

## Payment Card Industry (PCI) Executive Report

11/01/2016

**ASV Scan Report Attestation of Scan Compliance**

Scan Customer Information				Approved Scanning Vendor Information			
Company:	Rural Computer Consultants			Company:	SecureWorks		
Contact:	Jason Buetow	Title:	Administrator	Contact:	Timothy Davis	Title:	Operations
Telephone:	320-365-4027	Email:	jbueto@rccbi.com	Telephone:	1-888-456-3210 x4	Email:	vms@secureworks.com
Business Address:	211 S. 10th St.,			Business Address:	One Concourse Parkway, Ste. 500		
City:	Bird Island	State/Province:	Minnesota	City:	Atlanta	State/Province:	Georgia
ZIP:	55310	URL:		ZIP:	30328	URL:	<a href="http://www.secureworks.com/">http://www.secureworks.com/</a>

**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: 1
- \* Date scan completed: 11/01/2016
- \* Scan expiration date (90 days from date scan completed): 01/30/2017

**Scan Customer Attestation**

Rural Computer Consultants attests on 11/01/2016 at 16:10:04 GMT 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. Rural Computer Consultants also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicated 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 SecureWorks under certificate number 3761-02-09, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide.

SecureWorks 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 Timothy Davis

# ASV Scan Report Executive Summary

## Part 1. Scan Information




Scan Customer Company:	Rural Computer Consultants	ASV Company:	SecureWorks
Date scan was completed:	11/01/2016	Scan expiration date:	01/30/2017

## Part 2. Component Compliance Summary

IP Address: 97.64.144.90	<b>PASS</b>
--------------------------	-------------

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

### 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 <small>Noted by the ASV for this Vulnerability</small>
97.64.144.90 <small>port 443/tcp-SSL</small>	42366 - SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST) CVE-2011-3389	 MED	4.3	<b>PASS</b>	ASV Score 2.6: The ASV access complexity is High for server side, because Javascript injection and MiTM capabilities and a vulnerable client that is not using record splitting are required to exploit this vulnerability.
97.64.144.90 <small>port 443/tcp-SSL</small>	38601 - SSL/TLS use of weak RC4 cipher CVE-2013-2566, CVE-2015-2808	 MED	4.3	<b>PASS</b>	ASV Score 2.6: The ASV access complexity is High for server side, because MiTM capabilities and a vulnerable client are required to exploit this vulnerability.
97.64.144.90 <small>port 443/tcp-SSL</small>	38628 - SSL/TLS Server supports TLSv1.0	 LOW	2.6	<b>PASS</b>	The vulnerability is not included in the NVD. ASV Score = 2.6

### 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
97.64.144.90	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.	42017 - Remote Access or Management Service Detected (SSH:port 22/TCP)	Yes	Limited

## Report Summary

Company:	Rural Computer Consultants
Hosts in Account:	1
Hosts Scanned:	1
Hosts Active:	1
Scan Date:	11/01/2016 at 15:15:17 GMT
Report Date:	11/01/2016 at 16:10:17 GMT
Report Title:	nov 1 2016 PCI
Template Title:	Payment Card Industry (PCI) Executive Report

## Summary of Vulnerabilities

Vulnerabilities Total	41	Average Security Risk		3.0
-----------------------	----	-----------------------	---	-----

