Platform Compliance Vulnerability Assessment

For

October 6, 2020

Submitted to:

IPTL
Gary Mitchell
Vice President Engineering
gary@IPTechnologyLabs.com
301-570-6611

Submitted by:

Process Improvement Achievers, LLC
Rick Mellendick
Chief Security Officer
Process Improvement Achievers, LLC
rmellendick@piachievers.com
443-895-5454

Table of Contents

Executive Summary

At the direction of IP Technology Labs (IPTL), Process Improvement Achievers, LLC (PI Achievers) was contracted to perform an independent platform compliance vulnerability assessment. The assessment began on June 25, 2020 and was completed Friday, September 30, 2020. As part of the services that were provided, PI Achievers conducted the vulnerability assessment for security compliance of the IPTL device capabilities, using the Fastlane platform as the basis of the testing: (Version iptl_m770_fw_100820_104629-4.3.14-5e).

This is not a certification assessment, but a compliance test to determine if the hardware and software that IPTL provides can be placed into a standards compliant network and enhance or maintain the high level of security that the network had prior to use of the IPTL devices. IPTL devices in and of themselves cannot be compliance certified for most compliance standards, (i.e. PCI, 508, Soc 1/ SSAE 18, Soc 2, ISO 27001, NERC CIP, and others), the system is what is certified.

The IPTL network components meet or exceed the strict compliance guidelines of these certifications. Placing these devices on a certified network/system should not negate the compliance of the network. The IPTL hardware platforms, software and firmware conform to compliance guidelines.

The findings in this report are based upon the scan results and probing of the Fastlane series device. The scan results are the same results that an auditor or attacker would see during compliance auditing or attack. All data that was captured from the IPTL devices was used for the purposes of this out brief only. PI Achievers, in following U.S. Department of Defense (DOD) data destruction guidance (multiple passes with encryption enabled during the process), destroys raw data that is collected from each assessment once the assessment and out brief have been completed.

The assessment included all external IP addresses that have been provided by IPTL. This type of assessment gauges the risk posture of the hardware and software that could be used to leverage access to the data associated with IPTL. All vulnerabilities reported in this out brief were tested and validated.

The findings in this report are based upon the scan results and probing of the devices as well as a full scan of all services and any available web services within the address ranges and devices provided. The findings were broken down into three categories: Critical (0), High (0), and Medium (0). All results are included within this out brief including the nmap scans, web application scans, SSL scans, and Nessus scan data.

Scope, Approach, and Methodology

PI Achievers performed a Platform Compliance Vulnerability Assessment 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 this assessment using our standard testing methodology, which includes reconnaissance of the target, discovery of services, Radio Frequency (RF) testing and vulnerability scanning of the services discovered. The objective of the assessment was to enumerate any and all of the services found

on the IPTL devices and prioritize the vulnerabilities that could be exploited to gain unauthorized access to any of the IPTL devices or associated infrastructure. 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 Fastlane hardware based on PCI DSS 4. This assessment was not just a PCI audit but a full black box security test of the ports, protocols and services running on the device, along with the back end IPTL internet facing IP addresses. All testing was done in a repeatable way to alleviate any false positives and target directly on the services and sockets of the device. 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).

Findings and Recommendations

PI Achievers uses the guide below when determining criticality of a finding. The criticality is based on the vulnerability, absence of security control, system mis-configuration, or risk to data.

> **Critical** = Should be addressed first in the remediation plan based on the the client's risk tolerance level: A vulnerability exists, there is an absence of a security control, or there is a system mis-configuration which allows for full network access or denial of service, or which allows for data exfiltration, loss of data availability, or the compromise of data integrity.
>
> **High** = Should be addressed next in the remediation plan based on the client's risk tolerance level: A vulnerability exists, there is an absence of a security control, or there is system mis-configuration which could allow for network access, or which allows for data exfiltration, loss of data availability, or the compromise of data integrity.
>
> **Medium** = Should be addressed next in the remediation plan based on the client's risk tolerance level: A vulnerability exists which allows for loss of data availability or the compromise of data integrity, but there could be compensating controls in place to minimize the impact.

Service Performed	Critical	High	Medium	Grade
Vulnerability Assessment Results	**0**	**0**	**0**	**A+**

Automated and Manual Testing

Testing Configuration for the Fastlane test device:

- 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
- An internal NTP server was configured at NTP.PIAchievers.com

- DNS calls were ported to local DNS and monitored
- Connected on a closed network

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 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. A complete list of tools used during this assessment may be found in the Appendix 1.

SSL Scan

There were no significant findings with the SSL scan of the system. The raw results are in appendix 2.

NMAP

There are no significant findings with the NMAP (Port Scan) of the system. The raw results are in appendix 3.

