# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **03/18/2025** | **Mike R. Montminy** | **Parts 1, 2, and 3 completed** |
| **1.1** | **03/19/2025** | **Mike R. Montminy** | **Parts 4 and 5 completed** |

## Client



## Instructions

Submit this completed vulnerability assessment report. Replace the bracketed text with the relevant information. In this report, identify your security vulnerability findings and recommend 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 include images or supporting materials. If you include them, make certain to insert them in 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

Mike R. Montminy

**1. Interpreting Client Needs**

Determine your client’s needs and potential threats and attacks associated with the company’s application and software security requirements. Consider the following questions 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 on secure communications to consider?
* What external threats might be present now and in the immediate future?
* What modernization requirements must be considered, such as the role of open-source libraries and evolving web application technologies?

The biggest security concern with Artemis Financial will be a secure communication network between clients and AF. Artemis handles a variety of confidential data relating to customers, so having secure communication protocols in place will be essential in protection against and data interception and thus ensuring an end-to-end encryption solution. If Artemis chooses to start working internationally, then there is a plethora of regulations that must be adhered to. The GDPR and FDIC all have laws to ensure protection of customer data and to notify any customers of data breachers. The application will have to be developed to follow all guidelines without issues. The most applicable external threat AF could face is an SQL injection where a malicious entity chooses to inset an SQL query as an input in an application to pull confidential data out of a database. The main modernization requirement that must be considered is ensuring all web services are HTTPS secured and not HTTP as a way of boosting all client and server interactions. A second modernization requirement is that everything is running the newest possible version of any open-source libraries that may be used to ensure minimal security vulnerabilities.

**2. Areas of Security**

Refer to the vulnerability assessment process flow diagram. Identify which areas of security apply to Artemis Financials' software application. Justify your reasoning for why each area is relevant to the software application.

Cryptography: This area is highly important due to the sensitivity of the data that a customer may be entering at any given time. Any lead of customer data could lead to a full breach of financial information, privacy, address, etc. Having strong cryptography will ensure that all forms of client and server communications using the data will be heavily secure and encrypted.

Client / Server: This area is important as sensitive financial and personal information will be sent between the AF server databases and a client device consistently. If these communication methods stay unsecured then a potential malicious individual could easily grab the information and cause copious amounts of damage with the information that has been pulled.

Input Validations: Customers will need to sign on to the service using usernames, passwords, emails, and possibly two factor authentication methods. It is ideal to have an application that ensures only specific information is given out based on the login credentials that get used. The application must also have SQL injection protections that use input forms as the exploit type.

Code Quality: Following secure coding practices with the aim to avoid any vulnerabilities that could come up from a developer practicing poor coding practices. Techniques for preventing an SQL injection must be implemented in order to ensure customer data is safe at all times.

API: This area is highly important as the program is currently using the RESTful API. APIs act as a medium for server responses and any client requests. This leads to APIs being a hot target for any attackers trying to intercept the communications. It is vital to all information both AF clients and AF themselves to have a highly secure API.

**3. Manual Review**

Continue working through the vulnerability assessment process flow diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

