

# Payment Card Industry (PCI) Executive Report

01/02/2023

## ASV Scan Report Attestation of Scan Compliance

A1. Scan Customer Information				A2. Approved Scanning Vendor Information			
Company:	Qualys_Training_tenley@wildun.ca			Company:	Qualys		
Contact Name:	Tenley Wiltshire	Job Title:		Contact Name:	-	Job Title:	-
Telephone:		Email:	tenley@wildun.ca	Telephone:	-	Email:	-
Business Address:	919 E Hillsdale Blvd,			Business Address:	919 E Hillsdale Blvd, 4th Floor		
City:	Foster City, CA 94404	State/Province:	California	City:	Foster City	State/Province:	California
ZIP/postal code:		Country:	United States of America	ZIP/postal code:	94404	Country:	United States of America
URL:				URL:	http://www.qualys.com/		

A3. Scan Status			
Date scan completed	12/25/2022	Scan expiration date (90 days from date scan completed)	03/25/2023
Compliance Status	<b>FAIL</b>	Scan report type	Full scan
Number of unique in-scope components scanned	2		
Number of identified failing vulnerabilities	3		
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope	0		

A.4 Scan Customer Attestation
<p>Qualys_Training_tenley@wildun.ca attests on 01/02/2023 at 15:11:50 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.</p> <p>Qualys_Training_tenley@wildun.ca 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.</p>
A.5 ASV Attestation
<p>This scan and report was prepared and conducted by Qualys under certificate number 3728-01-17, according to internal processes that meet PCI DSS requirement 11.2.2 and the ASV Program Guide.</p> <p>Qualys 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</p>

## ASV Scan Report Summary

### Part 1. Scan Information

Scan Customer Company:	Qualys_Training_tenley@wildun.ca	ASV Company:	Qualys
Date scan was completed:	12/25/2022	Scan expiration date:	03/25/2023

## Part 2. Component Compliance Summary

64.41.200.245, demo15.s02.sjc01.qualys.com	<b>FAIL</b>
64.41.200.247, trn-win7.trn.qualys.com	<b>PASS</b>

## 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>
64.41.200.245, demo15.s02.sjc01.qualys.com <small>port 22/tcp</small>	38739 - Deprecated SSH Cryptographic Settings	<b>MED</b>	6.4	<b>FAIL</b>	The vulnerability is not included in the NVD. ASV Score = 6.4
64.41.200.245, demo15.s02.sjc01.qualys.com	45002 - Global User List Found Using Other QIDS	<b>MED</b>	5	<b>FAIL</b>	Automatic Failure: Built-in or default accounts and passwords The vulnerability is not included in the NVD.
64.41.200.245, demo15.s02.sjc01.qualys.com <small>port 22/tcp</small>	38737 - OpenSSH User Enumeration CVE-2018-15473	<b>MED</b>	5	<b>FAIL</b>	
64.41.200.245, demo15.s02.sjc01.qualys.com	82003 - ICMP Timestamp Request CVE-1999-0524	<b>LOW</b>	2.1	<b>PASS</b>	The vulnerability is purely a denial-of-service (DoS) vulnerability.
<b>Consolidated Solution/Correction Plan for 64.41.200.245</b>  <b>ASV Comment:</b> Please update OpenSSH to the latest versions. Change built-in or default accounts and passwords.					
64.41.200.247, trn-win7.trn.qualys.com	82003 - ICMP Timestamp Request CVE-1999-0524	<b>LOW</b>	2.1	<b>PASS</b>	The vulnerability is purely a denial-of-service (DoS) vulnerability.
64.41.200.247, trn-win7.trn.qualys.com	70000 - NetBIOS Name Accessible	<b>LOW</b>	0	<b>PASS</b>	The vulnerability is not included in the NVD. ASV Score = 0

## Part 3b. Special Notes by Component

Component	Special Note	Item Noted (remote access software, POS software, etc.)	Scan customer's description of actions taken and declaration that software is either implemented securely or removed
64.41.200.245	Remote Access	42017 - Remote Access or Management Service Detected (SSH:port 22/TCP)	No - Student Test
64.41.200.247	Unknown services	82023 - Open TCP Services List (TCP/IP)	No - Student Test
64.41.200.247	Unknown services	82004 - Open UDP Services List (TCP/IP)	No - Student Test

### Part 3c. Special Notes Full Text

#### Note

##### Remote Access

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 2) confirm it is either implemented securely or disabled/removed.

##### Unknown services

Note to Scan Customer : Unidentified services have been detected. Due to increased risk to the cardholder data environment, identify the service, then either 1) justify the business need for this service and confirm it is securely implemented, or 2) identify the service and confirm that it is disabled. 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.

64.41.200.245-64.41.200.247

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

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

64.41.200.245, demo15.s02.sjc01.qualys.com

64.41.200.247, trn-win7.trn.qualys.com

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

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

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.

