PCI ASV Vulnerability Scan Report

Executive Summary

Table of Contents

Appendix A: ASV Scan Report Attestation of Scan Compliance

A.1 Scan Customer Information

Company:	Genpact
Contact Name:	Ankur Shrivastava
Job Title:	

Telephone:	E-mail:	ankur.shrivastava@genpact.com

Business Address:		
City:	State/Province:	ZIP/Postal code:
Country: India		
Website/URL:		

A.2 Approved Scanning Vendor Information

Company:	ControlCase
Contact Name:	ControlCase ASV Team
Job Title:	

Telephone: +1 703 483 6383	E-mail:	asv@controlcase.com

Business Address:	12015 Lee Jackson Memorial Hwy Suite 520	
City: Fairfax	State/Province: VA	ZIP/Postal code: 22033
Country:		
Website/URL: www.controlcase.com		

A.3 Scan Status

Date scan completed: October 30, 2020 (GMT)	Scan expiration date (90 days from date scan completed) : January 28, 2021 (GMT)

Compliance Status: ☒ **Pass**	Scan report type:	☒ Full Scan ☐ Partial scan or rescan
Number of unique in-scope components scanned:		26
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

A.4 Scan Customer Attestation

Genpact attests on October 30, 2020 (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. Genpact 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 ControlCase under certificate number 4250-01-13, according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide. ControlCase 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 ControlCase.

Appendix B: ASV Scan Report Summary

Part 1. Scan Information			
Scan Customer Company:	Genpact	ASV Company:	ControlCase
Date scan was completed:	October 30, 2020	Scan expiration date:	January 28, 2021

Part 2. Component Compliance Summary			
IP Address:	38.142.188.30	☒ **Pass**	☐ **Fail**
IP Address:	69.174.28.138	☒ **Pass**	☐ **Fail**
IP Address:	59.160.97.246	☒ **Pass**	☐ **Fail**
IP Address:	202.54.240.182	☒ **Pass**	☐ **Fail**
IP Address:	125.21.0.182	☒ **Pass**	☐ **Fail**
IP Address:	125.21.44.66	☒ **Pass**	☐ **Fail**
IP Address:	182.19.62.165	☒ **Pass**	☐ **Fail**
IP Address:	122.15.135.129	☒ **Pass**	☐ **Fail**
IP Address:	216.195.64.30	☒ **Pass**	☐ **Fail**
IP Address:	216.195.64.34	☒ **Pass**	☐ **Fail**
IP Address:	4.59.196.78	☒ **Pass**	☐ **Fail**
IP Address:	67.154.112.26	☒ **Pass**	☐ **Fail**
IP Address:	50.207.117.50	☒ **Pass**	☐ **Fail**
IP Address:	12.125.232.106	☒ **Pass**	☐ **Fail**
IP Address:	122.55.2.142	☒ **Pass**	☐ **Fail**
IP Address:	222.127.146.122	☒ **Pass**	☐ **Fail**
IP Address:	32.6.166.114	☒ **Pass**	☐ **Fail**
IP Address:	32.6.166.118	☒ **Pass**	☐ **Fail**
IP Address:	121.241.98.81	☒ **Pass**	☐ **Fail**
IP Address:	125.23.240.158	☒ **Pass**	☐ **Fail**
IP Address:	115.114.73.26	☒ **Pass**	☐ **Fail**
IP Address:	32.6.185.174	☒ **Pass**	☐ **Fail**
IP Address:	32.6.185.182	☒ **Pass**	☐ **Fail**
IP Address:	32.6.185.186	☒ **Pass**	☐ **Fail**
IP Address:	12.87.39.214	☒ **Pass**	☐ **Fail**
IP Address:	157.130.132.82	☒ **Pass**	☐ **Fail**

