Pitney Bowes

SmartLink™ PB-4000

Network Attached Peripherals Security (NAPS) Certification Testing Report

November 11, 2021

Executive Summary

ICSA Labs recently completed Network Attached Peripherals Security (NAPS) certification testing against the Pitney Bowes SmartLink™ PB-4000 communication device. Pitney Bowes describes the device as follows:

> SmartLink™ connects your digital postage meter to the Pitney Bowes Commerce Cloud. The device is compatible with mailstation2™. SmartLink™ uses your internet connection to sync with the Pitney Bowes Data Center to download postal rate updates, refill postage, and update software.

Following the recently-completed security testing test cycle, ICSA Labs continues to maintain that Pitney Bowes designed and built a versatile communication solution with security in mind. **ICSA Labs is pleased to announce that the Pitney Bowes SmartLink™ PB-4000 has retained ICSA Labs Network Attached Peripherals Security (NAPS) Certification**.

Tested Device

ICSA Labs successfully completed testing of the SmartLink™ on:

UIC Version 38.17

Scope of NAPS Security Testing

ICSA Labs uses a Security Testing Framework as the basis for NAPS security certification testing. The framework contains 6 categories of testing elements – Alerting/Logging, Authentication, Communications, Cryptography, Physical Security, and Platform Security. From this framework, ICSA Labs applies a set of security and privacy testing requirements appropriate for the particular kind of NAPS device being tested. In the case of the Pitney Bowes SmartLink™ PB-4000, the requirements listed in Appendix 1 were selected by ICSA Labs and served as the basis for security testing.

The SmartLink™ PB-4000 has wired and wireless networking and a USB port. Configuration was accomplished as explained in the "Setup" section below.

Set Up

The initial network configuration is accomplished by visiting https://setup.smartlink.pitneybowes.com/connection and following the on screen prompts. When configuring the WIFI interface, the settings (SSID and network password) are sent to the device by flashing light. There is no configuration needed for the wired network interface unless the Advanced Setup option is selected. ICSA Labs chose to test the SmartLink™ PB-4000 using the wired Ethernet interface with the Advanced Setup option. This enabled setting a static IP address, default gateway and DNS server.

Findings

Below are the 6 categories of testing elements taken from ICSA Labs' Security Testing Framework that is the basis for ICSA Labs NAPS security certification testing. Noteworthy items shedding light on the product or the testing performed by ICSA Labs is included alongside each category.

During testing, ICSA Labs extracted the Pitney Bowes server public TLS v.1.2 key from packet captures. This certificate was then hosted on a local system with a mismatched private key. Communication from the SmartLink PB-4000 device was redirected to the local system to see if the device would properly validate the certificate. Once a connection was attempted the connection was aborted due to the invalid certificate.

Alerting/Logging	Authentication	Communications
There is no logging functionality in the network adapter.	The Pitney Bowes SmartLink™ PB-4000 device does not utilize remote authentication.	Communications from the LAN ports utilize TLSv1.2 algorithms. The only non-encrypted communications observed were DNS requests. All other observed communication from the device utilized TLS V1.2
Cryptography	**Physical Security**	**Platform Security**
The SmartLink™ PB-4000 device supports 3 TLS cipher suites. This was determined by capturing traffic between the SmartLink and a Pitney Bowes private cloud server. The server selects a cipher suite from the list of 3. ICSA Labs observed the Server respond with NIST approved cipher suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256.	No physical security requirements were tested. It is ICSA Labs' view that – given the typical deployment environment for the SmartLink™ PB-4000 – that there will be compensating controls protecting the device from tampering as well as restricting access to its physical interfaces.	There were no listening ports found during testing on the SmartLink™ PB-4000 device.

Conclusion

Following successful security testing, the Pitney Bowes SmartLink™ PB-4000 met the requirements against which it was tested to retain ICSA Labs Network Attached Peripherals Security (NAPS) Certification.

Appendix 1

Below we list the requirements chosen by ICSA Labs from its Security Testing Framework that were tested during this engagement.

1. In the case of cryptography, MUST support:
    a. FIPS 140-2 approved algorithms;
    b. NIST-recommended cryptographic strength requirements (NIST SP 800-131A);
    c. NIST-recommended cipher suites (NIST SP 800-52 rv1);
2. MUST be invulnerable to exploits known within the information security community.
3. MUST support standards-based secure protocols that provide authentication, data confidentiality, data integrity, and replay protection to safeguard administrative traffic.
4. MUST support authentication for administrative access.

Note that there are testing elements in the Security Testing Framework not listed above that ICSA Labs intentionally excluded from this engagement. Any such testing element found in the framework but not listed above:

a. is not sufficiently relevant,
b. is outside the scope of the testing contract, or
c. sufficient compensating controls exist in the environment where the device is typically deployed precluding the need to test it.

Examples of compensating controls are protection from traditional network security products such as a network firewall and/or an advanced threat defense solution.

Authority

This report is issued by the authority of the General Manager, ICSA Labs. Tests are performed under normal operating conditions.

Darren Hartman

Darren Hartman, General Manager, ICSA Labs

ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For over 30 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

www.icsalabs.com

Pitney Bowes

Pitney Bowes is a global technology company powering billions of transactions – physical and digital – in the connected and borderless world of commerce. Clients around the world, including 90 percent of the Fortune 500, rely on products, solutions, services and data from Pitney Bowes in the areas of customer information management, location intelligence, customer engagement, shipping, mailing, and global ecommerce.

www.pitneybowes.com