# 1 Executive Security Assessment Report

## 1.1 Analysis Overview

The security assessment was conducted on the domain **tvtfcu-dc.cert.fec-dc.fiservapps.com**. The analysis commenced on **06-04** at **13:00** and concluded in **00h:09m:42s**. The assessment utilized a Basic scan type. The evaluation focused on identifying High and Medium-risk vulnerabilities within the domain's infrastructure, employing methodologies aligned with OWASP and OSCP standards.

## 1.2 Summary of Findings

The security assessment identified **1 Medium-risk**, **2 Low-risk**, and **15 informational** issues. The most significant finding is the Medium-risk exposure due to an open HTTP port (**80**) without encryption, which could lead to data interception if not redirected to HTTPS. This requires immediate attention to ensure secure data transmission. Additionally, the SSL/TLS analysis revealed that all endpoints support modern protocols, with **1** endpoint using TLS 1.3, which is ideal. The SSL certificate expiration analysis indicates that **1** domain should be monitored for renewal within **158 days**. Overall, the infrastructure shows a normal service density and no shared hosting risks, but continuous monitoring and timely updates are recommended to maintain security posture.

## 1.3 Key Security Issues

| Title | Risk |
|---|---|
| Nmap Port Scan Results Analysis | Medium |
| SSL/TLS Protocols Security Assessment | Low |
| SSL Certificate Expiration Analysis | Low |

### 1.3.1 Nmap Port Scan Results Analysis

**Description:**
The analysis identified an open HTTP port (**80**) on IP **107.162.254.112** running without encryption. This lack of encryption poses a risk of data interception unless there is a redirection to HTTPS or if HTTP Strict Transport Security (HSTS) is enabled.

**Affected Assets:**
- IP: **107.162.254.112** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

**Recommendations:**
Immediate implementation of HTTPS redirection for port **80** is advised to ensure encrypted data transmission. Enabling HSTS can further enhance security by enforcing secure connections.

### 1.3.2 SSL/TLS Protocols Security Assessment

**Description:**
The SSL/TLS protocol analysis confirmed that all endpoints support modern protocols, with one endpoint utilizing TLS 1.3, which is considered best practice for security and performance. No deprecated protocols like SSLv3, TLS 1.0, or TLS 1.1 were detected, indicating a strong security posture.

**Affected Assets:**
- **1** endpoint with TLS 1.3 support - **1** endpoint using TLS 1.2

**Recommendations:**
Maintain current protocol configurations to ensure continued compliance with best practices. Regularly review and update configurations as new vulnerabilities and recommendations emerge.

### 1.3.3 SSL Certificate Expiration Analysis

**Description:**
The SSL certificate expiration analysis revealed that the domain **tvtfcu-dc.cert.fec-dc.fiservapps.com** has **158 days** remaining until expiration, placing it in the "Monitor" category.
**Affected Assets:**
- Domain: **tvtfcu-dc.cert.fec-dc.fiservapps.com** - Expiration Date: **2025-11-09**
**Recommendations:**
Monitor the certificate expiration date closely and plan for renewal well in advance to prevent any service disruptions or security lapses.

## 1.4 General Recommendations

To maintain a robust security posture, it is crucial to implement HTTPS across all services, regularly update SSL/TLS configurations, and monitor certificate expiration dates diligently. Continuous security assessments and timely updates will help mitigate potential risks and enhance the overall security framework of the infrastructure.