National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Pulse Secure, LLC

Pulse Connect Secure 8.2R4.10 running on the PSA300, PSA3000, PSA5000, PSA7000c, PSA7000f, MAG2600, MAG4610, MAG-SM160, and MAG-SM360 Platforms

Report Number: CCEVS-VR-VID10821-2017
Dated: **September 20, 2017**
Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Panel

Patrick W. Mallett, PhD

MITRE Corp, McLean, VA

Kenneth Stutterheim

The Aerospace Corporation, Columbia, MD

Common Criteria Testing Laboratory

Michael C. Baron

Ryan Day

UL Verification Services Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the Pulse Connect Secure 8.2R4.10

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The TOE is classified as a Network Device (a generic infrastructure device that can be connected to a network). The TOE is an infrastructure network device that provides secure remote management, auditing, and updating capabilities. The TOE provides secure remote management using a HTTPS/TLS web interface. The TOE generates audit logs and transmits the audit logs to a remote syslog server over a mutually authenticated TLS channel.

The TOE consists of the following hardware:

- PSA300, PSA3000, PSA5000, PSA7000c, PSA7000f, MAG2600, MAG4610, MAG-SM160, and MAG-SM360

Running the following software:

- Pulse Connect Secure 8.2R4.10

The TOE's operational environment must provide the following services to support the secure operation of the TOE:

- DNS Server
- Local Console
- Syslog Server
- Web Browser
- CRL Server
- [MAG-SM160 and MAG-SM360 only] Chassis, one of:
    - MAG6610
    - MAG6611

This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
DNS Server	Conformant with RFC 1035
Local Console	RS-232 Serial Console

Syslog Server	○ Conformant with RFC 5424 (Syslog Protocol) ○ Supporting Syslog over TLS (RFC 5425) ○ Acting as a TLSv1.1 and/or TLSv1.2 server ○ Supporting Client Certificate authentication ○ Supporting at least one of the following cipher suites: ▪ TLS_RSA_WITH_AES_128_CBC_SHA ▪ TLS_RSA_WITH_AES_256_CBC_SHA ▪ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ▪ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ▪ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ▪ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ▪ TLS_RSA_WITH_AES_128_CBC_SHA256 ▪ TLS_RSA_WITH_AES_256_CBC_ SHA256 ▪ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ▪ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ▪ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ▪ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Web Browser	○ Internet Explorer 11, Google Chrome 50, or Firefox 38 ○ Supporting TLSv1.1 and/or TLSv1.2 ○ Supporting at least one of the following ciphersuites: ▪ TLS_RSA_WITH_AES_128_CBC_SHA ▪ TLS_RSA_WITH_AES_256_CBC_SHA ▪ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ▪ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ▪ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ▪ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ▪ TLS_RSA_WITH_AES_128_CBC_SHA256 ▪ TLS_RSA_WITH_AES_256_CBC_ SHA256 ▪ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ▪ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ▪ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ▪ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
CRL Server	CRL Server conformant with RFC 5280
[MAG-SM160 and MAG-SM360 only] Chassis, one of the following components listed in the column to the right	○ MAG6610 ○ MAG6611

Table 1: Operational Environment Components

2 Identification of the TOE

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE), the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Pulse Connect Secure
Protection Profile	collaborative Protection Profile for Network Devices, Version 1.0, dated February 27, 2015 [NDcPP]
Security Target	Pulse Connect Secure Security Target, Version 1.0, September 5, 2017
Dates of Evaluation	May 2016 – September 2017
Conformance Result	Pass
Common Criteria Version	3.1r4
Common Evaluation Methodology (CEM) Version	3.1r4
Evaluation Technical Report (ETR)	17-3624-R-0026 V1.1
Sponsor/Developer	Pulse Secure, LLC
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc.
CCTL Evaluators	Michael C. Baron, Ryan Day
CCEVS Validators	Patrick W. Mallett, PhD; Kenneth Stutterheim

Table 2: TOE Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before

July 12, 2017.

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

- Audit
- Cryptography
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

4.1 Audit

The TOE generates audit records for security relevant events. The TOE maintains a local audit log as well as sending the audit records to a remote Syslog server. Audit records sent to the remote server are protected by a TLS connection. Each audit record includes identity (username, IP address, or process), date and time of the event, type of event, and the outcome of the event. The TOE prevents modification to the local audit log.

4.2 Cryptographic Operations

The TOE implements CAVP validated cryptographic algorithms for random bit generation, encryption/decryption, authentication, and integrity protection/verification. These algorithms are used to provide security for the TLS and HTTPs connections as well as verifying firmware updates.

4.3 Identification and Authentication

The TOE authenticates administrative users using a username/password or username/X.509 certificate combination. The TOE does not allow access to any administrative functions prior to successful authentication.

