****

# Practices for Secure Software Report

Table of Contents

[Document Revision History 3](#_Toc102040754)

[Client 3](#_Toc102040755)

[Instructions 3](#_Toc102040756)

[Developer 4](#_Toc102040757)

[1. Algorithm Cipher 4](#_Toc102040758)

[2. Certificate Generation 4](#_Toc102040759)

[3. Deploy Cipher 4](#_Toc102040760)

[4. Secure Communications 4](#_Toc102040761)

[5. Secondary Testing 4](#_Toc102040762)

[6. Functional Testing 4](#_Toc102040763)

[7. Summary 4](#_Toc102040764)

[8. Industry Standard Best Practices 4](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **10/13/2023** | **Russell Willis** |  |

## Client



## Instructions

Submit this completed practices for secure software report. Replace the bracketed text with the relevant information. You must document your process for writing secure communications and refactoring code that complies with software security testing protocols.

* Respond to the 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 Two Guidelines and Rubric for more detailed instructions about each section of the template.

## Developer

Russell Willis

## Algorithm Cipher

The AES(Advanced Encryption Standard) is a is a commonly used encryption algorithm that uses a symmetric key algorithm that uses block ciphers.

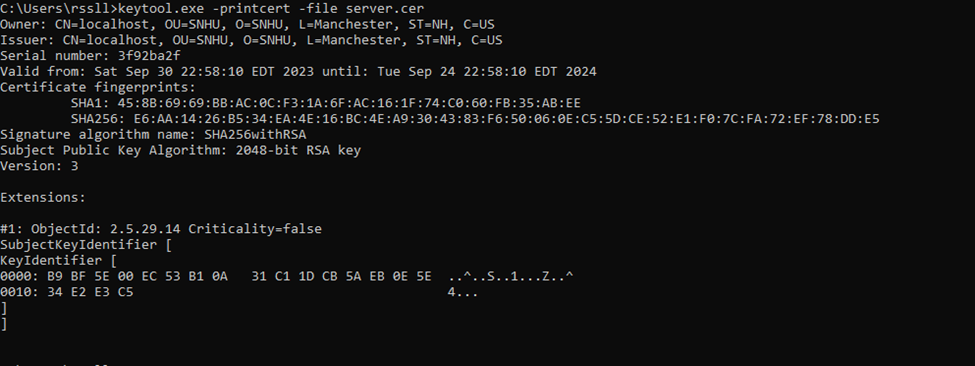
AES uses a secure has function which means it gets an arbitrary bit string as input and returns it as a fixed length string as the output. The bit levels of AES go as follows: 128, 192, and 256-bit.

Random numbers are used often to generate keys or to add some randomness to encryptions. Symmetric keys are used for encryption and decryption of the same key, where non symmetric keys use different keys for encryption and decryption.

The beginning of encryption can be traced back all the way to ancient Egypt around 1900 BC. Back then it was more about during battles, making it easy to have secret messages without them being figured out. Now encryption is continuously evolving and becoming more and more secure.\

## Certificate Generation

Insert a screenshot below of the CER file.



