

Payment Card Industry (PCI) Executive Report

11/21/2024

ASV Scan Report Attestation of Scan Compliance

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	Prymera Consulting Private Limited			Company:	Sectigo Limited		
Contact Name:	Dhruv Patel	Job Title:		Contact Name:	-	Job Title:	-
Telephone:		Email:	dhruv@remitso.com	Telephone:	-	Email:	-
Business Address:	Unit No 10, 16th Floor, Aurora Waterfront,			Business Address:	3rd Floor Building 26, Office Village Exchange Quay, Trafford Road		
City:	Kolkata	State/Province:		City:	Salford	State/Province:	None
ZIP/postal code:		Country:	India	ZIP/postal code:	M5 3EQ	Country:	United Kingdom
URL:				URL:	https://sectigo.com/		

A.3 Scan Status			
Date scan completed	11/21/2024	Scan expiration date (90 days from date scan completed)	02/19/2025
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 components were out of scope			0

A.4 Scan Customer Attestation

Prymera Consulting Private Limited attests on 11/21/2024 at 18:50:23 GMT that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.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.

Prymera Consulting Private Limited 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.

A.5 ASV Attestation

This scan and report was prepared and conducted by Sectigo Limited under certificate number 4172-01-17, according to internal processes that meet PCI DSS requirement 11.3.2 and the ASV Program Guide.

Sectigo Limited 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 N/A

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company:	Prymera Consulting Private Limited	ASV Company:	Sectigo Limited
Date scan was completed:	11/21/2024	Scan expiration date:	02/19/2025









Part 2. Component Compliance Summary

54.163.109.116, app.demo.remitso.com

PASS

Part 2. Component Compliance Summary - (Hosts Not Current)

Part 3a. Vulnerabilities Noted for each Component

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls <small>Noted by the ASV for this Vulnerability</small>
54.163.109.116, app.demo.remitso.com	38904 - OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent CVE-2023-38408	 HIGH	9.8	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com	42046 - OpenSSH Remote Unauthenticated Code Execution Vulnerability (regreSSHion) CVE-2024-6387	 HIGH	8.1	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com	38919 - OpenSSH Authentication Bypass Vulnerability CVE-2023-51767	 HIGH	7	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com	38915 - OpenSSH OS Command Injection Vulnerability CVE-2023-51385	 MED	6.5	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com	38928 - OpenSSH Incomplete Constrains Sensitive Information Disclosure Vulnerability CVE-2023-51384	 MED	5.5	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com	38903 - OpenSSH Probable User Enumeration Vulnerability CVE-2016-20012	 MED	5.3	PASS	The software version installed is not vulnerable.
54.163.109.116, app.demo.remitso.com port 22/tcp	38909 - SHA1 deprecated setting for SSH	 LOW	3.7	PASS	The vulnerability is not included in the NVD. ASV Score = 3.7
54.163.109.116, app.demo.remitso.com	38900 - OpenSSH Public-Key Authentication Vulnerability CVE-2021-36368	 LOW	3.7	PASS	

Part 3b. Special Notes to Scan Customer by Component

Component	Special Note to Scan Customer	Item Noted	Per section 7.2 of the ASV Program Guide, scan customer's description of action taken and declaration that software is either needed for business and implemented securely, or removed