Part 3a. Vulnerabilities Noted for each Component

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score[1]	Compliance Status Pass	Compliance Status Fail	Exceptions, False Positives, or Compensating Controls
38.142.188.30 : 500	Pre-shared Key Off-line Bruteforcing Using IKE Aggressive Mode	■ Low	5	☒	☐	Genpact - Global confirmed ControlCase that strong pre-shared key is being used, hence passed.
38.142.188.30	ICMP Replies Received	■ Low	0.0	☒	☐	
38.142.188.30	Host Name Not Available	■ Low	0.0	☒	☐	
38.142.188.30	DNS Host Name	■ Low	0.0	☒	☐	
38.142.188.30	Traceroute	■ Low	0.0	☒	☐	
38.142.188.30	Target Network Information	■ Low	0.0	☒	☐	
38.142.188.30	Internet Service Provider	■ Low	0.0	☒	☐	
38.142.188.30	Host Scan Time	■ Low	0.0	☒	☐	
38.142.188.30	Scan Activity per Port	■ Low	0.0	☒	☐	
38.142.188.30	Remote Access or Management Service Detected	■ Low	0.0	☒	☐	
38.142.188.30	Open UDP Services List	■ Low	0.0	☒	☐	
38.142.188.30	Firewall Detected	■ Low	0.0	☒	☐	
38.142.188.30	ICMP Timestamp Request	■ Low	0.0	☒	☐	
Consolidated Solution/Correction Plan for above Component:						
59.160.97.246	ICMP Replies Received	■ Low	0.0	☒	☐	
59.160.97.246	DNS Host Name	■ Low	0.0	☒	☐	
59.160.97.246	Traceroute	■ Low	0.0	☒	☐	
59.160.97.246	Target Network Information	■ Low	0.0	☒	☐	
59.160.97.246	Internet Service Provider	■ Low	0.0	☒	☐	
59.160.97.246	Host Names Found	■ Low	0.0	☒	☐	
59.160.97.246	Host Scan Time	■ Low	0.0	☒	☐	
59.160.97.246	Firewall Detected	■ Low	0.0	☒	☐	
59.160.97.246	ICMP Timestamp Request	■ Low	0.0	☒	☐	

Consolidated Solution/Correction Plan for above Component:

202.54.240.182	ICMP Replies Received	🟩 Low	0.0	☒	☐	
202.54.240.182	DNS Host Name	🟩 Low	0.0	☒	☐	
202.54.240.182	Traceroute	🟩 Low	0.0	☒	☐	
202.54.240.182	Target Network Information	🟩 Low	0.0	☒	☐	
202.54.240.182	Internet Service Provider	🟩 Low	0.0	☒	☐	
202.54.240.182	Host Names Found	🟩 Low	0.0	☒	☐	
202.54.240.182	Host Scan Time	🟩 Low	0.0	☒	☐	

Consolidated Solution/Correction Plan for above Component:

125.21.0.182	ICMP Replies Received	🟩 Low	0.0	☒	☐	
125.21.0.182	Host Name Not Available	🟩 Low	0.0	☒	☐	
125.21.0.182	DNS Host Name	🟩 Low	0.0	☒	☐	
125.21.0.182	Host Scan Time	🟩 Low	0.0	☒	☐	
125.21.0.182	Firewall Detected	🟩 Low	0.0	☒	☐	

Consolidated Solution/Correction Plan for above Component:

125.21.44.66	ICMP Replies Received	🟩 Low	0.0	☒	☐	
125.21.44.66	Host Name Not Available	🟩 Low	0.0	☒	☐	
125.21.44.66	DNS Host Name	🟩 Low	0.0	☒	☐	
125.21.44.66	Traceroute	🟩 Low	0.0	☒	☐	
125.21.44.66	Internet Service Provider	🟩 Low	0.0	☒	☐	
125.21.44.66	Host Scan Time	🟩 Low	0.0	☒	☐	
125.21.44.66	Firewall Detected	🟩 Low	0.0	☒	☐	

Consolidated Solution/Correction Plan for above Component:

216.195.64.30	ICMP Replies Received	🟩 Low	0.0	☒	☐	
216.195.64.30	DNS Host Name	🟩 Low	0.0	☒	☐	
216.195.64.30	Host Names Found	🟩 Low	0.0	☒	☐	

216.195.64.30	Host Scan Time		0.0	☒	☐	
		Low				
216.195.64.30	Firewall Detected	Low	0.0	☒	☐	

Consolidated Solution/Correction Plan for above Component:

