ASV Scan Report Executive Summary

Report Generated: February 17, 2021

Part 1. Scan Information

Scan Customer Company: ABC Coffee Shop
Date scan was completed: February 17, 2021
ASV Company: SAINT Corporation
Scan expiration date: May 18, 2021

Part 2. Component Compliance Summary

Host Name	PCI Compliant?
192.0.2.15	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
192.0.2.15:80	Autocomplete enabled for password input		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:443	Load Balancer detected		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:25	Remote OS available		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:23	Remote OS available		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:80	Remote OS available		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:22	Remote OS available		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:443	Remote OS available		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:22	SSH supports weak MAC algorithms		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:25	SSL/TLS server allows anonymous key exchange		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:25	Sendmail command VRFY is enabled		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:443	TCP timestamp requests enabled		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:443	Web server default page detected		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.

192.0.2.15:80	Web server default page detected		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:80	Web site may be vulnerable to clickjacking attacks		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15:443	weak https cache policy		low	2.6	PASS	SAINT calculated its own CVSS score for this vulnerability because it was not found in the NVD.
192.0.2.15	ICMP timestamp requests enabled	CVE-1999-0524	low	0.0	PASS	

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.
192.0.2.15	Remote Access Software	Remote access ports: 22 (SSH), 23 (telnet)	These services are needed for remote administration and have been secured using host-based access controls.
192.0.2.15	Load Balancers	Load Balancer detected	The environment behind the load balancer was scanned as part of our PCI DSS internal vulnerability scans.
192.0.2.15	Anonymous (Non-authenticated) Key-agreement Protocols	Anonymous key exchange supported	Anonymous key exchange is not used in any session where TLS /SSL is used as a security control to protect cardholder data or access to the cardholder data environment.
192.0.2.15	Insecure Services / Industry-deprecated Protocols	Insecure services / Industry-deprecated protocols detected: SHA1	A firewall protects the cardholder data environment from this service.

Part 3c. Special Notes - Full Text

Remote access ports

Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, 1) justify the business need for this software to the ASV and confirm it is implemented securely, or 2) confirm it is disabled/removed. Consult your ASV if you have questions about this Special Note.

Load Balancer detected

Note to scan customer: As you were unable to validate that the configuration of the environment behind your load balancers is synchronized, it is your responsibility to ensure that the environment is scanned as part of the internal vulnerability scans required by the PCI DSS.

Anonymous key exchange supported

Note to scan customer: Due to increased risk of "man in the middle" attacks when anonymous (non-authenticated) key-agreement protocols are used, 1) justify the business need for this protocol or service to the ASV, or 2) confirm it is disabled/removed. Consult your ASV if you have questions about this Special Note.

Insecure services / Industry-deprecated protocols detected

Note to scan customer: Insecure services and industry-deprecated protocols can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, 1) justify the business need for this service and confirm additional controls are in place to secure use of the service, or 2) confirm that it is disabled. Consult your ASV if you have questions about this Special Note.

Part 4a. Scope Submitted by Scan Customer for Discovery

- 192.0.2.15

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

- 192.0.2.15

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

No out-of-scope components were found.

Scan Session: sample_scan; Scan Policy: PCI External; Scan Data Set: 17 February 2021 12:54