Merchant Certificate of Compliance

Certificate of VERIFIED PCI Compliance

Awarded To:

Fundación Escuela Bancaria y Comercial

(7132231)

Self - Assessment Questionnaire Passed:

SAQ D, v3.2r1.1

Date Awarded:

05/07/2019

Most Recent Scan Date:

05/07/2019

Certificate Number:

05201907223101

1st SECURE IT
When compliance is not enough

This is to certify that the named merchant has completed the proper Self-Assessment Questionnaire and associated remediation activities using the ExpertPCI^{TM} program, and has been found PCI compliant per the PCI Security Standards, as set forth by the Payment Card Industry Security Standards Council and endorsed by the major payment brands.

Based upon the information provided by the merchant regarding their policies, procedures and technical systems that store, process and/or transmit cardholder data and the ASV scans of those systems (as required), the Merchant has satisfactorily met the requirements of PCI DSS on the date of issue. No other guarantees are given.

This certificate of compliance should be printed and kept on file, in the event merchant is required to show validation of PCI DSS compliance. It is the merchant's responsibility to maintain current and on-going PCI DSS compliance. If scans have been completed, current scan reports should be kept with the certificate of compliance.

1st Secure IT LLC makes no representation or warranty to any third party as to whether merchant's systems are secure or protected from attack and/or breaches, or whether cardholder data is at risk of being compromised. 1st Secure IT LLC accepts no liability to any third party in the event of loss or damage of any description, caused by any failure in or breach of merchant's security. This certificate is for the sole purpose of identifying compliance and can not be used for any other purpose.

Mark Akins **CISSP, PCI QSA**

ASV Scan Report - Attestation of Scan Compliance

1. Scan Customer Information

Company: Fundaci√≥n Escuela Bancaria y Comercial, A.C.	**Contact Name:** Anabel L√≥pez Ch√°vez	
Job Title: Administrator	**Telephone:** 91492000	
E-mail: fundacionebc@ebc.edu.mx	**Business Address:** Liverpool 54, Ju√°rez CMX	
City: Mexico	**State/Province:**	**ZIP:** 06600
Country:	**URL:**	

2. Approved Scanning Vendor Information

Company: SAINT Corporation	**Contact Name:** SAINT ASV Staff	
Job Title: IT Security Consultant	**Telephone:** 301-656-0521	
E-mail: asvstaff@saintcorporation.com	**Business Address:** 4720 Montgomery Lane Suite 800	
City: Bethesda	**State/Province:** MD	**ZIP:** 20814
Country:	**URL:** http://www.saintcorporation.com	

3. Scan Status

Date scan completed: May 7, 2019	**Scan expiration date (90 days from scan date):** Aug. 5, 2019
Compliance Status: PASS	**Scan Report Type:** Full scan
Number of unique in-scope components scanned: 1	**Number of identified failing vulnerabilities:** 0
Number of components found by ASV but not scanned because scan customer confirmed they were out of scope: 0	

4. Scan Customer Attestation

Fundaci√≥n Escuela Bancaria y Comercial, A.C. attests on May 7, 2019 that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section 3, "Scan Status") which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions including compensating controls if applicable is accurate and complete. Fundaci√≥n Escuela Bancaria y Comercial A.C. also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

Signature:____________________________ Name:______________________ Title:______________________

5. ASV Attestation

This scan and report was prepared and conducted by SAINT Corporation under certificate number 4268-01-11, according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide.
SAINT Corporation attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by SAINT ASV Staff.

SAINTwriter Assessment Report

Report Generated: May 7, 2019

1 Introduction

On May 7, 2019, at 2:01 AM, a PCI assessment was conducted using the SAINT 9.5.19 vulnerability scanner. The scan discovered a total of one live host, and detected zero critical problems, zero areas of concern, and zero potential problems. The hosts and problems detected are discussed in greater detail in the following sections.

