 to 8.5.56 did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of service.

CWE-401 Improper Release of Memory Before Removing Last Reference ('Memory Leak'), CWE-476 NULL Pointer Dereference

[CVE-2020-13935](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13935)

The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service.

CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')

[CVE-2020-17527](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17527)

While investigating bug 64830 it was discovered that Apache Tomcat 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to 9.0.39 and 8.5.0 to 8.5.59 could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream. While this would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests.

CWE-200 Information Exposure

[CVE-2021-25122](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25122)

When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41 and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request.

[CVE-2021-41079](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41079)

Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.

CWE-20 Improper Input Validation

[CVE-2022-29885](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29885)

The documentation of Apache Tomcat 10.1.0-M1 to 10.1.0-M14, 10.0.0-M1 to 10.0.20, 9.0.13 to 9.0.62 and 8.5.38 to 8.5.78 for the EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network. This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted network, particularly DoS risks.

[CVE-2020-9484](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9484)

When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.

CWE-502 Deserialization of Untrusted Data

[CVE-2021-25329](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25329)

The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue.

[CVE-2021-30640](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30640)

A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.

[CVE-2021-24122](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24122)

When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances.

CWE-200 Information Exposure

[CVE-2021-33037](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33037)

Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

[CVE-2019-17569](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-17569)

The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

[CVE-2020-1935](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1935)

In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

[CVE-2020-13943](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13943)

If an HTTP/2 client connecting to Apache Tomcat 10.0.0-M1 to 10.0.0-M7, 9.0.0.M1 to 9.0.37 or 8.5.0 to 8.5.57 exceeded the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it was possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This could lead to users seeing responses for unexpected resources.

**Solution:** Update to current version, check default AJP Connector configuration. Use HTTPS. Check for current patches.

Dependency: tomcat-embed-websocket-9.0.30.jar

[CVE-2020-1938](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1938)

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

CWE-269 Improper Privilege Management

[CVE-2020-8022](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8022)

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CWE-276 Incorrect Default Permissions

[CVE-2020-11996](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11996)

A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat 10.0.0-M1 to 10.0.0-M5, 9.0.0.M1 to 9.0.35 and 8.5.0 to 8.5.55 could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive.

[CVE-2020-13934](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13934)

An h2c direct connection to Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M5 to 9.0.36 and 8.5.1 to 8.5.56 did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of service.

CWE-401 Improper Release of Memory Before Removing Last Reference ('Memory Leak'), CWE-476 NULL Pointer Dereference

[CVE-2020-13935](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13935)

The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service.

CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')

[CVE-2020-17527](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17527)

While investigating bug 64830 it was discovered that Apache Tomcat 10.0.0-M1 to 10.0.0-M9, 9.0.0-M1 to 9.0.39 and 8.5.0 to 8.5.59 could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream. While this would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests.

CWE-200 Information Exposure

[CVE-2021-25122](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25122)

When responding to new h2c connection requests, Apache Tomcat versions 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41 and 8.5.0 to 8.5.61 could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request.

[CVE-2021-41079](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41079)

Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.

CWE-20 Improper Input Validation

[CVE-2022-29885](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29885)

The documentation of Apache Tomcat 10.1.0-M1 to 10.1.0-M14, 10.0.0-M1 to 10.0.20, 9.0.13 to 9.0.62 and 8.5.38 to 8.5.78 for the EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network. This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted network, particularly DoS risks.

[CVE-2020-9484](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9484)

When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.

CWE-502 Deserialization of Untrusted Data

[CVE-2021-25329](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25329)

The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue.

[CVE-2021-30640](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30640)

A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.

CWE-287 Improper Authentication

[CVE-2021-24122](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24122)

When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances.

CWE-200 Information Exposure

[CVE-2021-33037](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33037)

Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

[CVE-2019-17569](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-17569)

The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

[CVE-2020-1935](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1935)

In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

[CVE-2020-13943](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13943)

If an HTTP/2 client connecting to Apache Tomcat 10.0.0-M1 to 10.0.0-M7, 9.0.0.M1 to 9.0.37 or 8.5.0 to 8.5.57 exceeded the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it was possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This could lead to users seeing responses for unexpected resources.

**Solution:** Update and Patch to newest versions.

## 5. Mitigation Plan

After interpreting your results from the manual review and static testing, identify the steps to remedy the identified security vulnerabilities for Artemis Financial’s software application.

The static testing showed many of the vulnerabilities present in this application can be mitigated by updating the dependencies. It is extremely important to stay up to date with software updates and patches of known vulnerabilities. HTTPS should be the standard to ensure secure client/server connections. Robust input validation should be implemented on both client and server sides. Source code should be cleaned up and more clearly commented.