4.59.196.78	ICMP Replies Received	Low	0.0	☒	☐	
4.59.196.78	DNS Host Name	Low	0.0	☒	☐	
4.59.196.78	Traceroute	Low	0.0	☒	☐	
4.59.196.78	Target Network Information	Low	0.0	☒	☐	
4.59.196.78	Internet Service Provider	Low	0.0	☒	☐	
4.59.196.78	Host Names Found	Low	0.0	☒	☐	
4.59.196.78	Host Scan Time	Low	0.0	☒	☐	
4.59.196.78	Firewall Detected	Low	0.0	☒	☐	
4.59.196.78	ICMP Timestamp Request	Low	0.0	☒	☐	

Consolidated Solution/Correction Plan for above Component:

50.207.117.50	ICMP Replies Received	Low	0.0	☒	☐	
50.207.117.50	Host Uptime Based on TCP TimeStamp Option	Low	0.0	☒	☐	
50.207.117.50	Degree of Randomness of TCP Initial Sequence Numbers	Low	0.0	☒	☐	
50.207.117.50	IP ID Values Randomness	Low	0.0	☒	☐	
50.207.117.50	DNS Host Name	Low	0.0	☒	☐	
50.207.117.50	Traceroute	Low	0.0	☒	☐	
50.207.117.50	Target Network Information	Low	0.0	☒	☐	
50.207.117.50	Internet Service Provider	Low	0.0	☒	☐	
50.207.117.50	Host Names Found	Low	0.0	☒	☐	
50.207.117.50	Host Scan Time	Low	0.0	☒	☐	
50.207.117.50	Scan Activity per Port	Low	0.0	☒	☐	
50.207.117.50	Open TCP Services List	Low	0.0	☒	☐	
50.207.117.50	Operating System Detected	Low	0.0	☒	☐	

50.207.117.50	Firewall Detected	■Low	0.0	☒	☐	
Consolidated Solution/Correction Plan for above Component:						
12.125.232.106	ICMP Replies Received	■Low	0.0	☒	☐	
12.125.232.106	Host Name Not Available	■Low	0.0	☒	☐	
12.125.232.106	DNS Host Name	■Low	0.0	☒	☐	
12.125.232.106	Traceroute	■Low	0.0	☒	☐	
12.125.232.106	Target Network Information	■Low	0.0	☒	☐	
12.125.232.106	Internet Service Provider	■Low	0.0	☒	☐	
12.125.232.106	Host Scan Time	■Low	0.0	☒	☐	
12.125.232.106	Firewall Detected	■Low	0.0	☒	☐	
12.125.232.106	ICMP Timestamp Request	■Low	0.0	☒	☐	
Consolidated Solution/Correction Plan for above Component:						
122.55.2.142	ICMP Replies Received	■Low	0.0	☒	☐	
122.55.2.142	DNS Host Name	■Low	0.0	☒	☐	
122.55.2.142	Traceroute	■Low	0.0	☒	☐	
122.55.2.142	Internet Service Provider	■Low	0.0	☒	☐	
122.55.2.142	Cisco IOS Installed on Target Host	■Low	0.0	☒	☐	
122.55.2.142	Host Names Found	■Low	0.0	☒	☐	
122.55.2.142	Host Scan Time	■Low	0.0	☒	☐	
122.55.2.142	Scan Activity per Port	■Low	0.0	☒	☐	
122.55.2.142	Remote Access or Management Service Detected	■Low	0.0	☒	☐	
122.55.2.142	Open TCP Services List	■Low	0.0	☒	☐	
122.55.2.142	Open UDP Services List	■Low	0.0	☒	☐	
122.55.2.142	Operating System Detected	■Low	0.0	☒	☐	
122.55.2.142 : 53	Named Daemon Version Number Disclosure Vulnerability	■Low	0.0	☒	☐	

