



PCI ASV Vulnerability Scan Report

Executive Summary

Table of Contents

| | |
|---|---|
| Table of Contents | 2 |
| Appendix A: ASV Scan Report Attestation of Scan Compliance | 3 |
| A.1 Scan Customer Information | 3 |
| A.2 Approved Scanning Vendor Information | 3 |
| A.3 Scan Status | 3 |
| A.4 Scan Customer Attestation | 3 |
| A.5 ASV Attestation | 3 |
| Appendix B: ASV Scan Report Summary | 4 |
| Part 1. Scan Information | 4 |
| Part 2. Component Compliance Summary | 5 |
| Part 3a. Vulnerabilities Noted for each Component | 6 |
| Part 3b. Special Notes by Component | 7 |
| Part 3c. Special Notes - Full Text | 7 |
| Part 4a. Scan Scope Submitted by Scan Customer for Discovery | 7 |
| Part 4b. Scan Customer Designated "In-Scope" Components (Scanned) | 7 |
| Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned) | 7 |

Appendix A: ASV Scan Report Attestation of Scan Compliance

| | | |
|--------------------------------------|-------------------|---------------------------------------|
| A.1 Scan Customer Information | | |
| Company: | Genpact | |
| Contact Name: | Ankur Shrivastava | |
| Job Title: | | |
| Telephone: | 01206407443 | 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: | March 09, 2021 (GMT) | Scan expiration date (90 days from date scan completed) : June 07, 2021 (GMT) |
| Compliance Status: | <input checked="" type="checkbox"/> Pass | Scan report type: <input checked="" type="checkbox"/> Full Scan <input type="checkbox"/> Partial scan or rescan |
| 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 | |

| | | |
|--------------------------------------|--|--|
| A.4 Scan Customer Attestation | | |
|--------------------------------------|--|--|

Genpact attests on March 09, 2021 (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: | March 09, 2021 | Scan expiration date: | June 07, 2021 |

| Part 2. Component Compliance Summary | | | |
|--------------------------------------|---------------|---|--------------------------------------|
| IP Address: | 12.250.251.30 | <input checked="" type="checkbox"/> Pass | <input type="checkbox"/> Fail |

Part 3a. Vulnerabilities Noted for each Component

| Component | Vulnerabilities Noted per Component | Severity Level | CVSS Score ¹ | Compliance Status | | Exceptions, False Positives, or Compensating Controls |
|---|-------------------------------------|---|-------------------------|-------------------------------------|--------------------------|---|
| | | | | Pass | Fail | |
| 12.250.251.30 | ICMP Replies Received |  Low | 0.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 12.250.251.30 | Host Name Not Available |  Low | 0.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 12.250.251.30 | DNS Host Name |  Low | 0.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 12.250.251.30 | Traceroute |  Low | 0.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 12.250.251.30 | Target Network Information |  Low | 0.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 12.250.251.30 | Internet Service Provider |  Low | 0.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 12.250.251.30 | Host Scan Time |  Low | 0.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 12.250.251.30 | Firewall Detected |  Low | 0.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 12.250.251.30 | ICMP Timestamp Request |  Low | 0.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 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 |
| | | | |

| |
|---|
| Part 3c. Special Notes - Full Text |
| |
| |
| |

| |
|---|
| Part 4a. Scan Scope Submitted by Scan Customer for Discovery |
| IP Address:Domain: 12.250.251.30 |
| |

| |
|--|
| Part 4b. Scan Customer Designated "In-Scope" Components (Scanned) |
| IP Address:Domain: 12.250.251.30 |
| |

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