****

# 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** | **[Date]** | **[Your name]** |  |

## 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

Christopher Rode

## Interpreting Client Needs

Artemis Financial is a financial institution that handles financial transactions. Secure communications are especially important to the company because they need to make sure their client's financial information is not being stolen by hackers or leaked or given to anyone but the intended client.

The company may make international transactions.

There are no government restrictions on secure communication.

There is a threat of attackers on the company. Many times, hackers will attack companies that deal with people's financial information to try and steal that information. In the futures hackers might develop new ways and technology to steal this information and breach the secure communication system.

To have great security the company may use open-source libraries.

## Areas of Security

Input validation- the inputs need to be secure and correct or they could produce the wrong output and potential crash the system.

API- there needs to be verification for each user to boost the overall security of the system. Things like 2-way authentication can help increase security of the system and prevent password stealing.

Cryptography- in case the data is taken it need to be impossible for the person who took it to understand and be able to use the stolen data. This is a final defense against attackers.

## Manual Review

The only thing that I noticed while doing a Manuel review was that the maven spring plugin that was being used could be updated to a more recent version.

## Static Testing

Vulnerability:

CVE-2013-1624 & CVE-2016-1000341

Recommended solution is to upgrade to 1.5 or 1.7 version

CVE-2015-6644 (OSSINDEX )

Recommended solution to upgrade Bouncy Castle in Android to 5.1.1 LMY49F and 6.0 ,2016-01-01

CVE-2015-7940 (OSSINDEX )

Recommended solution: to upgrade libraries to 1.5 and above.

CVE-2016-1000338 & CVE-2016-1000342.

Recommended Solution: update the cryptography – Red hat Fuse has included a package

CVE-2016-1000343

Possible solution: from the link I was directed to, setting the parameter in the code with the correct values. I was out of my comfort zone

CVE-2016-1000344 & CVE-2016-1000352

Dependency: Log4j.api.2.12.1.jar

Vulnerability: CVE-2020-9488

Possible Solution would be to upgrade to log4j2

Vulnerability: CVE-2017-18640\

Possible solution: use filter, use OWASP. From what I gathered, we would need to implement load configurations in the code.

CVE-2019-17569

Possible solution to upgrade tomcat 9.0.31

CVE-2020-11996

Possible solution would be to upgrade to 9.0.36

CVE-2020-13934

Possible Solution: would be to download YaST online\_update or "zypper patch"\

CVE-2020-13935

Possible Solution: Customers using ePO 5.10: Update to ePO 5.10.0 Update 9. Customers using ePO 5.9.1 and earlier: Do either of the following:

Upgrade to ePO 5.10.0 Update 9 to receive fixes for the Java, Tomcat, and XSS issues.

Upgrade to ePO 5.9.1 (if not on it already) and apply ePO 5.9.1 Hotfix EPO-919400 to receive fixes for only the Java and Tomcat issues.

Also, version 9.0.31-1~deb10u2 is recommended to upgrade to

CVE-2020-1938

Possible Solution: Many 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 would fix any issues related to this vulnerability

CVE-2020-8022

Possible Solution would be to upgrade to tomcat 9.0.35 download “YaST online\_update or "zypper patch".- openSUSE Leap 15.1 (noarch): tomcat-9.0.35-lp151.3.21.1 tomcat-admin-webapps-9.0.35-lp151.3.21.1 tomcat-docs-webapp-9.0.35-lp151.3.21.1 tomcat-el-3\_0-api-9.0.35-lp151.3.21.1 tomcat-embed-9.0.35-lp151.3.21.1 tomcat-javadoc-9.0.35-lp151.3.21.1 tomcat-jsp-2\_3-api-9.0.35-lp151.3.21.1 tomcat-jsvc-9.0.35-lp151.3.21.1 tomcat-lib-9.0.35-lp151.3.21.1 tomcat-servlet-4\_0-api-9.0.35-lp151.3.21.1 tomcat-webapps-9.0.35-lp151.3.21.1

CVE-2020-9484

Possible solutions: running this command would enable the application to be protection from any intrusion.

Vulnerability: CVE-2020-5421

Possible Solution: upgrade to an acceptable springframe work from 4.3.29 all the way up to 5.2.9

## Mitigation Plan

Above I listed all the vulnerabilities that the dependency check detected. Most of them are just out of data plugin versions that can be Easly fixed by updating them. Each of the vulnerability's listed above also comes with a recommended solution and can be fixed by the developer.