54.163.109.116	Embedded links or code from out-of-scope domains	150010 - External Links Discovered (Web Application: port 80/tcp)	<p>Yes - Actions Taken to Address Identified Risks Content Delivery Network (CDN):</p> <p>Verified the authenticity and security of cdnjs.cloudflare.com as a trusted source. Considered self-hosting critical external resources (e.g., animate.min.css) to eliminate dependency on third-party CDNs. Google reCAPTCHA:</p> <p>Evaluated the API key configuration to ensure it complies with data protection regulations. Restricted API usage to specific domains to prevent abuse. Documentation Links:</p> <p>Confirmed that links to documentation (cakephp.org) are for developer reference only and do not impact production security. Google Fonts:</p> <p>Evaluated the feasibility of self-hosting required fonts to reduce dependency on external services. General Safeguards:</p> <p>Implemented Subresource Integrity (SRI) for external scripts and styles where applicable. Enforced HTTPS for all external resources to ensure secure transmission. Reviewed and updated the Content Security Policy (CSP) to restrict access to trusted domains only.</p>
54.163.109.116	Embedded links or code from out-of-scope domains	150010 - External Links Discovered (Web Application: port 443/tcp)	<p>Yes - Actions Taken to Address Identified Risks Content Delivery Network (CDN):</p> <p>Verified the authenticity and security of cdnjs.cloudflare.com as a trusted source. Considered self-hosting critical external resources (e.g., animate.min.css) to eliminate dependency on third-party CDNs. Google reCAPTCHA:</p> <p>Evaluated the API key configuration to ensure it complies with data protection regulations. Restricted API usage to specific domains to prevent abuse. Documentation Links:</p> <p>Confirmed that links to documentation (cakephp.org) are for developer reference only and do not impact production security. Google Fonts:</p> <p>Evaluated the feasibility of self-hosting required fonts to reduce dependency on external services. General Safeguards:</p> <p>Implemented Subresource Integrity (SRI) for external scripts and styles where applicable. Enforced HTTPS for all external resources to ensure secure transmission. Reviewed and updated the Content Security Policy (CSP) to restrict access to trusted domains only.</p>
54.163.109.116	Remote Access	42017 - Remote Access or Management Service Detected (SSH:port 22/TCP)	<p>Yes - SSH access is now limited to specific IP addresses belonging to authorized system administrators.</p>

Part 3c. Special Notes Full Text

Note

Embedded links or code from out-of-scope domains

Special Note to Scan Customer: Due to increased risk to the cardholder data environment when embedded links redirect traffic to domains outside the merchant's CDE scope, 1) confirm that this code is obtained from a trusted source, that the embedded links redirect to a trusted source, and that the code is implemented securely, or 2) confirm that the code has been removed. Consult your ASV if you have questions about this Special Note.

Remote Access

Special Note to Scan Customer: 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 confirm it is implemented securely, or 2) confirm it is disabled/ removed. Consult your ASV if you have questions about this Special Note.

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Addresses/ranges/subnets, domains, URLs, etc.

54.163.109.116

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

IP Addresses/ranges/subnets, domains, URLs, etc.

54.163.109.116, app.demo.remitso.com

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

IP Addresses/ranges/subnets, domains, URLs, etc.

Evaluation

IP Addresses/Ranges : - (not active) Scan customer attests that this IP address is not issued/assigned to any physical or virtual host. ASV confirmed it is nonresponsive.

Evaluation

Report Summary

Company:	Prymera Consulting Private Limited
Hosts in Account:	1 IP
Hosts Active:	1
Hosts Scanned:	1
Scan Date:	11/21/2024 at 10:56:23 GMT
Report Date:	11/21/2024 at 18:50:27 GMT
Report Title:	PCI Scan
Template Title:	Payment Card Industry (PCI) Executive Report

Summary of Vulnerabilities

Vulnerabilities Total	53	Average Security Risk		2.0
-----------------------	----	-----------------------	---	-----

by Severity

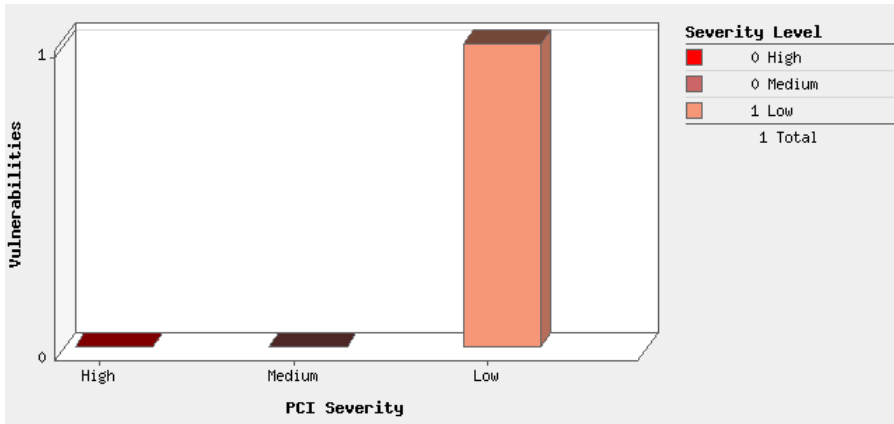
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	2	2
2	1	1	4	6
1	0	0	45	45
Total	1	1	51	53

