protiviti®

Face the Future with Confidence

CENTRAL FLORIDA EXPRESSWAY AUTHORITY SOURCE CODE REVIEW - SUMMARY

2/23/2020

Table of Content

I. Executive Summary

Background

In Q3 2019, CFX engaged a third party, Protiviti, to perform web application and secure code review of five (5) applications. The project focused on evaluating controls that directly correlate to threats and risks that may compromise the confidentiality, integrity, and availability of systems or proprietary information that reside on CFX infrastructure.

Fieldwork was performed remotely from Protiviti security labs in Philadelphia, PA between August 19, 2019 and September 13, 2019. Protiviti performed retesting of several vulnerabilities as requested by CFX to confirm successful remediation during the engagement.

Objectives and Scope

This engagement was executed with the intent of assessing existing controls within the web application that are designed to minimize the risks to the organization. As such, Protiviti attempted to identify security vulnerabilities, circumvent security controls, and to execute authorized exploits within the application. Emphasis was placed on evaluating application controls that restrict unauthorized access to the CFX applications, the data it transmits, and the critical account data (e.g. credentials, PHI data, etc.) it stores.

The scope of the security assessment included the following:

- **Web Application Security Testing (EpassWeb**) – Performed a series of security tests against the web application using automated commercial application scanning tools and web application proxies to crawl and map the target applications. Specifically, application entry points, programming languages, structure, and error codes were identified to complete the application mapping process. Protiviti leveraged the data collected from the crawling and mapping phase to perform a series of automated tests, manual tests, and validation activities to evaluate the security posture of the application.
- **Secure Source Code Review (Epass Mobile, Web API, Epass Web, VesWeb)** – Performed source code analysis using automated static code analysis tools to find potential issues within the web application source code. Protiviti then performed manual false positive analysis to validate identified vulnerabilities. Manual analysis was then performed to identify issues that were not identified during the automated process.

Impact Summary

Web application assessments are goal-driven exercises where an outside party attempts to understand and emulate a real-world attacker in order to obtain specific objectives such as data or system access. Source code review is a technical coding review where the outside party is provided with the application source code in order to identify coding flaws and verify that best practices are followed. Protiviti worked with CFX to establish the following goals and targets for this assessment:

1. Bypass authentication controls or gain unauthorized access to the in-scope application. **(Not Achieved)**
2. Escalate privileges on the application from a lower privileged user role. **(Not Achieved)**
3. Gain access to web application host systems or the internal network. **(Not Achieved)**
4. Gain access to sensitive information that directly enables the compromise of an end user. **(Not Achieved)**

Summary of Results

During this security assessment, Protiviti discovered one (1) High, one (1) Medium, and eight (8) Low priority vulnerabilities. Additionally, the team discovered two (2) Informational issues.

The following are issues rated as High or Medium identified during the assessment:

Web Application Assessment

- **Input Sanitization**

Source Code Assessment

- **Hardcoded Sensitive Information**

Strategic Recommendations

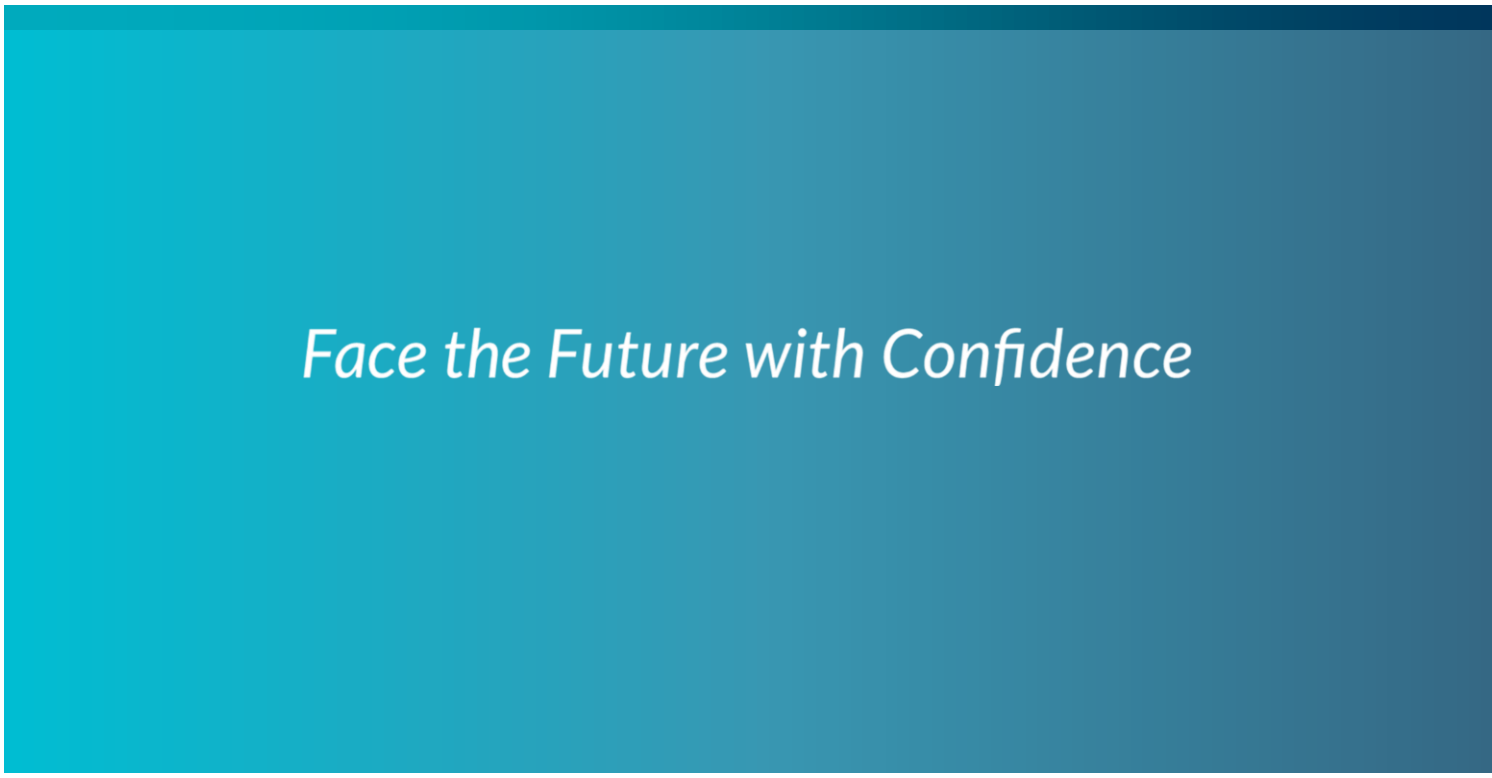
The following high-level recommendations are provided to help mitigate the risks identified in this report.

- **Application Security Architecture and Ongoing Analysis:** Perform ongoing testing of web applications prior to release on a quarterly basis.

- **Enhance Secure Coding Practices and Input Validation:** Continue to educate developers to follow secure coding best practices and techniques with a specific emphasis on input validation and output sanitization.

- **Incorporate Security into the SDLC:** Security guidelines, such as OpenSAMM, should be incorporated into the Software Development Life Cycle (SDLC) process including defining security requirements for developed applications.

It should be noted that many of Protiviti's recommendations contain instructions for specific system configuration changes (e.g., version upgrade). All recommendations should be properly evaluated and tested in a non-production environment prior to implementation on production systems. The detailed findings matrix contains a listing of findings and recommendations for this project.



protiviti®