ASV Scan Report - Attestation of Scan Compliance

1. Scan Customer Information

Company: Southside Obgyn PC	**Contact Name:** Jocelyn Coffee	
Job Title: Administrator	**Telephone:** 317-865-3600	
E-mail: jcoffee@southsideobgyn.com	**Business Address:** 8051 South Emerson Ave Ste 400	
City: Indianapolis	**State/Province:** IN	**ZIP:** 46237
Country:	**URL:**	

2. Approved Scanning Vendor Information

Company: SAINT Corporation	**Contact Name:** Sam Kline	
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: US	**URL:** http://www.saintcorporation.com	

3. Scan Status

Date scan completed: Aug. 7, 2020	**Scan expiration date (90 days from scan date):** Nov. 5, 2020
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

Southside Obgyn PC attests on August 7, 2020 that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section 3, "Scan Status") includes all components 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. Southside Obgyn PC 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 4268-01-13, 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 Sam Kline.

Scan Session: mID297216; Scan Policy: PCI External; Scan Data Set: 7 August 2020 01:40

SAINTwriter Assessment Report

Report Generated: September 16, 2020

1 Introduction

On August 7, 2020, at 1:40 AM, a PCI External assessment was conducted using the SAINT 9.8.26 vulnerability scanner. The scan discovered a total of one live host, and detected zero critical problems, zero areas of concern, and three 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.

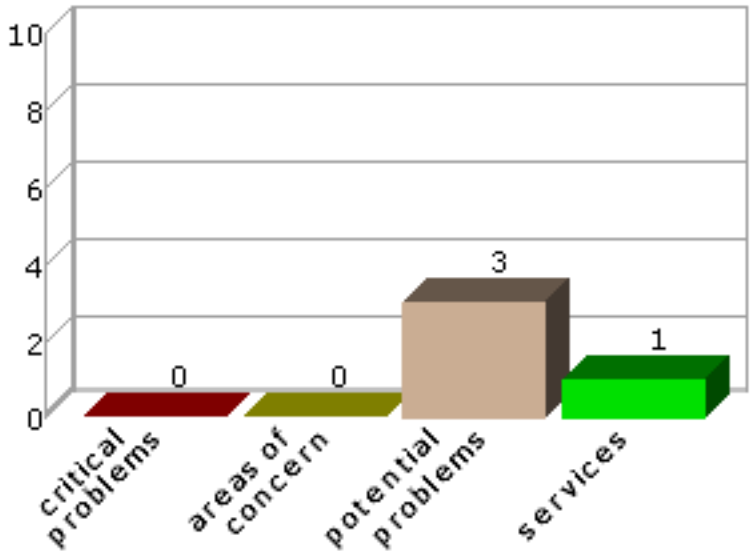
POTENTIAL PROBLEMS
Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

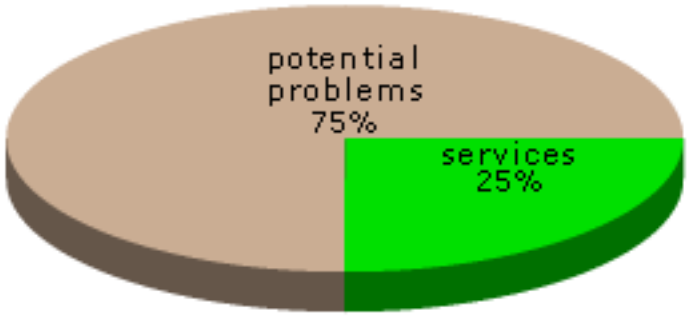
SERVICES
Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The sections below summarize the results of the scan.

