protiviti®
Face the Future with Confidence

CENTRAL FLORIDA EXPRESSWAY AUTHORITY
PENETRATION TEST REPORT SUMMARY

October 17, 2018

Disclaimer

This report is intended solely for the use of management of Central Florida Expressway Authority (“Client” or “CFX”) and is not to be used or relied upon by others for any purpose whatsoever. This report and the related findings and recommendations detailed herein provide management with information about the condition or risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.

This report presents the results of an External and Internal Penetration Test performed by Protiviti during June 2018. The scope of the review was limited to specific target systems which were agreed upon during project scoping. This executive summary report is designed for the reader to understand the level of security assessed, to identify security deficiencies, to identify areas of strength and weakness, and to develop a course of action to correct vulnerabilities and mitigate associated risks.

Penetration testing is an uncertain process which is based upon past experiences, currently available information, and known threats. It should be understood that all information security systems, which by their nature are dependent on their human operators, are vulnerable to some degree. Therefore, while the team believes to have identified the major security vulnerabilities on the systems analyzed, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate those exposures. This report identifies known vulnerabilities that were detected during the test period; new devices, configuration changes and new/future vulnerabilities were not tested. While the matters presented herein are the result of the review, had additional procedures been performed, other matters may have been identified that would have been reported to CFX.

Additionally, this report contains information concerning potential vulnerabilities of CFX's network(s)/system(s) and methods for exploiting them. The team recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein.

protiviti®

Table of Contents

I. Executive Summary 1
Background 1
Objectives and Scope 1
Approach 2
Summary of Results 2

protiviti®

I. Executive Summary

Background

As part of the 2018 Internal Audit plan, Protiviti performed both an internal and external penetration test against systems that were not within the Payment Card Industry ("PCI") environment, nor within the Intelligent Transportation Systems ("ITS") environment. The tests focused on simulating what actions an attacker would attempt both from the internet, and from within CFX's internal network.

Fieldwork was performed remotely from Protiviti security lab in Philadelphia, PA between June 13, 2018 and June 29, 2018.

Objectives and Scope

The objective of the engagement was to present a reasonable example of what an attacker could accomplish in a similar scenario. As such, Protiviti attempted to identify security vulnerabilities, circumvent security controls, and execute authorized exploits within the organization's environment. Emphasis was placed on assessing the configurations and controls that restrict unauthorized users from accessing CFX systems and the critical business data contained therein, along with testing controls that prevent users from escalating access to other areas of CFX technology environment.

The scope of the penetration test included the following:

- **External Penetration Test** – Performed network discovery and testing against CFX's internet-facing (external) assets in an attempt to identify exploitable weaknesses by a user who did not have physical access to CFX's office and/or internal network.
- **Internal Penetration Test** – Performed network discovery and testing against CFX's internal network environment in an attempt to identify exploitable weaknesses to gain unauthorized access to systems and data.

protiviti®

Approach

Penetration testing is a goal-driven exercise where Protiviti attempts to emulate a real-world attacker in order to obtain a specific objective. Therefore, Protiviti worked with CFX to establish the following goal(s) and target(s) for this assessment:

- Access the internal network by compromising externally-accessible systems.
- Obtain Domain Administrator access to CFX's Active Directory domain(s).
- Obtain server-level access to CFX's internal systems.
- Obtain access to sensitive data on CFX systems including: intellectual capital, personally identifiable information (PII), financial data, etc.

.

Summary of Results

During this penetration test, Protiviti discovered Critical, High, and Medium priority vulnerabilities within the CFX environment. Management has already implemented actions to remediate the Critical and High priority vulnerabilities, and is currently working to remediate the Medium priority vulnerabilities.

protiviti®