2 Summary

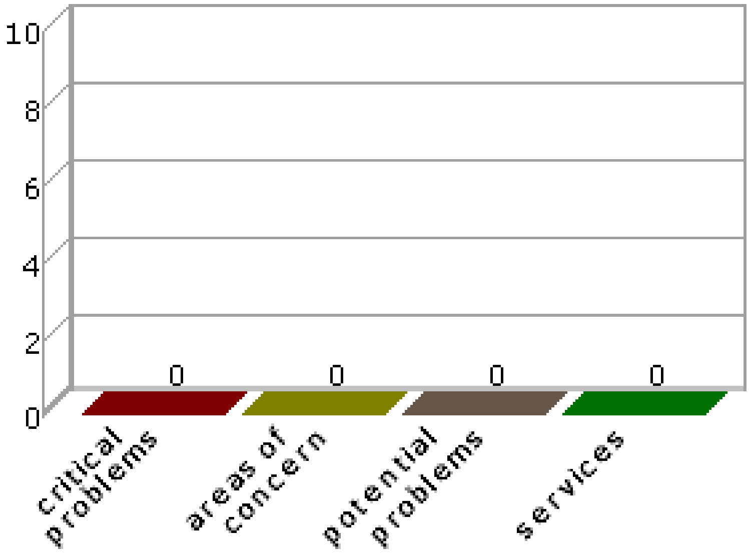
The following vulnerability severity levels are used to categorize the vulnerabilities:

> ***CRITICAL PROBLEMS***
> Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.
>
> ***AREAS OF CONCERN***
> Vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.
>
> ***POTENTIAL PROBLEMS***
> Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.
>
> ***SERVICES***
> Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The sections below summarize the results of the scan.

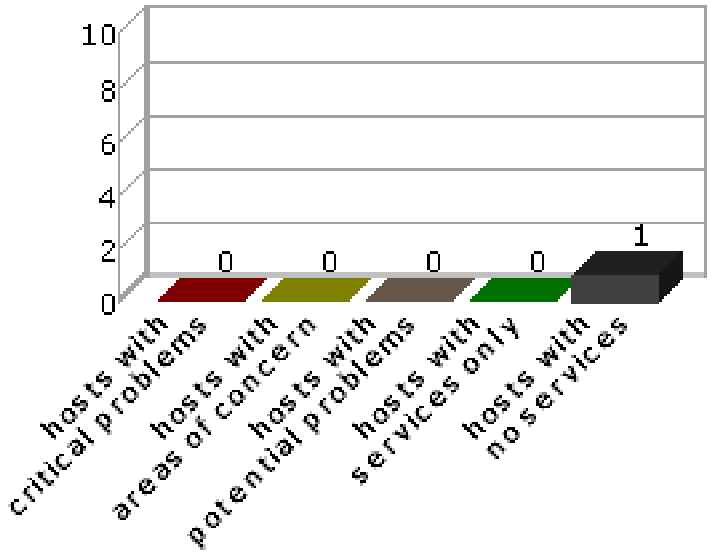
2.1 Vulnerabilities by Severity

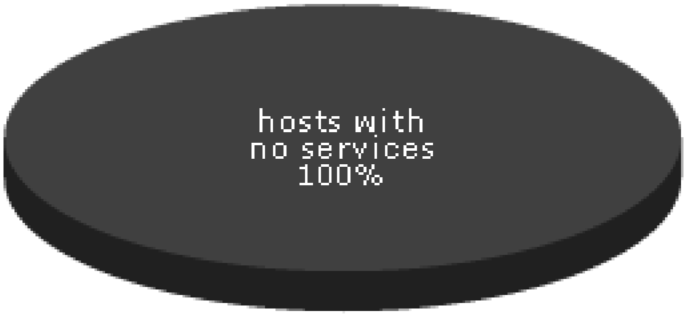
This section shows the overall number of vulnerabilities and services detected at each severity level.



2.2 Hosts by Severity

This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.

