CERTIFICATION REPORT

Network-Connected Postage Meter

Pitney Bowes
SendPro C-Series

Mailing Version: 1.0.35.2241b.penumbraBuild #:2243
SendPro™ Version: 2.0.114DBuild #:20113
Base SW Version: 03.03.1046

Issued On: Tuesday December 19th, 2023
Expires On: Sunday June 16th, 2024
Name: Travis Spann
Title: President

Travis Spann

This document shall not be used to claim product certification, approval, validation, or endorsement by any agency of the Federal Government. This document shall not be used to claim product approval, validation, or endorsement by AEGISOLVE, INC. This document may only be reproduced in its entirety without revision. The results only relate to the item(s) tested.

Revision History		
Document_Revision	Author	Description
Network-Connected Postage Meter Certification Report (Pitney_Bowes_23.12.19_V1.0)	Travis Spann	Initial release.

Table of Contents

Introduction

AEGISOLVE, INC. conducts certification testing to provide independent and unbiased third-party assurance that network-connected postage meter devices can meet industry accepted best security practices when installed and configured properly. Postage meter devices are verified to meet a set of testable requirements, which are publicly available.

Summary of Requirements

To attain certification the postage meter must pass a rigorous set of tests that verify that each of the following requirements are met.

- The postage meter uses industry accepted standards-based security protocols, which provide confidentiality, integrity, and authenticity for network-based communications.
- Standard-based cryptographic algorithms with sufficient strength that meet standards bodies recommendations are employed.
- No sensitive information is exposed in any non-secure communications.
- Strong administrative and user authentication is enforced, where applicable.
- If supported, logging is accurate and provides sufficient detail for authentication and other notable events.
- If remote device upgrades are supported, the postage meter relies on the secure communication capability to download the software upgrade.
- Known remotely exploitable vulnerabilities have been mitigated in the certified version listed in this report.

Certification testing does not necessarily determine that any identified features and functions of the product(s) under test, the overall product(s) under test, or any untargeted features and functions of the product(s) under test are free from security vulnerabilities or whether other relevant aspects operate adequately or correctly.

Product Description

The SendPro C-Series Mailing System is the simplest, all-in-one technology for office mailing and package shipping. It's a complete sending solution that makes it easy to process mail and send packages all from one place.

Summary of Findings

Pitney Bowes SendPro C-Series (Mailing Version: 1.0.35.2241b.penumbraBuild #:2243, SendPro™ Version: 2.0.114DBuild #:20113, Base SW Version: 03.03.1046) has successfully passed all applicable tests attaining the AEGISOLVE Network-Connected Postage Meter Certification.

Detailed Test Report

Test Configuration
The SendPro C-Series was installed into the test network as it would be installed in an end-user's network, in accordance with the Pitney Bowes administrative guidance. The test network was configured to monitor and capture all communications to and from the SendPro C-Series. Also, the test network was capable of intercepting and modifying traffic to thoroughly verify the proper implementation of security protocols and cryptographic algorithms, ensuring that the requirements were satisfied.

NOTE 1: The following services were not tested and are out-of-scope of this certification testing:
- Install scale (scale accessories are not applicable and out-of-scope)
- Print shipping label (print accessories are not applicable and out-of-scope)
- Printing an international label (print accessories are not applicable and out-of-scope)
- Print return label (print accessories are not applicable and out-of-scope)
- Print scan form (print accessories are not applicable and out-of-scope)
- Reprint label (print accessories are not applicable and out-of-scope)
- Cancel label (print accessories are not applicable and out-of-scope)
- Getting refund for label (print accessories are not applicable and out-of-scope)
- Using the scale (scale accessories are not applicable and out-of-scope)
- Zeroing the scale (scale accessories are not applicable and out-of-scope)

Security Protocol and Cryptography Implementation
During initial power-on, normal operations, and device upgrades packet captures of all communications were analyzed. Through packet analysis, review of the Pitney Bowes supplied documentation, and configuration settings, it was determined that the SendPro C-Series initially supported the following security protocols and strengths:

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

NOTE 2: We observed when the meter initiated a session, it offered non-Approved TLS cipher suites, however the communication was ultimately secured and established with a strong TLS cipher suite (e.g. TLS v1.2 with TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) by the TLS Server.

NOTE 3: It was determined by review of Pitney Bowes (PB) documentation and via functional testing that the meter connects to current PB servers/infrastructure (Version 1.2.72). Via functional testing it was determined that the Product Under Test (PUT) properly validated the PB server certificate, and that the PB server correctly enforced the use of an acceptable cipher suite as aforementioned in NOTE 2. Given that the PB server was able to correctly enforce the expected security policy onto the PUT (i.e. force the PUT to not connect using unacceptable ciphers) the high-level requirement for sufficiently secure communication is satisfied.

NOTE 4: The behavior of the PUT when connected to alternate PB's servers/infrastructure remains unknown and is out of scope of the certification.

The SendPro C-Series used non-secure protocols, HTTP, for non-sensitive communications such as generate_204 which is just a simple request to test if the network is ready to use, no sensitive data is exchanged here.

NOTE 5: Module arrived on site preconfigured.

Authentication
The SendPro C-Series supports a strong authentication mechanism for administrative and user authentication:

- Complex passwords

The SendPro C-Series securely implemented the authentication method above and prevented any attempts to circumvent the authentication mechanism. The SendPro C-Series supports administrative level roles.

NOTE 6: User Authentication is required for use of the SendPro Shipping Application and must be previously established outside of the machine. Mailing operations use the HW cryptographic module to provide secure device level authentication from the machine to PB infrastructure for key postal support operations.

Remote Upgrades
The SendPro C-Series supports remote upgrades. Upgrades are automatically received and can also be manually triggered via the rates and updates service through the GUI.

During the upgrade process, the communication to the remote server is secured by the protocol as described in the *Security Protocol and Cryptography Implementation* of this report.

NOTE 7: Tester required manufacturer support to perform remote upgrades. After some updates on their end, Aegisolve was able to perform the update service to enable some previously locked services.

Mitigation of Known Vulnerabilities
Through review of Pitney Bowes Security Advisories, research of public Vulnerabilities Databases, and vulnerability testing, no remotely exploitable vulnerabilities were discovered in the SendPro C-Series with versions listed above.

Initially, non-essential services were found to be listening on port 443. Pitney Bowes stated the listening service is required for a test configuration tool to interact with the system after it is manufactured and has no known vulnerabilities. During testing, no attempts to exploit the service succeeded.

NOTE 8: The tester performed several security scans and found no exploitable vulnerabilities.

About Pitney Bowes

Pitney Bowes is a global shipping and mailing company that provides technology, logistics, and financial services to more than 90 percent of the Fortune 500. Small business, retail, enterprise, and government clients around the world rely on Pitney Bowes to reduce the complexity of sending mail and parcels.

About AEGISOLVE

The AEGISOLVE mission is to develop, augment, and accelerate cybersecurity analysis and testing processes in ever-changing technological landscapes. Headquartered in Knoxville, Tennessee, AEGISOLVE is a trusted, independent, third-party laboratory providing critical testing and cybersecurity services to a wide array of industries since 2007. We're your direct partner and testing authority for all things cybersecurity. AEGISOLVE guides your organization through the challenges of cybersecurity compliance without the need for expensive consultants - i.e., the "middle-men".