122.55.2.142	ICMP Timestamp Request	🟩 Low	0.0	☒	☐	
Consolidated Solution/Correction Plan for above Component:						
222.127.146.122	ICMP Replies Received	🟩 Low	0.0	☒	☐	
222.127.146.122	Host Name Not Available	🟩 Low	0.0	☒	☐	
222.127.146.122	DNS Host Name	🟩 Low	0.0	☒	☐	
222.127.146.122	Traceroute	🟩 Low	0.0	☒	☐	
222.127.146.122	Internet Service Provider	🟩 Low	0.0	☒	☐	
222.127.146.122	Host Scan Time	🟩 Low	0.0	☒	☐	
222.127.146.122	Firewall Detected	🟩 Low	0.0	☒	☐	
222.127.146.122	ICMP Timestamp Request	🟩 Low	0.0	☒	☐	
Consolidated Solution/Correction Plan for above Component:						
125.23.240.158	ICMP Replies Received	🟩 Low	0.0	☒	☐	
125.23.240.158	Host Name Not Available	🟩 Low	0.0	☒	☐	
125.23.240.158	DNS Host Name	🟩 Low	0.0	☒	☐	
125.23.240.158	Traceroute	🟩 Low	0.0	☒	☐	
125.23.240.158	Internet Service Provider	🟩 Low	0.0	☒	☐	
125.23.240.158	Host Scan Time	🟩 Low	0.0	☒	☐	
125.23.240.158	Scan Activity per Port	🟩 Low	0.0	☒	☐	
125.23.240.158	Remote Access or Management Service Detected	🟩 Low	0.0	☒	☐	
125.23.240.158	Open UDP Services List	🟩 Low	0.0	☒	☐	
125.23.240.158	ICMP Timestamp Request	🟩 Low	0.0	☒	☐	
Consolidated Solution/Correction Plan for above Component:						
115.114.73.26	ICMP Replies Received	🟩 Low	0.0	☒	☐	
115.114.73.26	DNS Host Name	🟩 Low	0.0	☒	☐	
115.114.73.26	Traceroute	🟩 Low	0.0	☒	☐	
115.114.73.26	Internet Service Provider	🟩 Low	0.0	☒	☐	

115.114.73.26	Host Names Found	🟩 Low	0.0	☒	☐	
115.114.73.26	Host Scan Time	🟩 Low	0.0	☒	☐	
115.114.73.26	Scan Activity per Port	🟩 Low	0.0	☒	☐	
115.114.73.26	Remote Access or Management Service Detected	🟩 Low	0.0	☒	☐	
115.114.73.26	Open UDP Services List	🟩 Low	0.0	☒	☐	
115.114.73.26	ICMP Timestamp Request	🟩 Low	0.0	☒	☐	
Consolidated Solution/Correction Plan for above Component:						
12.87.39.214 : 22	Deprecated SSH Cryptographic Settings	🟨 Medium	6.4	☒	☐	Assessor has verified and confirmed that reported vulnerability is false-positive as per the evidence provided by Genpact. Hence, it is passed.
12.87.39.214	ICMP Replies Received	🟩 Low	0.0	☒	☐	
12.87.39.214	Host Uptime Based on TCP TimeStamp Option	🟩 Low	0.0	☒	☐	
12.87.39.214	Host Name Not Available	🟩 Low	0.0	☒	☐	
12.87.39.214	Degree of Randomness of TCP Initial Sequence Numbers	🟩 Low	0.0	☒	☐	
12.87.39.214	IP ID Values Randomness	🟩 Low	0.0	☒	☐	
12.87.39.214	DNS Host Name	🟩 Low	0.0	☒	☐	
12.87.39.214	Traceroute	🟩 Low	0.0	☒	☐	
12.87.39.214	Target Network Information	🟩 Low	0.0	☒	☐	
12.87.39.214	Internet Service Provider	🟩 Low	0.0	☒	☐	
12.87.39.214	Host Scan Time	🟩 Low	0.0	☒	☐	
12.87.39.214	Scan Activity per Port	🟩 Low	0.0	☒	☐	
12.87.39.214	Remote Access or Management Service Detected	🟩 Low	0.0	☒	☐	
12.87.39.214 : 22	SSH daemon information retrieving	🟩 Low	0.0	☒	☐	
12.87.39.214	Open TCP Services List	🟩 Low	0.0	☒	☐	
12.87.39.214	Open UDP Services List	🟩 Low	0.0	☒	☐	
12.87.39.214	Operating System Detected	🟩 Low	0.0	☒	☐	

12.87.39.214 : 22	SSH Banner	■ Low	0.0	⊠	☐	
12.87.39.214	ICMP Timestamp Request	■ Low	0.0	⊠	☐	

Consolidated Solution/Correction Plan for above Component:

Please refer the detailed report to remediate the above vulnerabilities.

