

# PCI DSS Scan Report Executive Summary

Scan Customer Information				Approved Scanning Vendor Information			
Company:	MEDIATION INFORMATION RES			Company:	Sysnet		
Contact:	R.I.S.	Title:		Contact:	Terry Johnson	Title:	ASV
Telephone:	5413451629	Email:	managed-services@sysnet.ie	Telephone:	+35314951300	Email:	Terry.Johnson@sysnetgs.com
Business adress:	1234 PEARL ST STE 4 EUGENE OR 97401-3642			Business adress:	4th Floor The Herbert Building Carrickmines Dublin 18 Republic Of Ireland		
URL:				URL:	www.sysnetglobalsolutions.com		
MID:	8003176438						

### Scan status:

- \* Compliance status: PASS
- \* Number of unique components scanned: 1
- \* Number of identified failing vulnerabilities: 0
- \* Number of components found by ASV but not scanned because scan customer confirmed components were out of scope: 6
- \* Date scan completed: March 31, 2017
- \* Scan expiration date (90 days from date scan completed): June 29, 2017

### Scan Customer Attestation

MEDIATION INFORMATION RES attests on April 03, 2017 that this scan 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 is accurate and complete. MEDIATION INFORMATION RES also acknowledges the following:

1. proper 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.

### ASV Attestation

This scan and report was prepared and conducted by Sysnet under certificate number 3937-01-11, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. Sysnet 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, and 3) active scan interference. This report and any exceptions were reviewed by Terry Johnson

## ASV Scan Report Executive Summary

Part 1. Scan Information			
Scan Customer Company:	MEDIATION INFORMATION RES	ASV Company:	Sysnet
Date scan was completed:	March 31, 2017	Scan expiration date:	June 29, 2017

Part 2. Component Compliance Summary	
IP Address: 174.129.234.29	<span style="background-color: green; color: white; padding: 5px 10px;">PASS</span>

Part 3a. Vulnerabilities Noted for each IP Address					
IP Address	Vulnerabilities noted per IP address	Severity level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
174.129.234.29	42432 - Possible Scan Interference	MED	4	PASS	Customer confirmed, no Active Protection System is present or blocking the scan, approved false positive.

Part 3b. Special Notes by IP Address				
IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
-	-	-	-	-

Report Summary	
Company:	MEDIATION INFORMATION RES
Hosts in account	1
Hosts scanned	1
Hosts active	1
Scan date	March 31, 2017
Report date	April 03, 2017

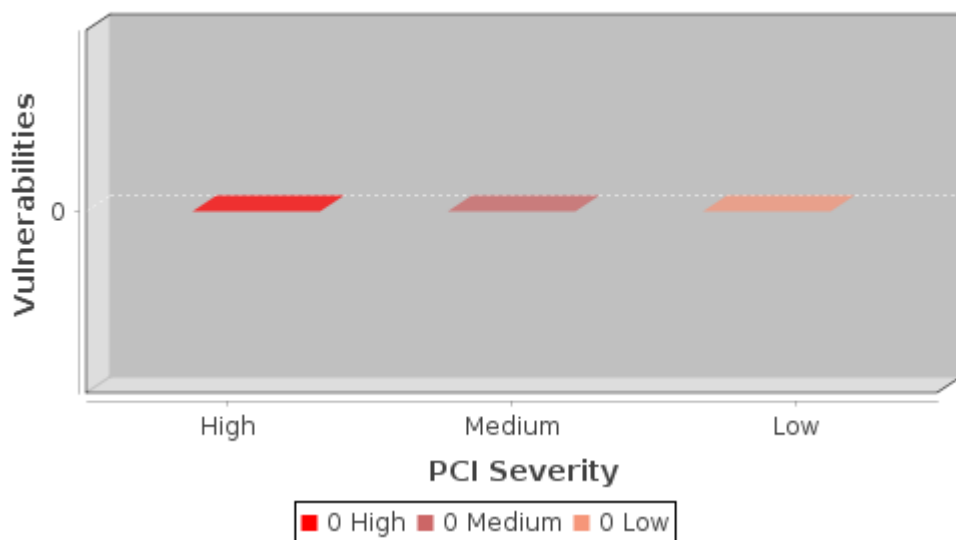
## Summary of Vulnerabilities

Vulnerabilities total:	15	Security risk:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
------------------------	----	----------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	---

