****

# Practices for Secure Software Report

Table of Contents

[Practices for Secure Software Report 1](#_Toc1903029535)

[Table of Contents 1](#_Toc667910372)

[Document Revision History 2](#_Toc1705169792)

[Client 3](#_Toc515197118)

[Developer 3](#_Toc31085204)

[1. Algorithm Cipher 3](#_Toc1248992255)

[2. Certificate Generation 3](#_Toc581508428)

[3. Deploy Cipher & 4. Secure Communications 4](#_Toc19026918)

[5. Secondary Testing 4](#_Toc1724378316)

[6. Functional Testing 5](#_Toc1279520384)

[7. Summary 5](#_Toc474474291)

[8. Industry Standard Best Practices 5](#_Toc50315126)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **8/11/2023** | **Ryan LeChien** |  |

## Client



## Developer

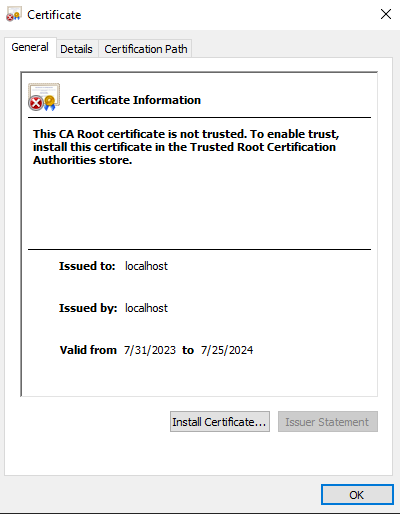
Ryan LeChien

## Algorithm Cipher

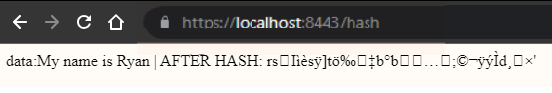
For the purpose of encrypting Artemis Financial’s web traffic and other data, the Advanced Encryption Standard algorithm, as specified by the National Institute of Standards and Technology in FIPS 197, is the most suitable cipher algorithm. As stated by its FIPS publication, AES is a “cryptographic algorithm that can be used to protect electronic data.” Furthermore, “[t]he AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.” As Artemis Financial seeks to encrypt its traffic data, AES is evidently the most appropriate algorithm because it can both encrypt and decrypt data. This bidirectionality of the algorithm will allow the traffic data to be encrypted upon transmission and decrypted upon retrieval.

The cipher of the AES algorithm uses a rounding function implementation on the tokenized input ten, twelve, or fourteen times. The number of times the rounding function is used is a function of the key length. This repetitive use of the encryption algorithm is the key to the algorithm’s security. By encrypting as a function of input, the encrypted output is secure, as the reason for cracking encrypted data is to find the unencrypted text—the encrypted data cannot be cracked as its decrypted form is unknown. Therefore, the Advanced Encryption Standard algorithm is very appropriate for encrypting Artemis Financial’s web traffic and other data.