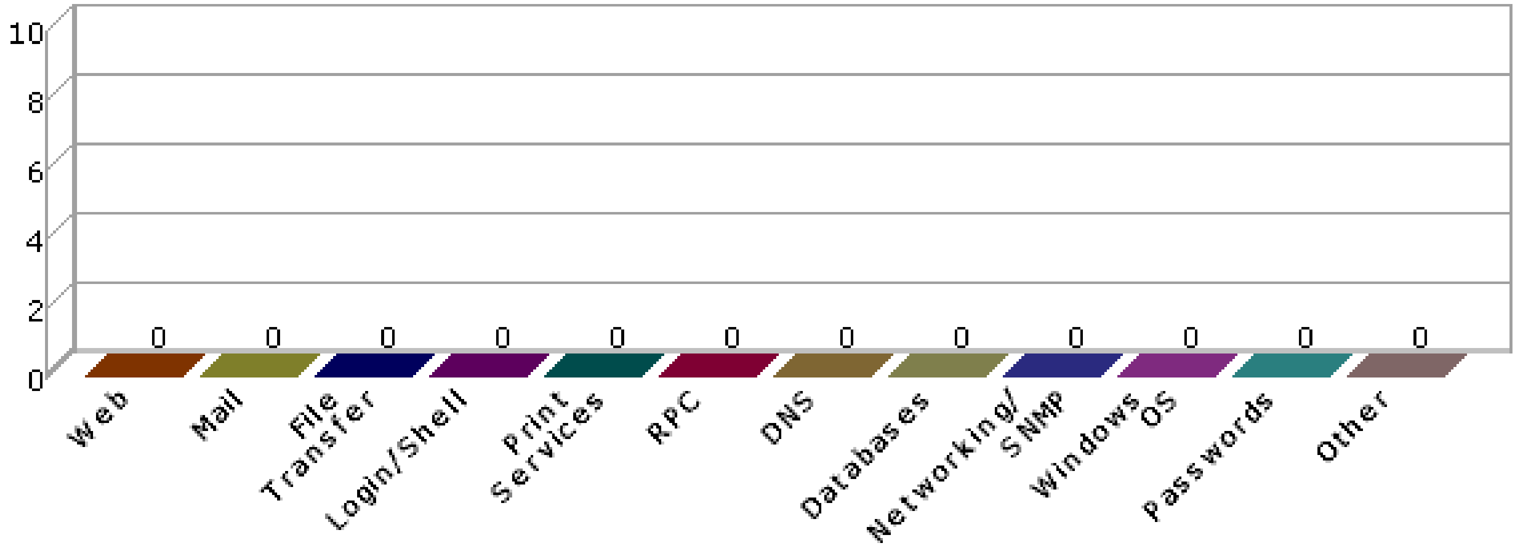




2.3 Vulnerabilities by Class

This section shows the number of vulnerabilities detected in each vulnerability class.

Class	Description
Web	Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
Mail	Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
File Transfer	Vulnerabilities in FTP and TFTP services
Login/Shell	Vulnerabilities in ssh, telnet, rlogin, rsh, or rexec services
Print Services	Vulnerabilities in lpd and other print daemons
RPC	Vulnerabilities in Remote Procedure Call services
DNS	Vulnerabilities in Domain Name Services
Databases	Vulnerabilities in database services
Networking/SNMP	Vulnerabilities in routers, switches, firewalls, or any SNMP service
Windows OS	Missing hotfixes or vulnerabilities in the registry or SMB shares
Passwords	Missing or easily guessed user passwords
Other	Any vulnerability which does not fit into one of the above classes



3 Overview

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

3.1 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type	Critical Problems	Areas of Concern	Potential Problems
201.131.12.21		201.131.12.21		0	0	0

3.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Severity	Vulnerability / Service	Class	CVE	Exploit Available?
201.131.12.21		nothing to report			

4 Details

The following sections provide details on the specific vulnerabilities detected on each host.

4.1 201.131.12.21

IP Address: 201.131.12.21
Scan time: May 07 02:01:21 2019

nothing to report

ASV Scan Report Executive Summary

Report Generated: May 7, 2019

Part 1. Scan Information

Scan Customer Company: Fundaci√≥n Escuela Bancaria y Comercial, A.C.	**ASV Company:** SAINT Corporation
Date scan was completed: May 7, 2019	**Scan expiration date:** August 5, 2019

Part 2. Component Compliance Summary

Host Name	PCI Compliant?
201.131.12.21	PASS

Part 3a. Vulnerabilities Noted for each Component

Component:Port	Vulnerability / Service	CVE	PCI Severity	CVSSv2 Base Score	PCI Compliant?	Exceptions, False positives, or Compensating Controls Noted by the ASV for this Vulnerability
201.131.12.21	nothing to report					

Part 3b. Special Notes by Component

Component	Special Note	Item Noted	Scan customer's description of action taken and declaration that software is either implemented securely or removed.

Part 3c. Special Notes - Full Text

Part 4a. Scope Submitted by Scan Customer for Discovery

- 201.131.12.21

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)

- 201.131.12.21

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)

No out-of-scope components were found.