## Report Summary

Company: Qualys\_Training\_tenley@wildun.ca  
Hosts in Account: 3 IP  
Hosts Active: 2  
Hosts Scanned: 3  
Scan Date: 12/25/2022 at 14:36:18 GMT  
Report Date: 01/02/2023 at 15:11:53 GMT  
Report Title: Q@ PCI Report  
Template Title: Payment Card Industry (PCI) Executive Report

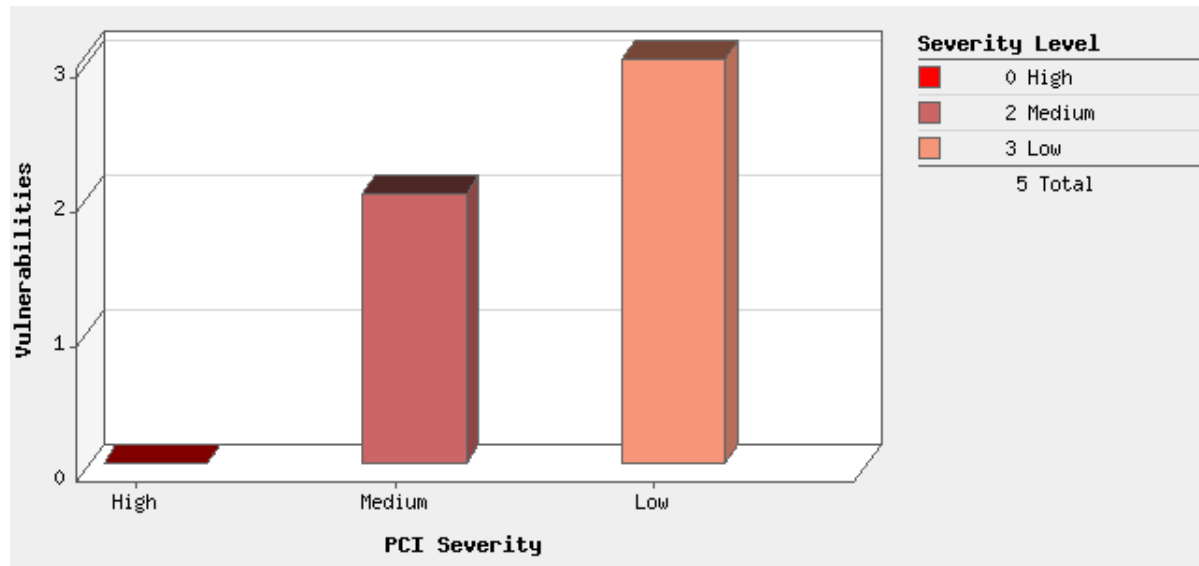
## Summary of Vulnerabilities

Vulnerabilities Total	46	Average Security Risk	<div><div></div><div></div><div></div><div></div><div></div></div>	2.5
-----------------------	----	-----------------------	--	-----

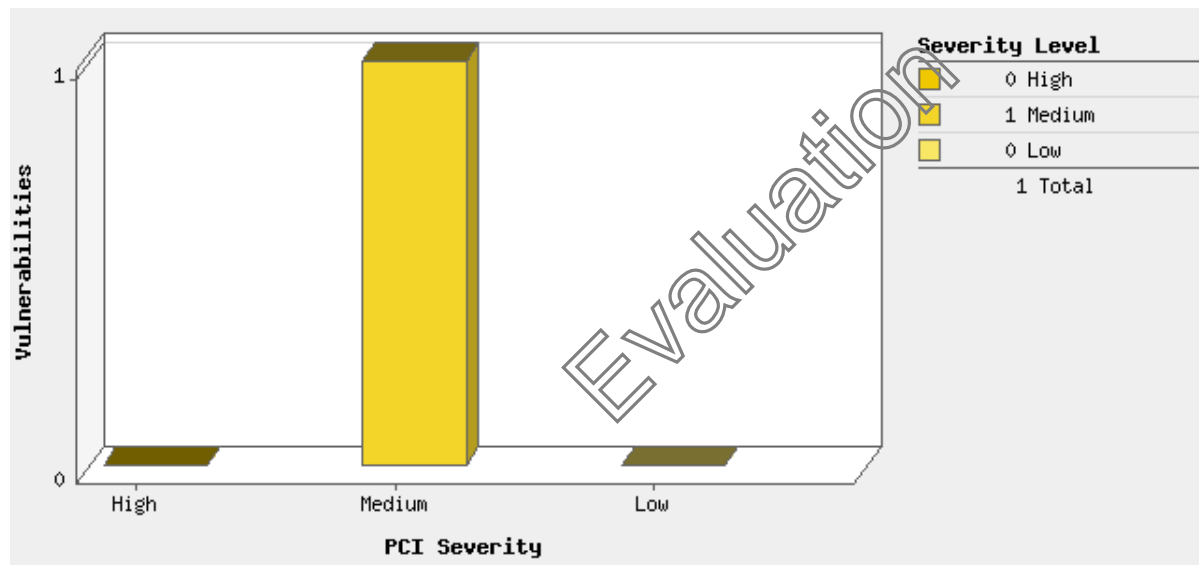
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	2	0	2	4
2	1	1	6	8
1	2	0	32	34
Total	5	1	40	46

by PCI Severity			
PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	2	1	3
Low	3	0	3
Total	5	1	6