The TOE supports passwords consisting of alphanumeric and special characters and enforces minimum password lengths. The TSF supports and certificates using RSA or ECDSA signature algorithms.

The TOE allows only users to view the login warning banner and send/receive ICMP packets prior to authentication.

4.4 Security Management

The TOE allows users with the Security Administrator role to administer the TOE over a remote web UI or a local CLI. These interfaces do not allow the Security Administrator to execute arbitrary commands or executables on the TOE.

The TOE can also receive configuration updates from an optional Pulse One management server in the environment.

4.5 Protection of the TSF

The TOE implements a number of self-protection mechanisms. It does not provide an interface for the reading of secret or private keys. The TOE ensures timestamps, timeouts, and certificate checks are accurate by maintaining a real-time clock as well as requiring the Security Administrator to update the clock once a month to minimize drift. Upon startup, the TOE runs a suite of self-tests to verify that it is operating correctly. The TOE also verifies the integrity and authenticity of firmware updates by verifying a digital signature of the update prior to installing it.

4.6 TOE Access

The TOE can be configured to display a warning and consent banner when an administrator attempts to establish an interactive session over the local CLI or remote web UI. The TOE also enforces a configurable inactivity timeout for remote and local administrative sessions.

4.7 Trusted Path/Channels

The TOE uses TLS to provide a trusted communication channel between itself and remote Syslog and any optional Pulse One servers that may be present in the environment. The trusted channel with the Syslog server utilizes X.509 certificates to perform mutual authentication. If the environment contains a Pulse One server, the trusted channel for authentication would utilize HAWK authentication to perform mutual authentication. The TOE initiates the TLS trusted channel with both types of remote server.

The TOE uses HTTPs/TLS to provide a trusted path between itself and remote administrative users. The TOE does not implement any additional methods of remote administration. The remote administrative users are responsible for initiating the trusted path when they wish to communicate with the TOE.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

Table 3: Assumptions

Assumption	Description
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.

Table 3: Assumptions	
Assumption	Description
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose Applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

Table 4: Threats	
Threat	Description
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks,

Table 4: Threats	
Threat	Description
	etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

Table 5: Organizational Security Policies	
OSP	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

6 Architectural Information

The TOE is classified as Network Device for Common Criteria purposes.

6.1 Architecture Overview

The TOE consists of hardware and software components.

6.1.1 TOE Hardware

The TOE consists of the following hardware:

- PSA300, PSA3000, PSA5000, PSA7000c, PSA7000f, MAG2600, MAG4610, MAG-SM160, and MAG-SM360

6.1.2 TOE Software

The TOE runs the following software:

- Pulse Connect Secure v8.2R4.10

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Pulse Policy Secure TOE. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

The guidance documents are provided to the product consumer via download from a web-based customer portal provided by the vendor. These documents apply to the CC Evaluated configuration:

7.1 Design Documentation

Document	Revision	Date
AssuranceDocument	1.4	August 5, 2016

7.2 Guidance Documentation

Document	Revision	Date
Pulse Connect Secure Operational User Guidance and Preparative Procedures, Pulse Secure LLC	0.6	June 5, 2017
PSA300 Hardware Guide	1.0	April 2016
PSA3000 Hardware Guide	1.0	April 2016

Document	Revision	Date
PSA5000 Hardware Guide	1.0	April 2016
PSA7000 Hardware Guide	1.0	April 2016
MAG Series Pulse Secure Gateways Hardware Guide	1.0	September 2015

7.3 Test Documentation

Document	Revision	Date
16-3624-R-0059	1.4	September 13, 2017

7.4 Vulnerability Assessment Documentation

Document	Revision	Date
16-3624-R-0059	1.4	September 13, 2017

7.5 Security Target

Document	Revision	Date
Pulse Connect Secure Security Target	1.0	September 5, 2017

Please note that any other documentation delivered with the product or that may be accessible on-line that is not listed above was not included in the scope of the evaluation nor was it used to set the product into its evaluated configuration, and therefore should not be relied upon to place the device into the compliant configuration.

8 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

8.1 Developer Testing

No testing was performed by the developer.

8.2 Evaluation Team Independent Testing

The evaluation team performed the independent testing activities to confirm the TOE operates to the TOE security functional requirements as specified in the ST for a product claiming

conformance to the collaborative Protection Profile for Network Devices Version 1.0, 27 February 2015 (NDcPP). The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in NDcPP. The Test Plan described how each test activity was to be performed. The evaluation team executed the tests specified in the Test Plan and documented the results in 'Test Document' listed above in Section 7.3.