## Deploy Cipher

A computer screen with a white background

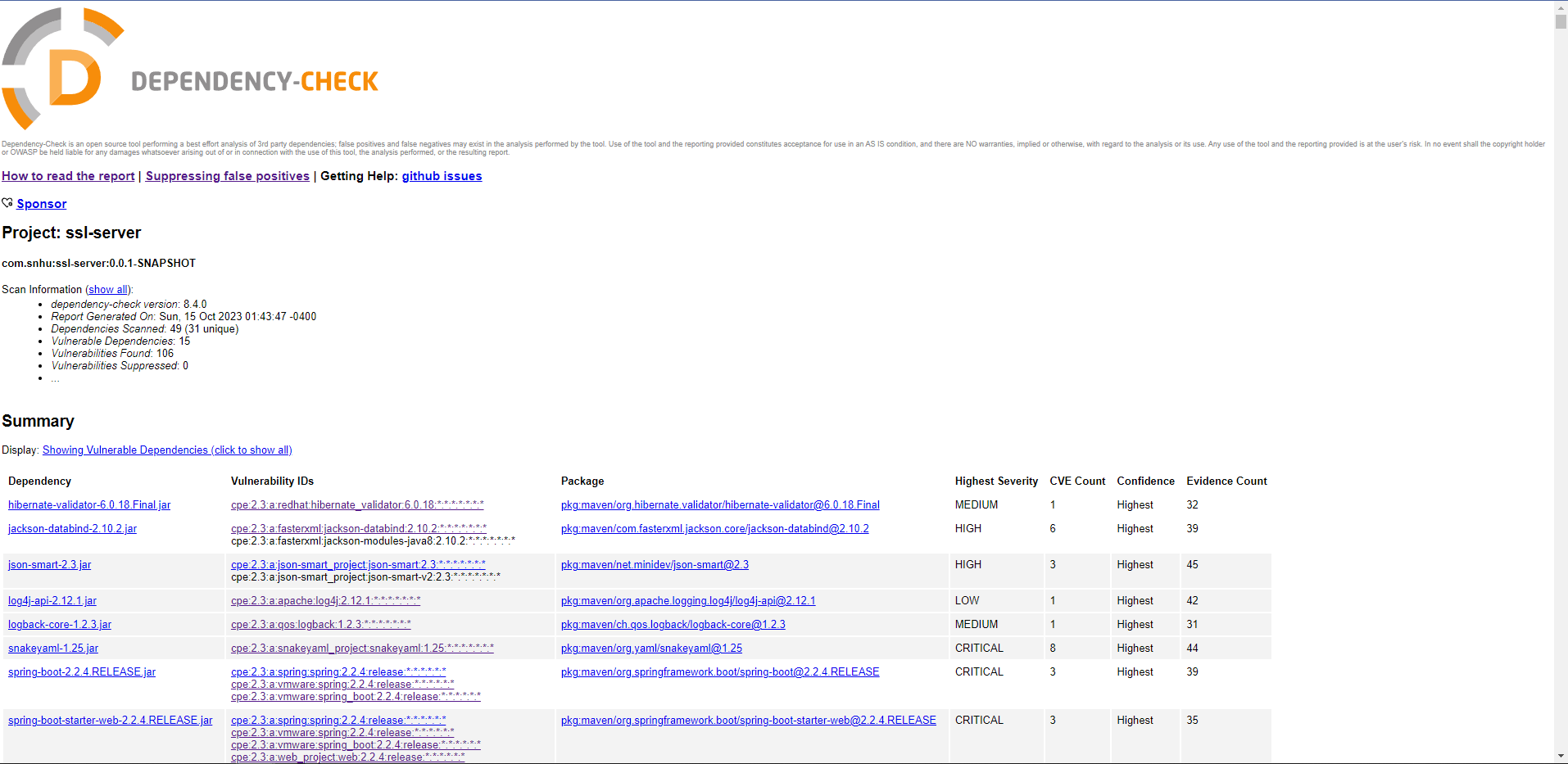
Description automatically generated

## Secure Communications

A computer screen with a white background

Description automatically generated

## Secondary Testing



## Functional Testing

A computer screen shot of text

Description automatically generated

## Summary

I added a secure rest controller to the application to serve as the secure controller. I updated the dependency check from 5.3.0 to 8.4.0 so that the static dependency check is as accurate as possible and to keep the security up to date as well.

## Industry Standard Best Practices

I used a strong encryption algorithm called AES with a key length of 256 bits to ensure that it is as secure as possible. I created a self-signed certificate to make secure https connection to help mitigate against known security vulnerabilities.

The value of using these safety measures is to make sure that the company is as safe as possible without having to deal with security vulnerabilities.