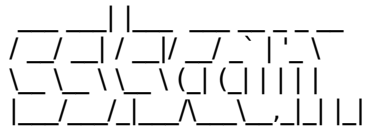
Nessus

The full PCI Internal and External results are in the raw data with an executive report in this outbrief as Appendix 4. Due to the nature of PCI DSS audits on security equipment there can be no common vulnerability scoring system (CVSS) score over a 4.0 for any vulnerabilities, this includes the Medium severity as well as Highs and Criticals. 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+. Nessus was also configured for deep web and web application inspection and network vulnerabilities in ports and protocols and services for the testing.

Appendix 1: Tools Used

Tool	Platform	Purpose
sipvicious	Linux	VoIP network spoofing
sipcrack	Linux	VoIP network encryption tool
sipdump	Linux	VoIP network traffic monitoring
VoIP Hopper	Linux	Tools used to collapse security VLANs
TCPdump	Linux	Remote traffic monitoring
bettercap	Linux	Man-in-the-Middle network spoofing
DNSrecon	Linux	DNS reconnaissance tool
Wireshark	Linux	Packet Analyzer (GUI)
Arachni	Linux	Web vulnerability spider scanner
nmap	OSX	Port scanning tool
Nessus	Linux	Vulnerability scanner
Custom scripts	All	Developed as needed
Aircrack-ng suite	Linux	Wireless vulnerability and system scanner
MDK3	Linux	Wireless stress testing software
Eye P.A.	Windows	Wireless pcap scanner
Channelizer	Windows	Wireless packet capture tool
InSSIDer	Windows	Wireless data evaluation tool
Spike	Windows	Radio Frequency spectrum analyzer
SSH/SCP/NC	All	Network communication and exfiltration tools
Hak5 Pineapple	Linux	Wireless Man in the Middle tools
ESP Key	Linux	Badging system control software
Prox3	Linux	Badge cloning software
Metasploit	All	Exploitation tool
Hydra	Linux	Brute force password tool for services
Custom trojan software	Linux	Tools for exfiltration
Various physical tools	N/A	Tools for covert entry and exit of the physical location
Snark tap	Linux	Network tap
Responder	Linux	NetBios scanner
netDiscover	Linux	Network based enumeration tool
Bettercap	Linux	Network Man-in-the-middle testing tool
Veracrypt	All	Data encryption tool
Kismet	Linux	RF assessment tool
BlueHydra	Linux	Bluetooth assessment tool
BlueSonar	Linux	Bluetooth assessment tool
Netcat	All	Socket testing tool
Netdiscover	Linux	Network enumeration tool
SpoofCard	Web	Phishing tool
Gqrx	Linux	Software defined radio scanner
Apple_Bleee	Linux	Apple device assessment tool
RTL_433	Linux	RF assessment tool
Dump_1090	Linux	RF assessment tool
SRSLTE	Linux	Phone assessment tool
Mimikatz	Linux	Password assessment tool

Appendix 2: SSL Scan



ssl scan IPTL Device
Version: 1.11.13-static
OpenSSL 1.0.2-chacha (1.0.2k-dev)
Connected to IPTL Device
Testing SSL server IPTL Device on port 443 using SNI name IPTL Device

TLS Fallback SCSV:
Server supports TLS Fallback SCSV
TLS renegotiation:
Session renegotiation not supported
TLS Compression:
Compression disabled

Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 2048 bits
Accepted TLSv1.2 256 bits AES256-GCM-SHA384
Accepted TLSv1.2 256 bits AES256-SHA256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA DHE 2048 bits
Accepted TLSv1.2 256 bits AES256-SHA

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: *.iptechnologylabs.com
Altnames: DNS: *.iptechnologylabs.com, DNS:iptechnologylabs.com
Issuer: RapidSSL RSA CA 2018

Not valid before: Jan 29 00:00:00 2020 GMT
Not valid after: Jan 28 12:00:00 2022 GMT

Appendix 3: Ports and Protocol Scan

Nmap scan report for 10.0.2.116
Host is up (0.0062s latency).
Not shown: 65534 closed ports
PORT STATE SERVICE VERSION
53/tcp open domain dnsmasq 2.76
| dns-nsid:
| NSID: ott-node18.dns.fgd.corp.fortinet.com
(6f74742d6e6f646531382e646e732e6667642e636f72702e666f7274696e65742e636f6d)
| id.server: ott-node18.dns.fgd.corp.fortinet.com
|_ bind.version: dnsmasq-2.76
80/tcp open http Apache httpd
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ Digest charset=UTF-8 realm=Device Login qop=auth
nonce=5eff7245:07c95f7006bdd06b2d8df59a40a23a6e
|_http-server-header: Apache
|_http-title: 401 Unauthorized

Appendix 4: Vulnerability Scan

piachievers

PI Achievers Vulnerability Report
Report generated by Nessus™

IPTL_7X_Scan
Wed, 30 Sep 2020 21:12:29 EDT

TABLE OF CONTENTS

Hosts Executive Summary

Collapse All | Expand All

10.0.2.116

0	0	0	0	15
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	14788	IP Protocols Scan
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	40472	PCI DSS compliance : options settings
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information

Hide Details