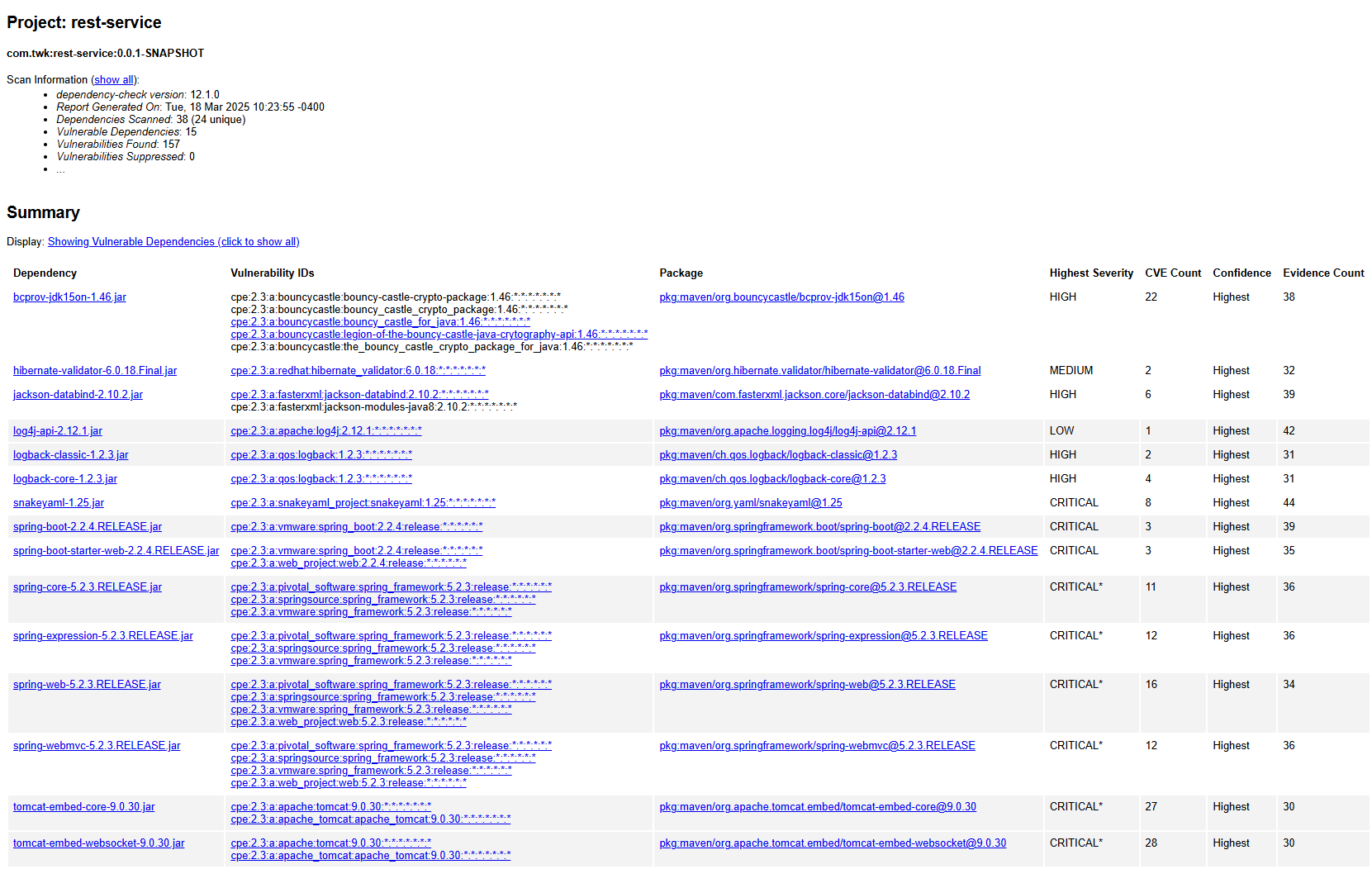
**Found Vulnerabilities:**

* **CRUD.java: Public accessor and constructor and insecure data handling**
* **CRUDController.java: Susceptible to a code inject**
* **Customer.java: Public accessor and constructor**
* **DocData.java: Input is handled with a URL instead of the POST method. This could lead to the browser history leaking out sensitive data.**
* **Greeting.java: Public accessor and constructor**
* **GreetingController.java: Zero input validation present**
* **No functioning API as of this moment**
* **No end-to-end encryption**

**4. Static Testing**

Run a dependency check on Artemis Financials' software application to identify all security vulnerabilities in the code. Record the output from the dependency-check report. Include the following items:

* The names or vulnerability codes of the known vulnerabilities
* A brief description and recommended solutions provided by the dependency-check report
* Any attribution that documents how this vulnerability has been identified or documented previously



