IP Tunnel Technology PCI DSS 3.2

Platform Compliance Vulnerability Assessment

For

IP Technology Labs
Network Communications Simplified™

June 27, 2016

Submitted To:

IP Technology Labs LLC
3470 Olney-Laytonsville RD , #313
Olney MD, 20832 USA
E: corporate@IpTechnologyLabs.com
T: +1 301 570 6611

Submitted By:

Rick Mellendick
Chief Security Officer
Process Improvement Achievers, LLC
T: 443-948-7600 ext. 102
E:rmellendick@piachievers.com
www.piachievers.com

Table of Contents

1 Executive Summary

Process Improvement Achievers, LLC. ("PI Achievers") was contracted by IP Technology Labs LLC. ("IpTL") to perform a **PCI DSS 3.2 Platform Vulnerability Assessment**. The assessment began on May 23, 2016 and was completed June 27, 2016. As part of the services that were provided, PI Achievers conducted a validation and platform vulnerability assessment for PCI DSS 3.2 compliance of the IP Technology Labs capabilities, using the 7xyz platform as the basis of the testing (firmware version iptl_m70_3.2.11-2z).

This is not a PCI Certification but a PCI compliance test. Under PCI DSS, devices in and of themselves cannot be PCI Certified but rather the complete system is certified. In order for the system to reach PCI certification the individual components must also conform to the PCI compliance guidelines. The outcomes of this assessment will determine suitability of the IP Technology Laps appliances. The final assessment will indicate the that the use of IpTL appliances, in a PCI certified network, with either add, detract, or keep the system baseline intact.

The findings in this report are based upon the scan results and probing of the IpTL 7X series device. The results of the assessment will be the same results an auditor will see during a PCI DSS audit. **IpTL appliances have an assessment value of 0.0. When IpTL is part of a PIC DSS 3.2 compliant system, the IpTL appliances will not detract from the security of the system, IpTL adds as to the security of the data in transit and protection of the PCI data.**

1.1 Summary of Findings

Configuration: The device was configured for testing with the following settings (in the raw data):

- No default accounts
- A default SSL configuration on port 80 for web management with the CA imported to the system
- A straight tunnel to an internal network host was running during all tests
- There was no connectivity to the support center or real time resource
- UDP was turned off (by default)
- An external NTP was configured to 0.north-america.pool.ntp.org
- DNS was ported to OpenDNS and validated by the Fortinet cloud DNS
- Internal DNS was turned off

Nessus: The full PCI Internal and External results are in the raw data with an executive report in this outbrief as Appendix 1. Due to the nature of PCI DSS audits on security equipment there can be no common vulnerability scoring system (CVSS) over a 4.0 for any vulnerabilities, this includes the Medium severities as well as Highs and Critical. The grades are not based on security but instead based on PCI compliance for the device, in this case the security of the device is also A+.

Table 1: Internal and External Nessus Vulnerability Scan Results

Findings	Critical	High	Medium	Low	Grade
Internal PCI Nessus Scan	0	0	0	0	A+

Findings	Critical	High	Medium	Low	Grade
External PCI Nessus Scan	0	0	0	0	A+

Arachni: There are no findings in the web application scan that are going to invalidate the PCI DSS version 3.2 compliance. (Appendix 2)

NMAP: There are no significant findings with the NMAP (Port Scan) of the system. This does include one non-default change, utilizing port 80 and turning on SSL for web management.

Manual Validation: The overall stance of the device hardware and software is compliant based on the Nessus PCI internal as well as external scan. The actual tests all passed (most are N/A for a hardware device) and explanations are in appendix 4**.** The tamper evident build and the hardware accessibility and the packing of the binary are all very positive and well done. The tunnel stayed connected and functional during the entirety of the assessment and even when at 100% utilization data was able to get through the tunnel. This is a tribute to the stability of the technology.

2 Scope, Approach, and Methodology

PI Achievers performed a platform and device testing service. The assessment results provide IP Technology Labs with validation of the capability of the tunnel technology to perform adequately within a compliant PCI DSS environment. PI Achievers performed all tests in our air-gapped, secure lab. The scope of work included an overall platform and device-testing service on the IP Technology Labs 7x platform hardware based on the newly releases PCI DSS 3.2.

2.1 Objective 1 – PCI DSS 3.2 Platform Vulnerability Assessment

During all phases of the engagement there were operations using automated and manual-scanning activities. The PCI DSS compliance program has a very specific set of standards to be assessed against. These were validated through technology and observations of the 12 PCI DSS Requirements and 416 associated testing procedures (not all were valid for these tests).

The following are the PCI Data standard High Level Overview:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect cardholder data
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software on all systems commonly affected by malware
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

2.2 Objective 2 – Analysis and Reporting

During the assessment, the PI Achievers team gathered raw data from the PCI DSS 3.2 Assessment including vulnerability scanning, port enumeration, web vulnerability assessment and following the

testing set forth by PCI DSS (Including custom Nessus PCI module for internal systems as well as external systems). This information was analyzed using a combination of automated tools and manual methods. This report was prepared and the results of the assessment are being presented to the POC.