2.1 Vulnerabilities by Severity

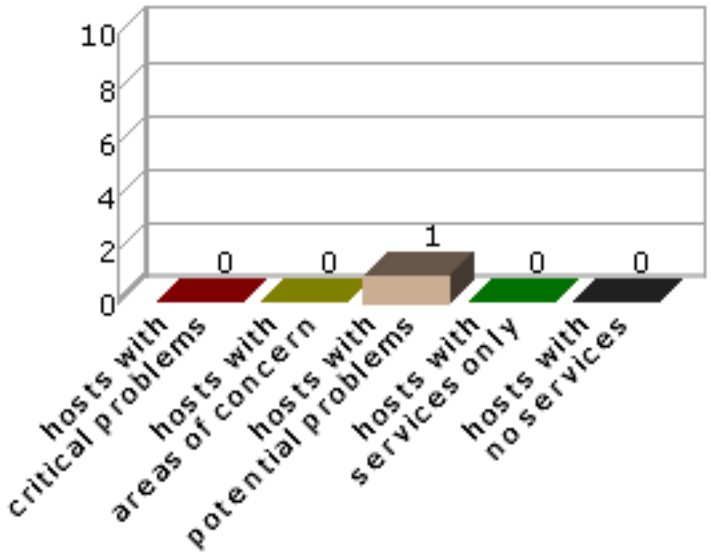
This section shows the overall number of vulnerabilities and services detected at each severity level.





2.2 Hosts by Severity

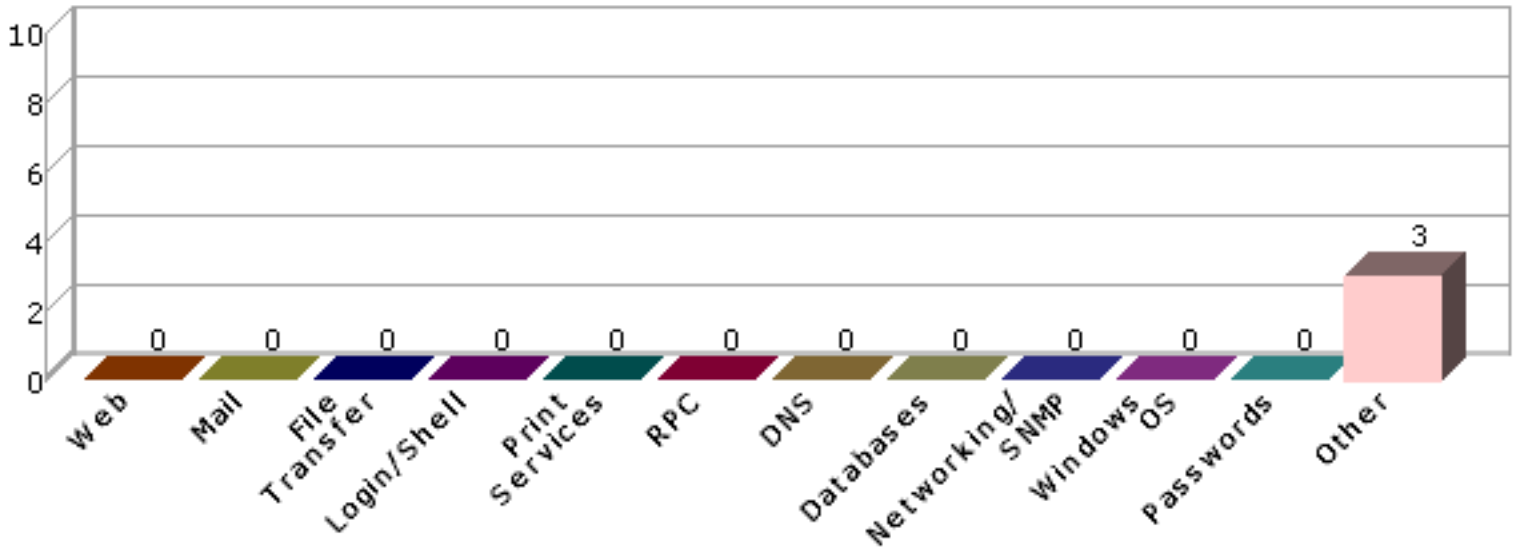
This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.