**Dependency:** [bcprov-jdk15on-1.46.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F0a3fe32a92a345d5869bde94221a1d53&wdorigin=AuthPrompt.OFFICECOM-WEB.START.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=7d9514a6-7acb-4bfc-8f17-8a5d8ae113b1&wdenableroaming=1&mscc=1&wdodb=1&hid=9B118CA1-902F-8000-3F9E-D08D89EF18A2.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&usid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l1_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7)**ID:** [**CVE-2023-33202**](https://nvd.nist.gov/vuln/detail/CVE-2023-33202)**Description:** Bouncy Castle for Java before 1.73 contains a potential Denial of Service (DoS) issue within the Bouncy Castle org.bouncycastle.openssl.PEMParser class. This class parses OpenSSL PEM encoded streams containing X.509 certificates, PKCS8 encoded keys, and PKCS7 objects. Parsing a file that has crafted ASN.1 data through the PEMParser causes an OutOfMemoryError, which can enable a denial of service attack.  
Fix: Update to newest stable version of BC

ID: [**CVE-2016-1000352**](https://nvd.nist.gov/vuln/detail/CVE-2016-1000352)

**Description:** 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.

Fix: Update past BC JCE Provider version 1.55

Dependency: [hibernate-validator-6.0.18.Final.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F0a3fe32a92a345d5869bde94221a1d53&wdorigin=AuthPrompt.OFFICECOM-WEB.START.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=7d9514a6-7acb-4bfc-8f17-8a5d8ae113b1&wdenableroaming=1&mscc=1&wdodb=1&hid=9B118CA1-902F-8000-3F9E-D08D89EF18A2.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&usid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l3_7fd00bcd87e14b6ba66279282ef15efa30dd2492)ID: [**CVE-2020-10693**](https://nvd.nist.gov/vuln/detail/CVE-2020-10693)

Description: 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.

Fix: Update to version 6.1.5 or newer

Dependency: [jackson-databind-2.10.2.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F0a3fe32a92a345d5869bde94221a1d53&wdorigin=AuthPrompt.OFFICECOM-WEB.START.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=7d9514a6-7acb-4bfc-8f17-8a5d8ae113b1&wdenableroaming=1&mscc=1&wdodb=1&hid=9B118CA1-902F-8000-3F9E-D08D89EF18A2.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&usid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l5_0528de95f198afafbcfb0c09d2e43b6e0ea663ec)ID: [**CVE-2023-35116**](https://nvd.nist.gov/vuln/detail/CVE-2023-35116)Description: 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.

Fix: Update to a version past 2.16.0

Dependency: [log4j-api-2.12.1.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F0a3fe32a92a345d5869bde94221a1d53&wdorigin=AuthPrompt.OFFICECOM-WEB.START.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=7d9514a6-7acb-4bfc-8f17-8a5d8ae113b1&wdenableroaming=1&mscc=1&wdodb=1&hid=9B118CA1-902F-8000-3F9E-D08D89EF18A2.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&usid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l10_a55e6d987f50a515c9260b0451b4fa217dc539cb)

ID: [**CVE-2021-44832**](https://nvd.nist.gov/vuln/detail/CVE-2021-44832)

Description: 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.

Fix: 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  
  
Dependency: [logback-core-1.2.3.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F3756620765734fbdbadd87b4ee289bca&wdorigin=AuthPrompt.OFFICECOM-WEB.START.UPLOAD&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=65087a52-da5e-4426-a35f-0bfdc16a6050&wdenableroaming=1&mscc=1&wdodb=1&hid=22338AA1-C0B1-8000-3F9E-D25B1AD8C599.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=af2ea32e-c924-c0a8-d930-0c157e6e5440&usid=af2ea32e-c924-c0a8-d930-0c157e6e5440&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l12_864344400c3d4d92dfeb0a305dc87d953677c03c) and [logback-classic-1.2.3.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F3756620765734fbdbadd87b4ee289bca&wdorigin=AuthPrompt.OFFICECOM-WEB.START.UPLOAD&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=65087a52-da5e-4426-a35f-0bfdc16a6050&wdenableroaming=1&mscc=1&wdodb=1&hid=22338AA1-C0B1-8000-3F9E-D25B1AD8C599.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=af2ea32e-c924-c0a8-d930-0c157e6e5440&usid=af2ea32e-c924-c0a8-d930-0c157e6e5440&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l11_7c4f3c474fb2c041d8028740440937705ebb473a)

ID: CVE-2023-6378

Description: A serialization vulnerability in logback receiver component part of logback version 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending poisoned data.