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

Common Vulnerability Scoring System (CVSS) base score, as indicated in the National Vulnerability Database (NVD), where available.

Part 3b. Special Notes by Component			
Component	Special Note	Item Noted (remote access software, POS software, etc.)	Scan customer's description of action taken and declaration that software is either implemented securely or removed
38.142.188.30	Remote Access or Management Service Detected	Service name: ISAKMP on UDP port 500.	Genpact has confirmed ControlCase that the service is implemented properly with strong passwords.
38.142.188.30	Remote Access or Management Service Detected	SNMP on UDP port 161.	Genpact has confirmed ControlCase that SNMP is securely implemented.
122.55.2.142	Remote Access or Management Service Detected	Service name: SNMP on UDP port 161.	Genpact has confirmed ControlCase that SNMP is securely implemented.
125.23.240.158	Remote Access or Management Service Detected	Service name: SNMP on UDP port 161.	Genpact has confirmed ControlCase that SNMP is securely implemented.
115.114.73.26	Remote Access or Management Service Detected	Service name: SNMP on UDP port 161.	Genpact has confirmed ControlCase that SNMP is securely implemented.
12.87.39.214	Remote Access or Management Service Detected	Service name: SSH on TCP port 22.	Genpact confirmed to Controlcase that the remote access service is securely implemented.

Part 3c. Special Notes - Full Text

Remote Access or Management Service Detected
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.

Part 4a. Scan Scope Submitted by Scan Customer for Discovery

IP Address:Domain:	38.142.188.30
IP Address:Domain:	69.174.28.138
IP Address:Domain:	59.160.97.246
IP Address:Domain:	202.54.240.182
IP Address:Domain:	125.21.0.182
IP Address:Domain:	125.21.44.66
IP Address:Domain:	182.19.62.165
IP Address:Domain:	122.15.135.129
IP Address:Domain:	216.195.64.30
IP Address:Domain:	216.195.64.34
IP Address:Domain:	4.59.196.78
IP Address:Domain:	67.154.112.26
IP Address:Domain:	50.207.117.50
IP Address:Domain:	12.125.232.106
IP Address:Domain:	122.55.2.142
IP Address:Domain:	222.127.146.122
IP Address:Domain:	32.6.166.114
IP Address:Domain:	32.6.166.118
IP Address:Domain:	121.241.98.81
IP Address:Domain:	125.23.240.158
IP Address:Domain:	115.114.73.26
IP Address:Domain:	32.6.185.174
IP Address:Domain:	32.6.185.182
IP Address:Domain:	32.6.185.186
IP Address:Domain:	12.87.39.214
IP Address:Domain:	157.130.132.82

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

IP Address:Domain:	38.142.188.30
IP Address:Domain:	69.174.28.138
IP Address:Domain:	59.160.97.246
IP Address:Domain:	202.54.240.182
IP Address:Domain:	125.21.0.182
IP Address:Domain:	125.21.44.66
IP Address:Domain:	182.19.62.165
IP Address:Domain:	122.15.135.129
IP Address:Domain:	216.195.64.30
IP Address:Domain:	216.195.64.34
IP Address:Domain:	4.59.196.78
IP Address:Domain:	67.154.112.26
IP Address:Domain:	50.207.117.50
IP Address:Domain:	12.125.232.106
IP Address:Domain:	122.55.2.142
IP Address:Domain:	222.127.146.122
IP Address:Domain:	32.6.166.114
IP Address:Domain:	32.6.166.118
IP Address:Domain:	121.241.98.81
IP Address:Domain:	125.23.240.158
IP Address:Domain:	115.114.73.26
IP Address:Domain:	32.6.185.174
IP Address:Domain:	32.6.185.182
IP Address:Domain:	32.6.185.186
IP Address:Domain:	12.87.39.214
IP Address:Domain:	157.130.132.82

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