This report contains an executive summary along with descriptions of work performed, detailed findings, and recommended mitigations. Raw test data output has been provided in an encrypted electronic format. At the conclusion of the outbrief, IP Technology Labs will have a better understanding of the following:

- List of prioritized findings associated with the target device and its ability to perform adequately in a PCI DSS 3.2 environment
- Approaches to correcting findings or mitigating their risks (If any)
- Compliance testing all based on the PCI DSS 3.2 included in the raw data

3 Findings and Recommendations (none)

PCI DSS audits on security equipment indicate there cannot be a CVSS value over 4.0 for each of the vulnerability categories. IpTL appliances have an assessment value of 0.0 on each vulnerability category. This indicates, that when IpTL is part of a PIC DSS 3.2 compliant system, the IpTL appliances will not detract in any way from the overall security posture of the system. In addition to 12 informational elements, the raw data included on the electronic media contains all of the findings:

Vulnerability	IpTL Score
critical	0
high	0
medium	0
low	0

This report only focuses on the findings that would render this system non-PCI compliant. A complete list of tools used during this assessment may be found in the Appendix 3.

Appendix 1: NMAP and Nessus Scan of an IPTL Model 7x

Device name/Type: 02-02-70-00-14-54/Model 75
Device IP Address: 10.0.2.12
Software version: Version 3.2.11-2z

Nmap UDP Scan

MBA: xxxx$ sudo nmap -sU 10.0.2.12
Starting Nmap 7.12 (https://nmap.org) at 2016-06-27 09:55 EDT
Nmap scan report for 10.0.2.12
Host is up (0.00048s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
5353/udp open|filtered zeroconf
MAC Address: 02:02:71:03:02:1A (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 1084.96 seconds

Nmap TCP scan

MBA: xxxx$ nmap -p 0-65535 10.0.2.12
Starting Nmap 7.12 (https://nmap.org) at 2016-06-27 09:35 EDT
Nmap scan report for 10.0.2.12
Host is up (0.0021s latency).
Not shown: 65534 closed ports
PORT STATE SERVICE
0/tcp filtered unknown
80/tcp open https
Nmap done: 1 IP address (1 host up) scanned in 10.20 seconds

Internal Nessus Scan Results:

Device Name: iptldevice.iptechnologylabs.com (10.0.2.12)

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

Details

Severity	Plugin Id	Name
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	14788	IP Protocols Scan
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported

Info	22964	Service Detection
Info	33930	PCI DSS Compliance : Passed
Info	46180	Additional DNS Hostnames
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	60020	PCI DSS Compliance : Handling False Positives

Vulnerability Criticality Descriptions

Critical = Should be addressed first in remediation plan: Vulnerability has the capability of allowing full and unauthorized network access

High = Should be addressed next in remediation plan based on organization's risk tolerance level: Allows for direct access to the internal network; could result in compromise of information

Medium = Should be addressed in remediation plan based on organization's risk tolerance level and business objectives: Risk of compromise, but unlikely; these could result in application, but not network access

Low = Should be reviewed and included in remediation plan at organization's discretion based on risk tolerance level, business objectives, and resource availability: Unlikely risk of compromise of application, OS, and network resources

External Nessus Scan Results

Device Name: iptldevice.iptechnologylabs.com (10.0.2.12)

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

Details

Severity	Plugin Id	Name
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	14788	IP Protocols Scan
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	33930	PCI DSS Compliance : Passed
Info	46180	Additional DNS Hostnames
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	60020	PCI DSS Compliance : Handling False Positives

Vulnerability Criticality Descriptions

Critical = Should be addressed first in remediation plan: Vulnerability has the capability of allowing full and unauthorized network access

High = Should be addressed next in remediation plan based on organization's risk tolerance level: Allows for direct access to the internal network; could result in compromise of information

Medium = Should be addressed in remediation plan based on organization's risk tolerance level and business objectives: Risk of compromise, but unlikely; these could result in application, but not network access

Low = Should be reviewed and included in remediation plan at organization's discretion based on risk tolerance level, business objectives, and resource availability: Unlikely risk of compromise of application, OS, and network resources

Appendix 2: Web Application Scans

These are the Arachni results from the web application scans. There are no findings in this scan that are going to invalidate the PCI DSS version 3.2 compliance.

Exposed localstart.asp page: Low Severity

To restrict access to specific pages on a webserver, developers can implement various methods of authentication, therefore only allowing access to clients with valid credentials. There are several forms of authentication that can be used. The simplest forms of authentication are known as Basic and Basic Realm. These methods of authentication have several known weaknesses such as being susceptible to brute force attacks. Additionally, when utilizing the NTLM mechanism in a windows environment, several disclosures of information exist, and any brute force attack occurs against the servers local users, or domain users if the web server is a domain member. Cyber-criminals will attempt to locate protected pages to gain access to them and also perform brute force attacks to discover valid credentials. Arachni discovered the following page requires NTLM based basic authentication in order to be accessed.

Vector type	HTTP method	Action
server	GET	https://10.0.2.12/localstart.asp

Missing 'X-Frame-Options' header: Informational Severity

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Vector type	HTTP method
Server	GET

Interesting response: Informational Severity

The server responded with a non 200 (OK) nor 404 (Not Found) status code. This is a non-issue, however exotic HTTP response status codes can provide useful insights into the behavior of the web application and assist with the penetration test.

Vector type	HTTP method	Action
Server	GET	https://10.0.2.12/localstart.asp

Appendix 3: PI Achievers' Tool list

Table 2: PI Achievers' Assessment Tools

Tool	Platform	Purpose
Wireshark	Linux	Packet Analyzer (GUI)
Eye P.A.	Windows	Wireless data visualization
Nessus	OSX	Vulnerability scanner
Pentoo	Linux	Custom penetration testing platform
Nmap	OSX	Port scanning tool
Aircrack Suite	Linux	Wireless enumeration
Custom scripts	All	Developed as needed
MSF Framework	Linux	Validating vulnerabilities
IP Technology Tunnels	Linux	Command and Control
Arachni	OSX	Web application scanner
Skipfish	Linux	Web application scanner