Fix: Update to a version past 1.14.12

Dependency: [snakeyaml-1.25.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F3756620765734fbdbadd87b4ee289bca&wdorigin=AuthPrompt.OFFICECOM-WEB.START.UPLOAD&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=65087a52-da5e-4426-a35f-0bfdc16a6050&wdenableroaming=1&mscc=1&wdodb=1&hid=22338AA1-C0B1-8000-3F9E-D25B1AD8C599.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=af2ea32e-c924-c0a8-d930-0c157e6e5440&usid=af2ea32e-c924-c0a8-d930-0c157e6e5440&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l15_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421)

ID: CVE-2022-1471

Description: SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution.

Fix: Update to a version past 2.0.0

Dependency: [spring-boot-2.2.4.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F3756620765734fbdbadd87b4ee289bca&wdorigin=AuthPrompt.OFFICECOM-WEB.START.UPLOAD&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=65087a52-da5e-4426-a35f-0bfdc16a6050&wdenableroaming=1&mscc=1&wdodb=1&hid=22338AA1-C0B1-8000-3F9E-D25B1AD8C599.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=af2ea32e-c924-c0a8-d930-0c157e6e5440&usid=af2ea32e-c924-c0a8-d930-0c157e6e5440&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l16_225a4fd31156c254e3bb92adb42ee8c6de812714) and [spring-boot-starter-web-2.2.4.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F3756620765734fbdbadd87b4ee289bca&wdorigin=AuthPrompt.OFFICECOM-WEB.START.UPLOAD&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=65087a52-da5e-4426-a35f-0bfdc16a6050&wdenableroaming=1&mscc=1&wdodb=1&hid=22338AA1-C0B1-8000-3F9E-D25B1AD8C599.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=af2ea32e-c924-c0a8-d930-0c157e6e5440&usid=af2ea32e-c924-c0a8-d930-0c157e6e5440&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l17_ec75d01d212b5229c16d872fb127744c0ed46ed8)

ID: CVE-2023-20883

Description: In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache.

Fix: Update to a version past 3.0.6

Dependency: [spring-core-5.2.3.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F0a3fe32a92a345d5869bde94221a1d53&wdorigin=AuthPrompt.OFFICECOM-WEB.START.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=7d9514a6-7acb-4bfc-8f17-8a5d8ae113b1&wdenableroaming=1&mscc=1&wdodb=1&hid=9B118CA1-902F-8000-3F9E-D08D89EF18A2.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&usid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l18_3734223040040e8c3fecd5faa3ae8a1ed6da146b) , [spring-expression-5.2.3.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F0a3fe32a92a345d5869bde94221a1d53&wdorigin=AuthPrompt.OFFICECOM-WEB.START.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=7d9514a6-7acb-4bfc-8f17-8a5d8ae113b1&wdenableroaming=1&mscc=1&wdodb=1&hid=9B118CA1-902F-8000-3F9E-D08D89EF18A2.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&usid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l19_d0c6bb10758805b2153c589686b8045554bfac2d) , [spring-web-5.2.3.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F0a3fe32a92a345d5869bde94221a1d53&wdorigin=AuthPrompt.OFFICECOM-WEB.START.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=7d9514a6-7acb-4bfc-8f17-8a5d8ae113b1&wdenableroaming=1&mscc=1&wdodb=1&hid=9B118CA1-902F-8000-3F9E-D08D89EF18A2.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&usid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l20_dd386a02e40b915ab400a3bf9f586d2dc4c0852c) , and [spring-webmvc-5.2.3.RELEASE.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F0a3fe32a92a345d5869bde94221a1d53&wdorigin=AuthPrompt.OFFICECOM-WEB.START.REC&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=7d9514a6-7acb-4bfc-8f17-8a5d8ae113b1&wdenableroaming=1&mscc=1&wdodb=1&hid=9B118CA1-902F-8000-3F9E-D08D89EF18A2.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&usid=50a7aee5-7e00-cb8b-e4e1-e14ed217d81b&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l21_745a62502023d2496b565b7fe102bb1ee229d6b7)ID: [**CVE-2023-20863**](https://nvd.nist.gov/vuln/detail/CVE-2023-20863)Description: In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.  
Fix: Update to a version past 6.0.8