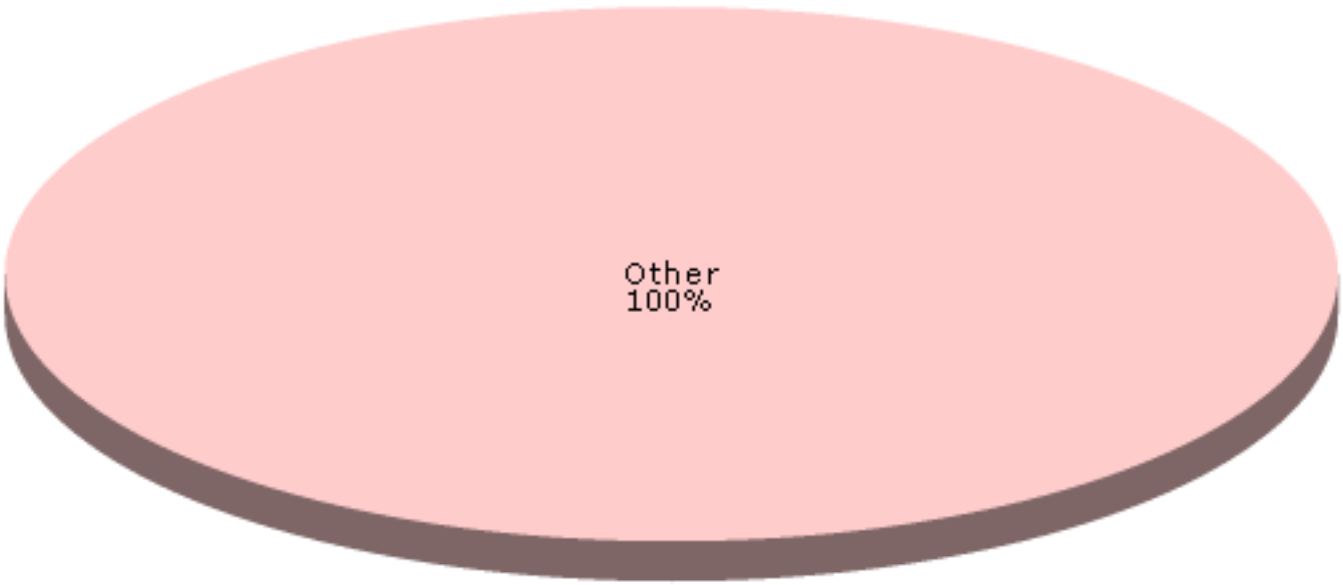


2.3 Vulnerabilities by Class

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

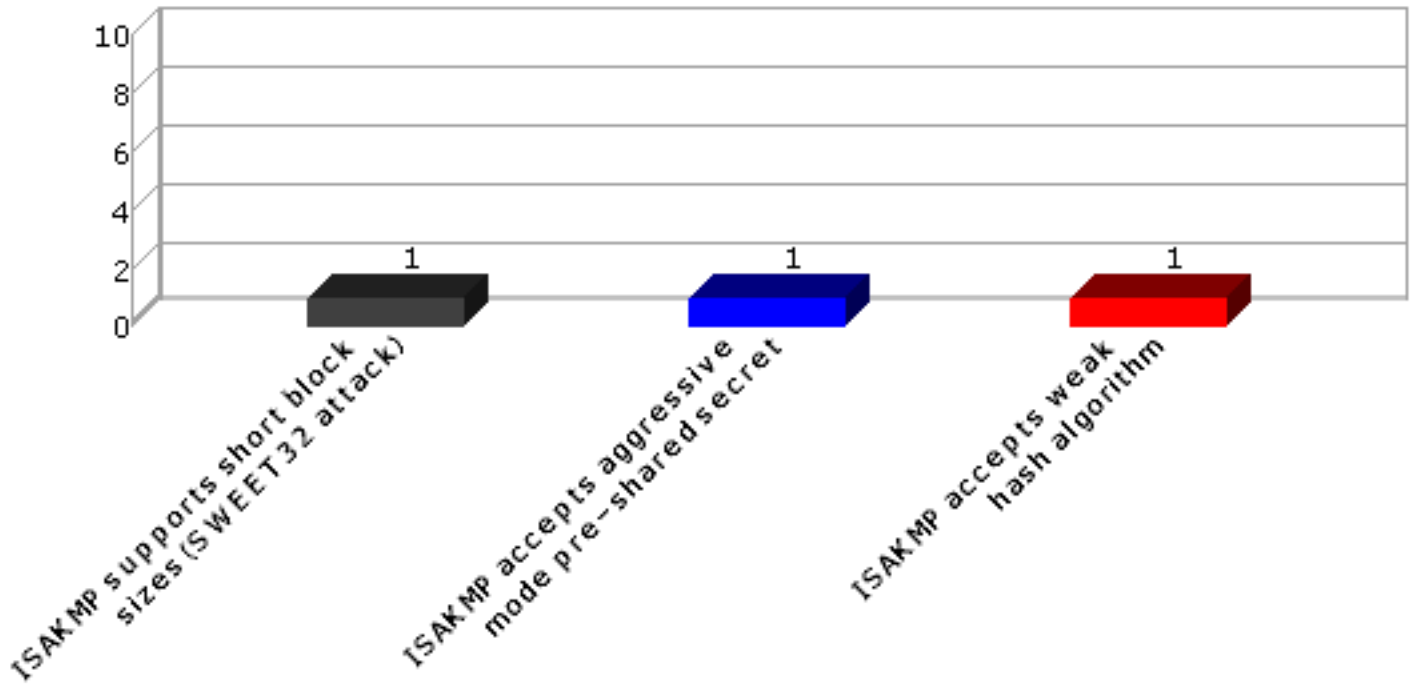
Class	Description
Web	Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
Mail	Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
File Transfer	Vulnerabilities in FTP and TFTP services
Login/Shell	Vulnerabilities in ssh, telnet, rlogin, rsh, or 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