### by Severity

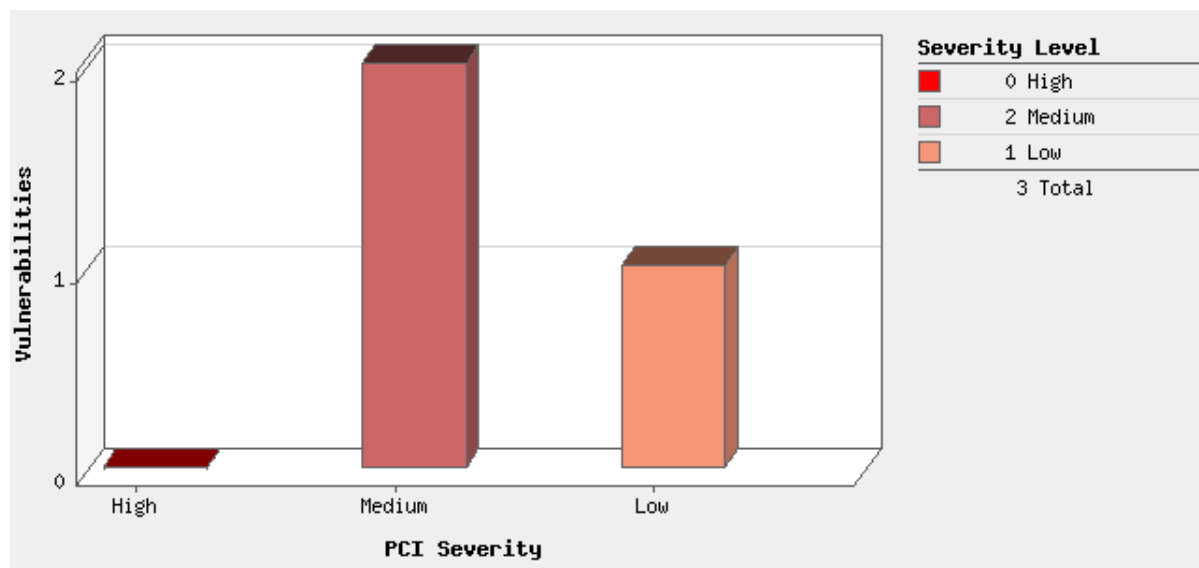
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	3	0	1	4
2	0	0	4	4
1	0	0	33	33
Total	3	0	38	41

### by PCI Severity

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

## Vulnerabilities by PCI Severity

---



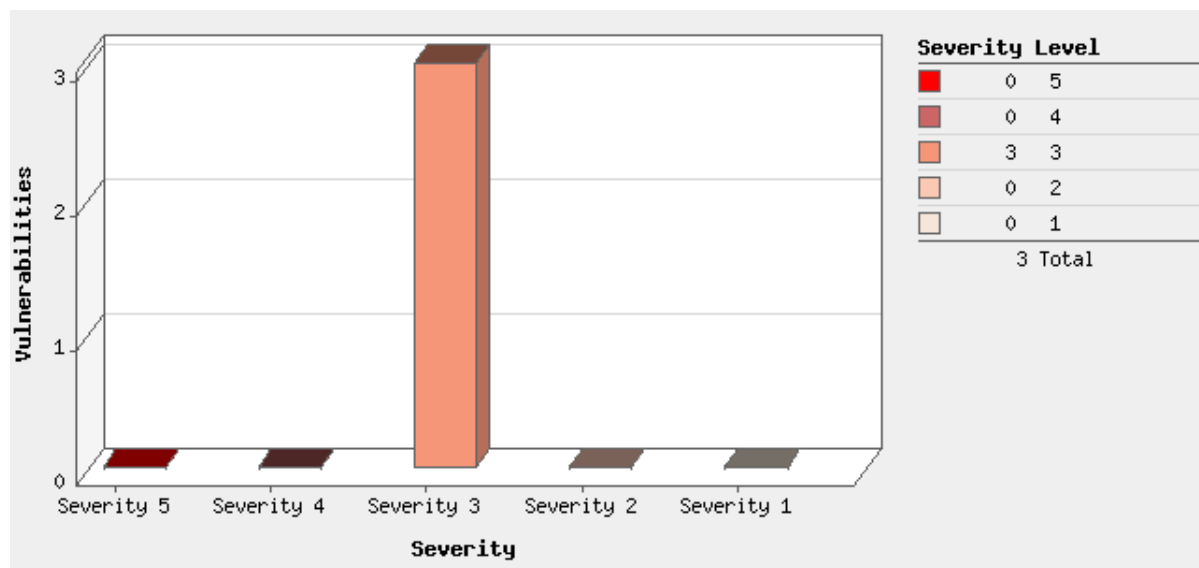
## Potential Vulnerabilities by PCI Severity

---

There is no data available

## Vulnerabilities by Severity

---



## Potential Vulnerabilities by Severity

---

There is no data available

## Appendices

### Hosts Scanned

97.64.144.90

### 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	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.