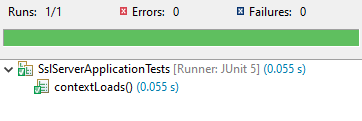
## Certificate Generation

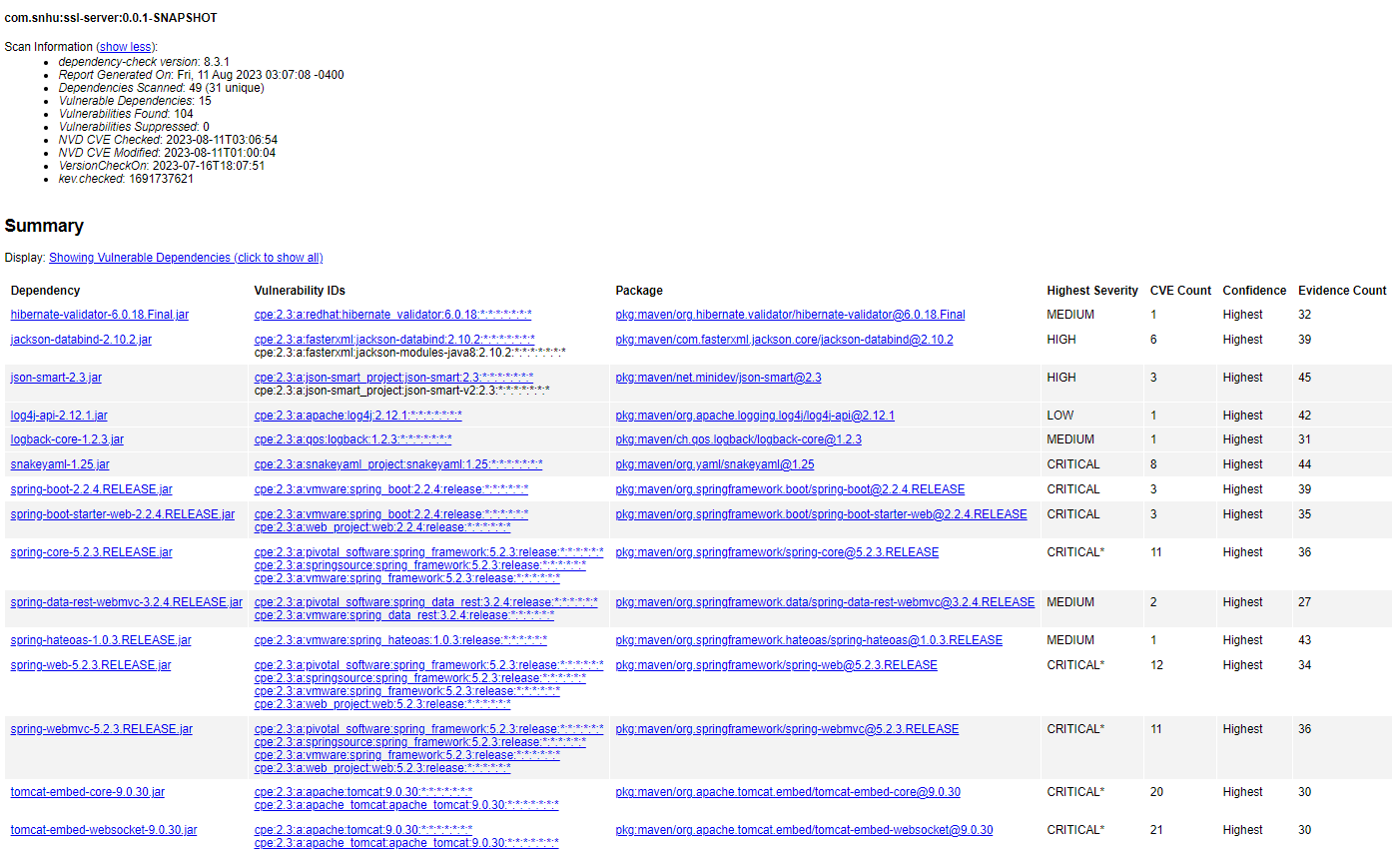


## Deploy Cipher & 4. Secure Communications

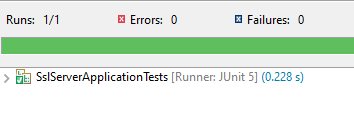


## Secondary Testing





## Functional Testing



## Summary

Of the key steps in the Vulnerability Assessment Process Flow Diagram, the step most addressed by the addition of the encryption and checksum verification steps is cryptography. Artemis Financial’s web communications are now encrypted, and a checksum is utilized to verify there is no tampering. All known vulnerabilities have been either addressed or deemed negligible.

## Industry Standard Best Practices

To mitigate known security vulnerabilities, the Common Vulnerabilities and Exposures database was queried, via the Maven dependency-check plug-in, to find known exploits that existed within the code. This consultation provided the development team with guaranteed knowledge of known exploits. To maintain the software application’s current security, only secure additions were made, namely the addition of an encryption standard for their web traffic and other data.

Applying industry standard best practices for secure coding is crucial for a company's overall wellbeing, as it serves as a robust foundation for protecting data, which in turn retains clientele. By adhering to these practices, developers can proactively identify and address potential vulnerabilities during the software’s development, reducing the likelihood of security flaws that could lead to data breaches. This proactive approach not only minimizes the need for reactive measures, but also maximizes development efficiency.