by PCI Severity

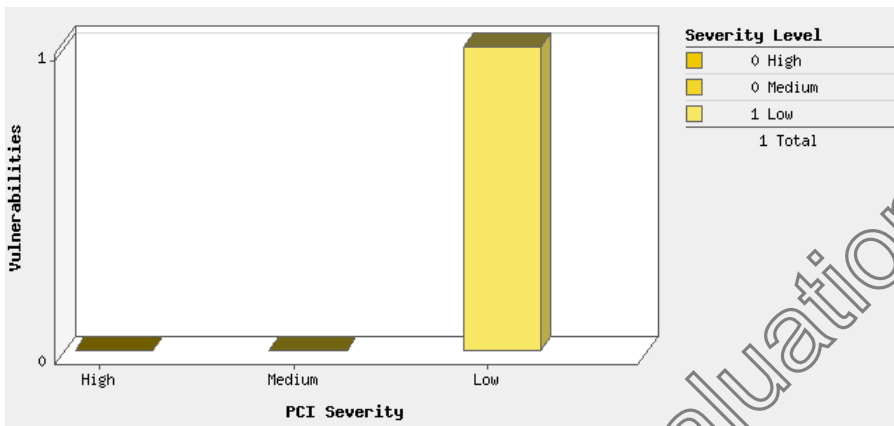
PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	0	0	0
Low	1	1	2
Total	1	1	2

Evaluation

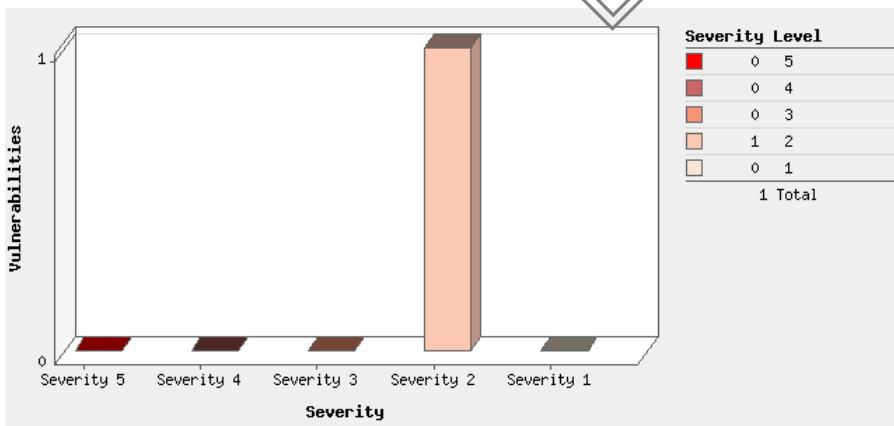
Vulnerabilities by PCI Severity



Potential Vulnerabilities by PCI Severity

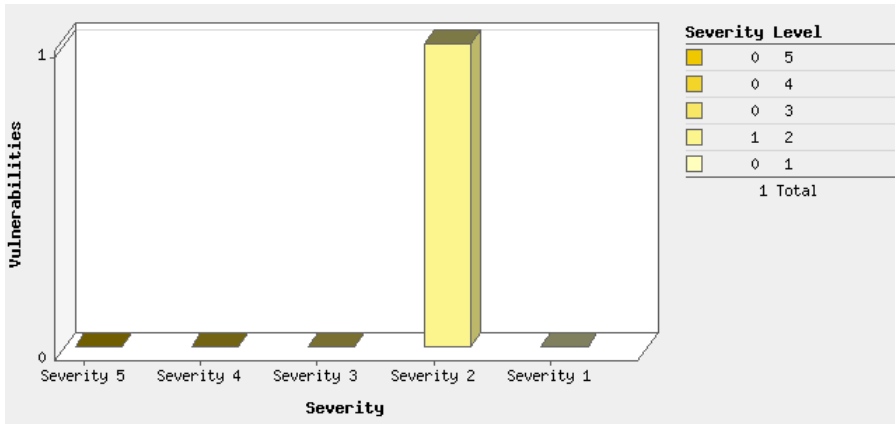


Vulnerabilities by Severity



Evaluation

Potential Vulnerabilities by Severity



Evaluation

Appendices

Hosts Scanned

54.163.109.116

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

Evaluation

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	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.

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	<p>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.</p>
	4	<p>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.</p>
	5	<p>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.</p>

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.

Evaluation