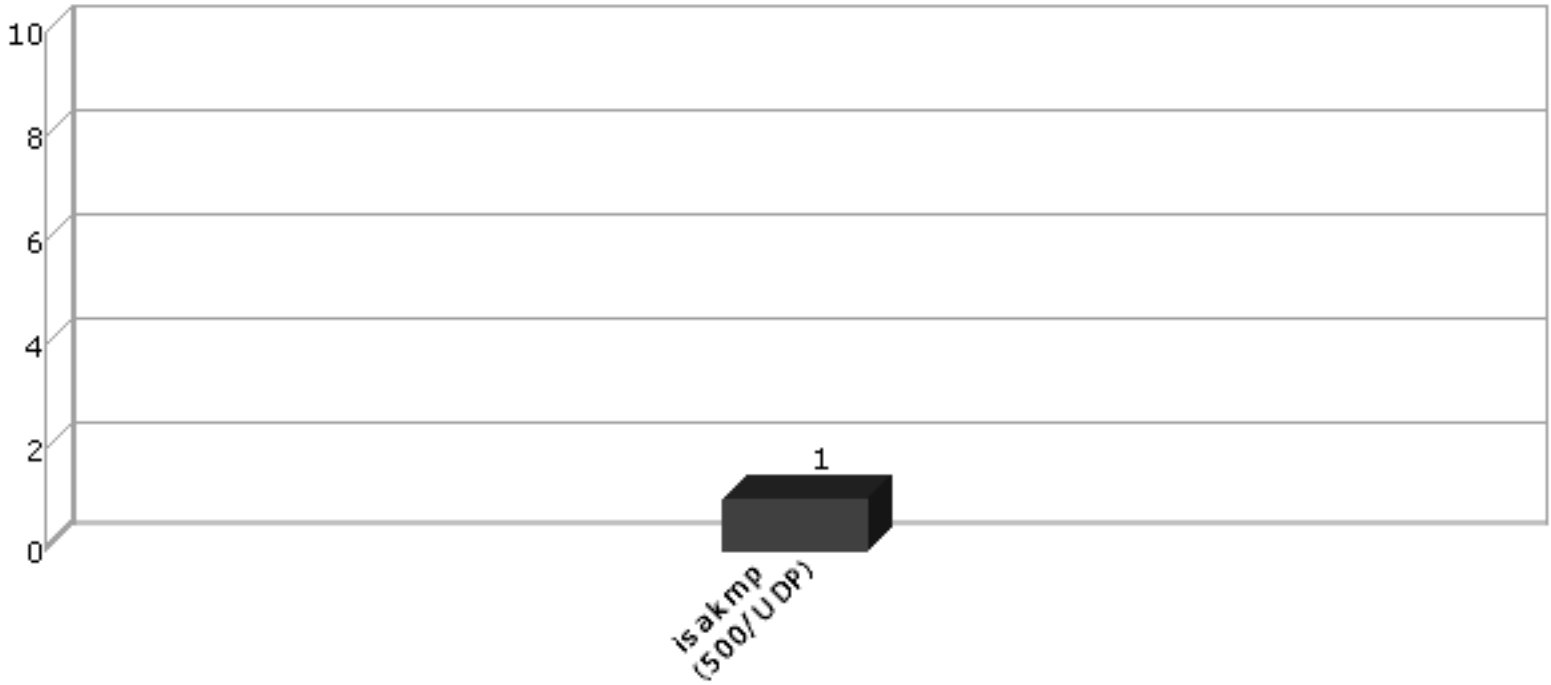
2.4 Top 10 Vulnerabilities

This section shows the most common vulnerabilities detected, and the number of occurrences.



2.5 Top 10 Services

This section shows the most common services detected, and the number of hosts on which they were detected.



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
12.158.85.210		12.158.85.210		0	0	3

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?
12.158.85.210	potential	ISAKMP accepts weak hash algorithm	Other		no
12.158.85.210	potential	ISAKMP accepts aggressive mode pre-shared secret authentication	Other	CVE-2002-1623	no
12.158.85.210	potential	ISAKMP supports short block sizes (SWEET32 attack)	Other	CVE-2016-2183	no
12.158.85.210	service	isakmp (500/UDP)			no

4 Details

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

4.1 12.158.85.210

IP Address: 12.158.85.210
Scan time: Aug 07 01:40:16 2020

ISAKMP accepts weak hash algorithm

Severity: Potential Problem

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Resolution

Configure the target machine not to accept weak encryption algorithms such as DES, weak key exchange algorithms such as Diffie-Hellman group 1 (768-bit modulus), or weak hash algorithms such as MD5 or SHA-1. On Windows, this can be done as follows:

1. From the Control Panel, go to *Administrative Tools*, then *Local Security Policy*.
2. Click on *IP Security Policies on Local Computer*.
3. Double-click on the active security policy to open its properties.
4. Go to the *General* tab, and click on the *Settings* button, then the *Methods* button.