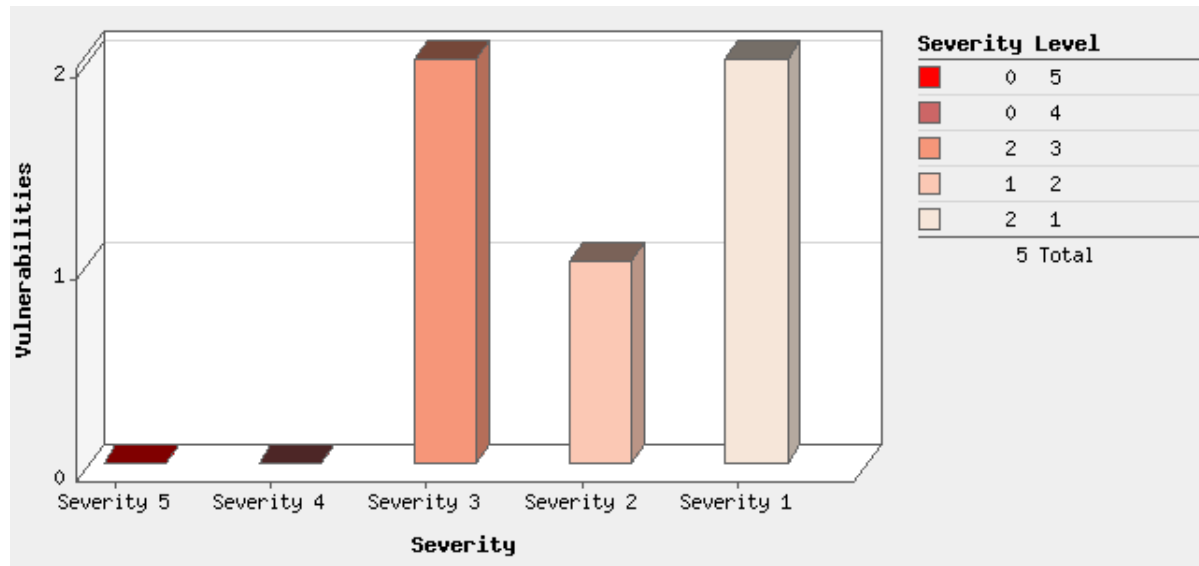
## Vulnerabilities by PCI Severity



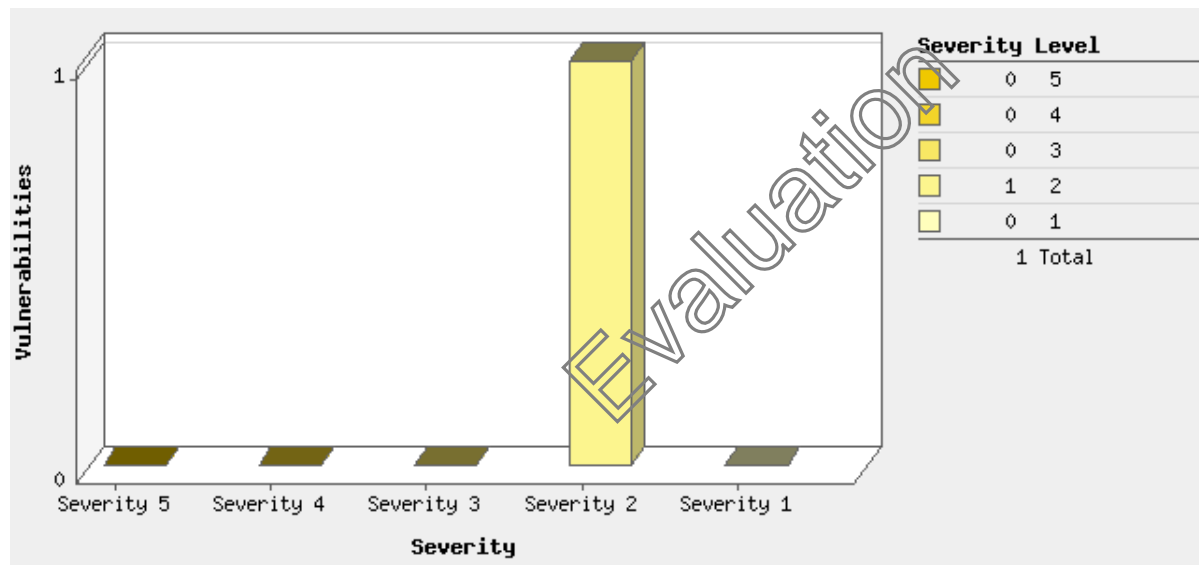
## Potential Vulnerabilities by PCI Severity



## Vulnerabilities by Severity



## Potential Vulnerabilities by Severity



## Appendices

### Host Comments

64.41.200.245, demo15.s02.sjc01.qualys.com

Please update OpenSSH to the latest versions. Change built-in or default accounts and passwords.

### Hosts Scanned

64.41.200.245, 64.41.200.247

### Hosts Not Alive

64.41.200.246

### 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

Evaluation

#### 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	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	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.

Evaluation

Evaluation