Dependency: [tomcat-embed-core-9.0.30.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F3756620765734fbdbadd87b4ee289bca&wdorigin=AuthPrompt.OFFICECOM-WEB.START.UPLOAD&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=65087a52-da5e-4426-a35f-0bfdc16a6050&wdenableroaming=1&mscc=1&wdodb=1&hid=22338AA1-C0B1-8000-3F9E-D25B1AD8C599.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=af2ea32e-c924-c0a8-d930-0c157e6e5440&usid=af2ea32e-c924-c0a8-d930-0c157e6e5440&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l22_ad32909314fe2ba02cec036434c0addd19bcc580) and [tomcat-embed-websocket-9.0.30.jar](https://usc-word-edit.officeapps.live.com/we/wordeditorframe.aspx?ui=en-US&rs=en-US&wopisrc=https%3A%2F%2Fsnhu-my.sharepoint.com%2Fpersonal%2Fmichael_montminy_snhu_edu%2F_vti_bin%2Fwopi.ashx%2Ffiles%2F3756620765734fbdbadd87b4ee289bca&wdorigin=AuthPrompt.OFFICECOM-WEB.START.UPLOAD&wdprevioussessionsrc=HarmonyWeb&wdprevioussession=65087a52-da5e-4426-a35f-0bfdc16a6050&wdenableroaming=1&mscc=1&wdodb=1&hid=22338AA1-C0B1-8000-3F9E-D25B1AD8C599.0&uih=sharepointcom&wdlcid=en-US&jsapi=1&jsapiver=v2&corrid=af2ea32e-c924-c0a8-d930-0c157e6e5440&usid=af2ea32e-c924-c0a8-d930-0c157e6e5440&newsession=1&sftc=1&uihit=docaspx&muv=1&cac=1&sams=1&mtf=1&sfp=1&sdp=1&hch=1&hwfh=1&dchat=1&sc=%7B%22pmo%22%3A%22https%3A%2F%2Fsnhu-my.sharepoint.com%22%2C%22pmshare%22%3Atrue%7D&ctp=LeastProtected&rct=Normal&csc=1&instantedit=1&wopicomplete=1&wdredirectionreason=Unified_SingleFlush#l24_33157f6bc5bfd03380ebb5ac476db0600a04168d)ID: CVE-2024-38286

Description: Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M20, from 10.1.0-M1 through 10.1.24, from 9.0.13 through 9.0.89. Older, unsupported versions may also be affected.  
Fix: Users are recommended to upgrade to version 11.0.0-M21, 10.1.25, or 9.0.90, which fixes the issue.

**5. Mitigation Plan**

Interpret the results from the manual review and static testing report. Then identify the steps to mitigate the identified security vulnerabilities for Artemis Financials' software application.

The first thing that must be done in mitigation of all vulnerabilities related to the AF API will be to update every plugin to the newest stable version. This helps in fixing a plethora of bugs and vulnerabilities and protect the application as best as possible. Input validation and error handling must be added in a few files to ensure security against something such as a code or SQL injection. The next step will be to have the development team add cryptographic strategies as a means of protecting customer personal and financial information such as routing numbers, account numbers, full name, address, IP, etc. Additionally, a swap over to HTTPS as the communication protocol to protect any server/client interactions will be needed. Finally, many of the public accessors, constructors, and mutators need to be addressed and swapped over to being private.