Independent testing was performed at the UL facility in San Luis Obispo, CA. The evaluators received two platforms identified in the TOE. The hardware/software was provided in the same form that normal customers would receive it. The evaluator installed and configured the TOE in accordance with the vendor provided guidance documentation, and performed the testing procedures as described in the Test Documentation.

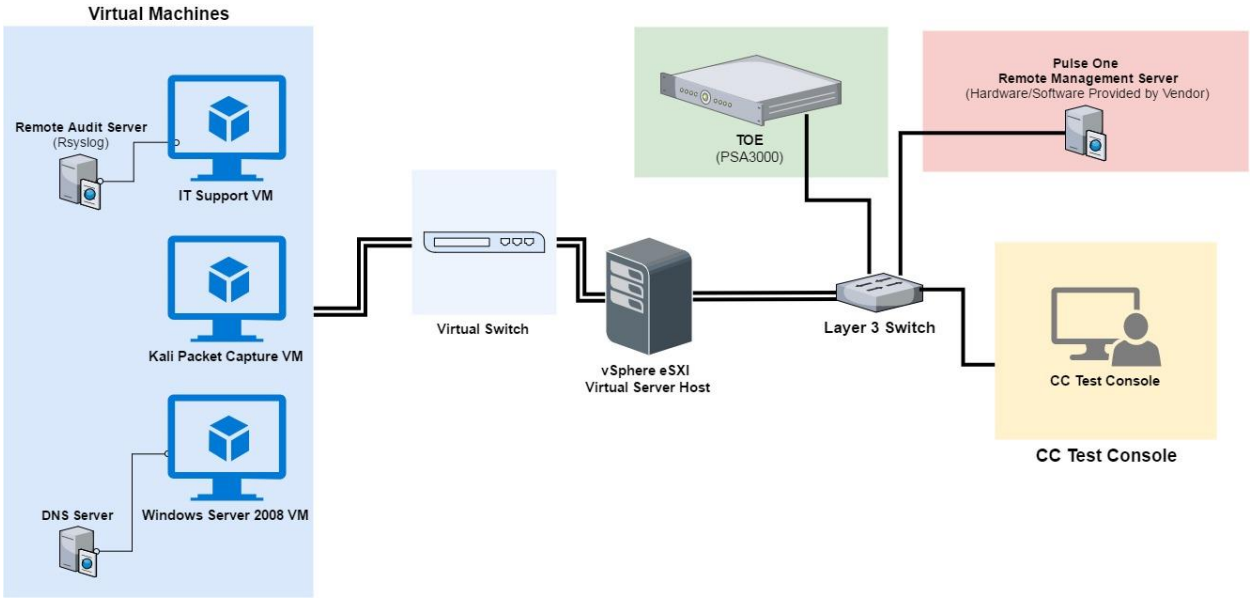

Figure 1 – Functional Testing Components Diagram

8.3 Vulnerability Analysis

The evaluation team performed a vulnerability assessment and penetration testing based on an initial port scan of the TOE. This comprehensive port scan identified any and all open ports and acquired all possible identifying information from the TOE. This information was compared to those services listed in the ST, and used as input into the public domain search. This step was performed several times. For additional information, see the Evaluation Technical Report.

Based on the output from the port scan, CVEdetails.org and cve.mitre.org were searched with the following terms:

- Pulse Connect Secure
- Pulse Connect Secure 8.2R4.10
- pulse secure crypto library
- Pulse Secure Cryptographic Module 2.0
- IVE OS 2.0

Based on the results, no vulnerabilities existed in the TOE at the time of the evaluation that were exploitable. No third party libraries were identified.

8.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in collaborative Protection Profile for Network Devices, Version 1.0, dated February 27, 2015 and Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, Version 1.0, dated February 27, 2015 as performed by the evaluation team). All NIAP Technical Decisions related to the protection profile security functional requirements as of the date of test were considered and applied as necessary.
- This evaluation covers only the specific product and software versions identified in this document, and not any earlier or later versions either released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the collaborative Protection Profile for Network Devices, Version 1.0 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.

UL has determined that the TOE meets the security criteria in the Security Target. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in September 2017.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). Those employing the devices must follow the configuration

instructions provided in the Operational Guidance documentation listed above to ensure the evaluated configuration is established and maintained.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Security Target

Pulse Connect Secure Security Target, Version 1.0, September 5, 2017

12 Terms

12.1 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

12.2 Terminology

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 4, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 4, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 4, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 4, CCMB-2009-07-004.

[5] Common Criteria Evaluation Technical Report VID10821, 17-3624-R-0026 Version 1.1, September 13, 2017

[6] Assurance Activity Report, VID 10821 17-3624-R-0027 V1.1, September 13, 2017

[7] Pulse Connect Secure Operational User Guidance and Preparative Procedures, Version 0.6, June 5, 2017