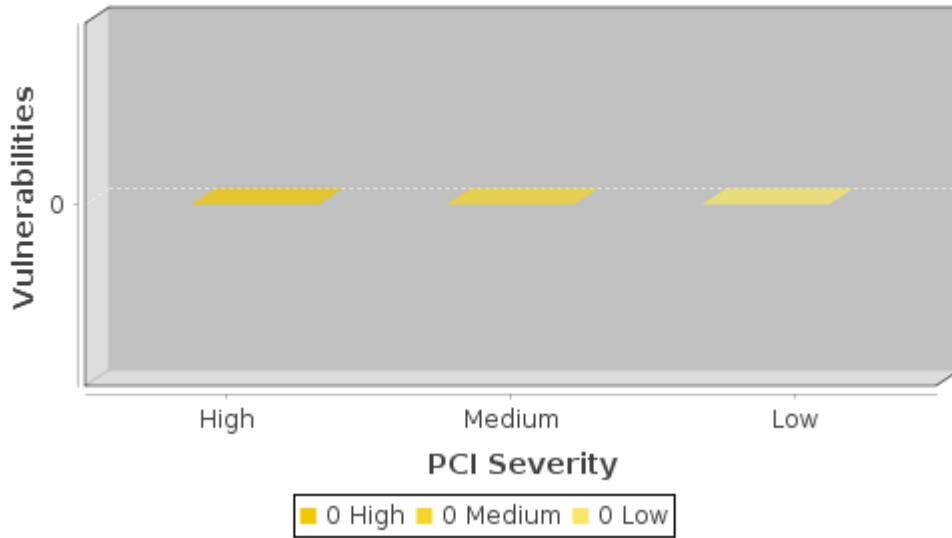
by Severity				
Severity	Confirmed	Potential	Information gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	0	0
2	0	0	2	2
1	0	0	13	13
Total	0	0	15	15

by PCI Severity			
PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	0	0	0
Low	0	0	0
Total	0	0	0

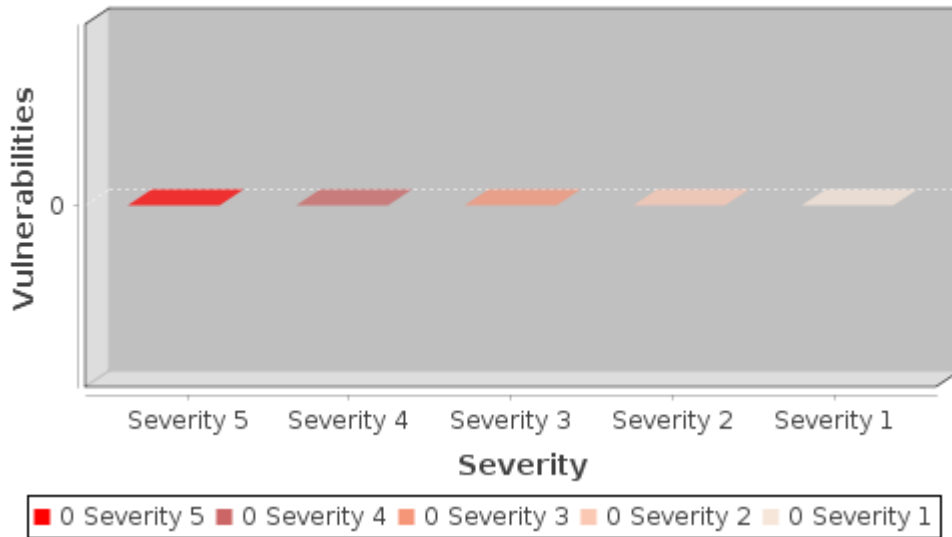
## Vulnerabilities by PCI Severity



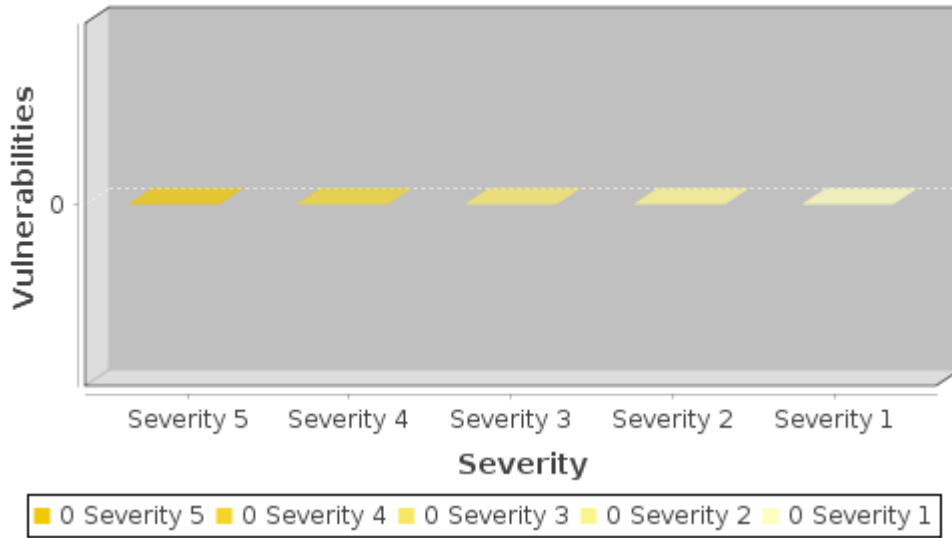
## Potential Vulnerabilities by PCI Severity



## Vulnerabilities by Severity



## Potential Vulnerabilities by Severity



Appendices

Hosts Scanned
174.129.234.29

Hosts Not Alive

Option Profile

Scan	
Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing	Standard
Vulnerability Detection	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off

Advanced	
Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

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
	1 Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
	2 Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	3 Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4 Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5 Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.




Severity	Level	Description
	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.
	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

### Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.




Severity	Level	Description
	1 Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
	2 Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
	3 Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
	4 Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
	5 Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.



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

### Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
	1 Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
	2 Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
	3 Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.