5. Highlight any security methods whose encryption type is DES, whose Diffie-Hellman group is Low (1), or whose integrity type is MD5 or SHA-1, and either remove them, or edit them and change the vulnerable parameter. *Note:* This could break compatibility with older peers.

For Cisco, see An Introduction to IP Security (IPSec) Encryption for more information on setting strong encryption algorithms.

For other operating systems, consult the operating system's or software vendor's documentation.

References

For more information about ISAKMP and IKE, see RFC 2408 and RFC 2409.

Technical Details

Service: isakmp
Encryption Algorithm: 3DES-CBC, Hash Algorithm: SHA1, Group Description: Diffie-Hellman 1024-bit MODP, Authentication Method: pre-shared key, Life Type: seconds, Life Duration: 28800

ISAKMP accepts aggressive mode pre-shared secret authentication

Severity: Potential Problem **CVE:** CVE-2002-1623

Impact

A remote attacker with the ability to sniff network traffic could see the usernames of the initiator and responder.

Resolution

Configure the target machine not to accept Aggressive Mode exchanges with pre-shared secret authentication.

References

For more information about this vulnerability, see CERT Vulnerability Note 886601.

Technical Details

Service: isakmp
Encryption Algorithm: 3DES-CBC, Hash Algorithm: SHA1, Group Description: Diffie-Hellman 1024-bit MODP, Authentication Method: pre-shared key, Life Type: seconds, Life Duration: 28800

ISAKMP supports short block sizes (SWEET32 attack)

Severity: Potential Problem **CVE:** CVE-2016-2183

Impact

A remote attacker with the ability to sniff network traffic could decrypt long-lived sessions.

