PCI Scan Vulnerability Report

SYSNET GLOBAL SOLUTIONS
a VIKINGCLOUD® company
APPROVED SCANNING VENDOR

PCI Status

The following table highlights the overall compliance status and each individual system's compliance status. Following the table is a detailed report specifying each system and its specific vulnerabilities.

Overall PCI Status	FAIL

Live IP Address Scanned	PCI Status
194.32.83.74	FAIL

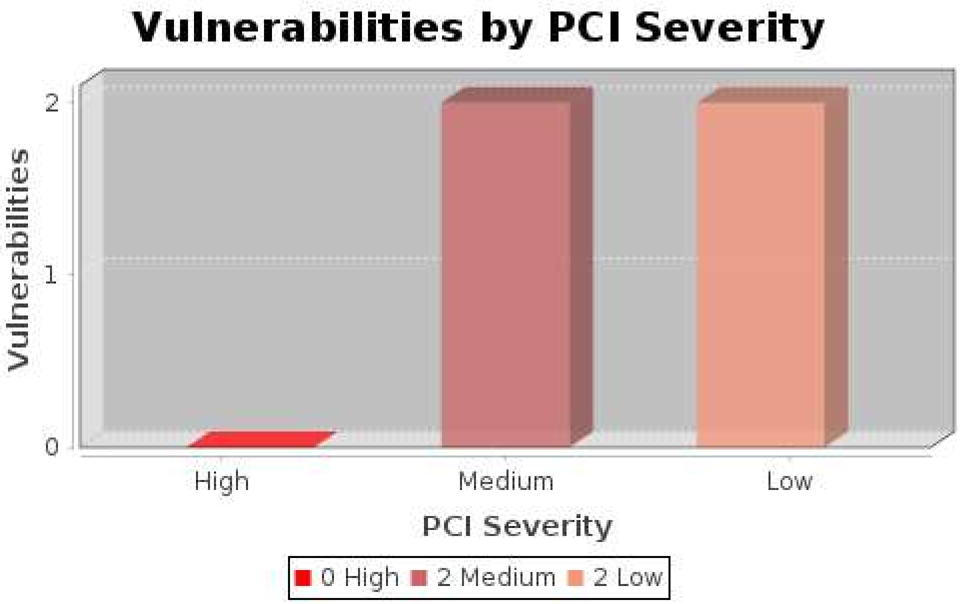
Report Summary	
Company:	RJW Phipp and Sons Ltd
Hosts in account	1
Hosts scanned	1
Hosts active	1
Scan date	October 08, 2025
Report date	October 08, 2025

Vulnerabilities by PCI Severity

Vulnerabilities total:	4

by PCI Severity

PCI Severity	**Total**
High	0
Medium	2
Low	2
Total	4



Detailed Results

194.32.83.74 (194.32.83.74,)

Vulnerabilities total:	4

Vulnerabilities (4)

Scanner Info port null/null

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2022-6487
Category:	Information
CVE ID:	-
Vendor Reference:	-
Last Update:	2022-06-10 13:32:42.0

THREAT:

Scanner Info

SOLUTION:

Scanner Info

EVIDENCE:

Target IP: 194.32.83.74

Scanner IP: ["10.200.0.80"]

Current Time: 08/10/2025 20:31

Framework Version: 10.83.0

CVT Version: 1.60.0

Carrier Version: 1.161.0

Enumerated Transform Set Information for VPN Device port 500/udp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**0.0** AV:N/AC:L/Au:N/C:N/I:N/A:N
Severity:	**low**
SLID:	SLID-2013-0565
Category:	Host Fingerprinting
CVE ID:	-
Vendor Reference:	-
Last Update:	2020-11-06 01:16:45.0

THREAT:

The following transform sets were identified on this VPN device.

SOLUTION:

This is an informational finding. No action is required, but if you wish to limit the transform sets it use, it may require configuration changes in the services configuration, which will vary by VPN technology.

EVIDENCE:

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: pre-shared key, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: pre-shared key, DH Group: Group 5

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: pre-shared key, DH Group: Group 14

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: RSA signatures, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: RSA signatures, DH Group: Group 5

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: RSA signatures, DH Group: Group 14

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: Checkpoint Hybrid, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: Checkpoint Hybrid, DH Group: Group 5

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: Checkpoint Hybrid, DH Group: Group 14

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: GSS or XAUTH1, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: GSS or XAUTH1, DH Group: Group 5

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: GSS or XAUTH1, DH Group: Group 14

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH2, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH2, DH Group: Group 5

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH2, DH Group: Group 14

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH5, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH5, DH Group: Group 5

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH5, DH Group: Group 14

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH6, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH6, DH Group: Group 5

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH6, DH Group: Group 14

Remote Access Service Detected port 500/udp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**6.3** CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
Severity:	**medium**
SLID:	SLID-2015-0447
Category:	Remote Access Service
CVE ID:	-
Vendor Reference:	-
Last Update:	2019-09-18 17:32:17.0

THREAT:
One or more remote access services were detected on the remote host. As defined by the PCI ASV Program Guide: "remote access software includes, but is not limited to: VPN (IPSec, PPTP, SSL), pcAnywhere, VNC, Microsoft Terminal Server, remote web-based administration, ssh, Telnet."

SOLUTION:
Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per PCI DSS requirement 8 or disabled/ removed.

EVIDENCE:
N/A

Weak Diffie-Hellman groups identified on VPN Device port 500/udp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

This vulnerability is not recognized in the National Vulnerability Database.

VULNERABILITY DETAILS

CVSS Base Score:	**6.5** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
Severity:	**medium**
SLID:	SLID-2015-0179
Category:	Weak Cryptography
CVE ID:	-
Vendor Reference:	-
Last Update:	2021-09-21 15:39:08.0

THREAT:

Diffie-Hellman Groups 1 to 4 are no longer considered safe for strong encryption. It is estimated that these groups have a security level of 80-90 bits which is no longer adequate to protect the encryption keys used during IKE phase 2. Furthermore, Group 5 (Modp-1536) has a security level of 120 bits which is slightly under to protect AES-128 encryption keys. Stronger groups have been designed for the Diffie-Hellman key exchange in RFC 3526.

SOLUTION:

Use Diffie-Hellman Key Exchange Group 5 or higher where possible, or the highest available to the VPN endpoints.

EVIDENCE:

```
Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: pre-shared key, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: RSA signatures, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: Checkpoint Hybrid, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: GSS or XAUTH1, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH2, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH5, DH Group: Group 2

Transform Set:: Mode: Main, Encryption: AES, Key Length: 256, Hash type: SHA, Auth method: XAUTH6, DH Group: Group 2
```

Appendices

Hosts Scanned

194.32.83.74

Hosts Not Alive

Report Legend

Payment Card Industry (PCI) Status

An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards. A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host.

An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards. A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host.

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.