Resolution

Disable ciphers which have a 64-bit block size, such as Triple-DES as follows:

- **Apache/OpenSSL:** Upgrade to OpenSSL 1.1.0, which disables Triple-DES ciphers by default. Alternatively, upgrade to OpenSSL 1.0.1u or 1.0.2i or higher, which classify Triple-DES ciphers as MEDIUM, and insert **`!MEDIUM`** in the **`SSLCipherSuite`** directive in the appropriate web server configuration file.
- **IIS:** Disable **`DES`** and **`3DES`** ciphers as described in Microsoft Knowledge Base Article 245030.
- **OpenSSH:** Add or modify the **`Ciphers`** setting in the **`sshd_config`** file and set it to **`aes128-ctr,aes192-ctr,aes256-ctr`**.
- **Windows ISAKMP:** From the Control Panel, go to *Administrative Tools*, then *Local Security Policy*. Click on *IP Security Policies on Local Computer*. Double-click on the active security policy to open its properties. Go to the *General* tab, and click on the *Settings* button, then the *Methods* button. Highlight any security methods whose encryption type is DES or 3DES, and either remove them, or edit them and change the encryption type.
- **Cisco ISAKMP:** Enter the command **`crypto isakmp policy encryption aes-256`**. For more information see Configuring IPsec and ISAKMP.

- Other: See the documentation for the software or device for information on disabling Triple-DES.

Note: disabling Triple-DES ciphers may affect compatibility with older clients.

References

For more information on the SWEET32 attack, see sweet32.info and the BugTraq ID 92630.

Technical Details

Service: isakmp
Encryption Algorithm: 3DES-CBC, Hash Algorithm: SHA1, Group Description: Diffie-Hellman 1024-bit MODP, Authentication Method: pre-shared key, Life Type: seconds, Life Duration: 28800

isakmp (500/UDP)

Severity: Service

Technical Details

Scan Session: mID297216; Scan Policy: PCI External; Scan Data Set: 7 August 2020 01:40

ASV Scan Report Executive Summary

Report Generated: September 16, 2020

Part 1. Scan Information

Scan Customer Company: Southside Obgyn PC	**ASV Company:** SAINT Corporation
Date scan was completed: August 7, 2020	**Scan expiration date:** November 5, 2020

Part 2. Component Compliance Summary

Host Name	PCI Compliant?
12.158.85.210	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
12.158.85.210:500	ISAKMP accepts aggressive mode pre-shared secret authentication	CVE-2002-1623	medium	5.0	PASS	Merchant attests that pre-shared key is long, complex, and rotated often as recommended by Cisco as a compensating control. (SAK)
12.158.85.210:500	ISAKMP supports short block sizes (SWEET32 attack)	CVE-2016-2183	medium	5.0	PASS	Merchant attests that affected service sends/receives less than 32GB per session. (SAK)

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.
12.158.85.210	Remote Access Software	Remote access ports: 500 (isakmp)	Cisco Meraki MX Client VPN requires Aggressive Mode IKE in order to use Pre-Shared Key authentication and avoid the installation of certificates on clients. We currently use complex PSK values, and rotate the keys as often as is practical. These PSK values are always an alphanumeric value greater than 16 characters.
12.158.85.210	Insecure Services / Industry-deprecated Protocols	Insecure services / Industry-deprecated protocols detected: SHA1	Cisco Meraki MX Client VPN requires Aggressive Mode IKE in order to use Pre-Shared Key authentication and avoid the installation of certificates on clients. We currently use complex PSK values, and rotate the keys as often as is practical. These PSK values are always an alphanumeric value greater than 16 characters.

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.

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

- 12.158.85.210

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

- 12.158.85.210

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

No out-of-scope components were found.

Scan Session: mID297216; Scan Policy: PCI External; Scan Data Set: 7 August 2020 01:40