Common Criteria

Certification Report

Aruba 2920 Switch Series, Version 5.011 WB\_15\_18\_0011I

 383-4-384

25 August 2016

Foreword

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian CC Scheme, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

Overview

The Canadian Common Criteria Scheme provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CygnaCom Solutions.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme, and to the Common Criteria portal (the official website of the International Common Criteria Project).

Table of Contents

Executive Summary 1

1 Identification of Target of Evaluation 2

1.1 Common Criteria Conformance 2

1.2 TOE description 2

1.3 TOE architecture 3

2 Security policy 4

2.1 Cryptographic functionality 4

3 Assumptions and Clarifications of Scope 5

3.1 Usage and Environmental assumptions 5

3.2 Clarification of Scope 5

4 Evaluated Configuration 6

4.1 Documentation 6

5 Evaluation Analysis Activities 7

5.1 Development 7

5.2 Guidance Documents 7

5.3 Life-cycle Support 7

6 Testing Activities 8

6.1 Assessment of Developer Tests 8

6.2 Conduct of Testing 8

6.3 Independent Functional Testing 8

6.4 Independent Penetration Testing 9

7 Results of the Evaluation 10

8 Supporting Content 11

8.1 List of Abbreviations 11

8.2 References 13

List of Figures

Figure 1 TOE Architecture 3

List of Tables

Table 1 TOE Identification 2

Table 2 Cryptographic Algorithm(s) 4

# Executive Summary

Aruba 2920 Switch Series, Version 5.011 WB\_15\_18\_0011I (hereafter referred to as the Target of Evaluation, or TOE), from Hewlett Packard Enterprise, was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE is a modular Ethernet switch, based on HPE Networking ASIC (application-specific integrated circuit), that in the evaluated configuration consists of the Aruba 2920 Switch Series. The TOE implements various networking protocols in Layer-2 and Layer-3. The TOE offers network management and interconnectivity functionality by offering nonblocking, line-rate Ethernet switching with Quality of Service (QoS) and a full complement of IPv4 and IPv6 features. The TOE consists of a hardware appliance with embedded software components.

CygnaCom Solutions is the CCEF that conducted the evaluation. This evaluation was completed on 11 July 2016 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Certified Products list (CPL) and the Common Criteria portal (the official website of the International Common Criteria Project).

# Identification of Target of Evaluation

The Target of Evaluation (TOE) is identified as follows:

1. TOE Identification

|  |  |
| --- | --- |
| TOE Name and Version | Aruba 2920 Switch Series, Version 5.011 WB\_15\_18\_0011IWB |
| Developer | Hewlett Packard Enterprise |
| Conformance Claim | **Protection Profile for for Network Devices, 08 June 2012, Version 1.1** |

## Common Criteria Conformance

 The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

## TOE description

The TOE is a modular Ethernet switch, based on HPE Networking ASIC (application-specific integrated circuit), that in the evaluated configuration consists of the Aruba 2920 Switch Series. The TOE implements various networking protocols in Layer-2 and Layer-3. The TOE offers network management and interconnectivity functionality by offering nonblocking, line-rate Ethernet switching with Quality of Service (QoS) and a full complement of IPv4 and IPv6 features. The TOE consists of a hardware appliance with embedded software components.

## TOE architecture

A diagram of the TOE architecture is as follows:



1. TOE Architecture

# Security policy

The TOE implements policies pertaining to the following security functional classes:

* Security Audit;
* Cryptographic Support;
* User Data Protection;
* Identification and Authentication;
* Security Management;
* Protection of the TOE Security Functionality (TSF);
* TOE Access; and
* Trusted Path/Channels.

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

## Cryptographic functionality

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in the TOE:

1. Cryptographic Algorithm(s)

|  |  |  |
| --- | --- | --- |
| Cryptographic Algorithm | Standard | Certificate Number |
| Advanced Encryption Standard (AES) | FIPS 197  | 3982 |
| Rivest Shamir Adleman (RSA) | FIPS 186-4 | 2043 |
| Secure Hash Algorithm (SHS) | FIPS 180-3  | 3287 |
| Keyed-Hash Message Authentication Code (HMAC) | FIPS 198 | 2598 |
| Component Validation List (CVL) | SP 800-131A | 811 |
| Deterministic Random Bit Generation (DRBG) | SP 800-90A | 1175 |

# Assumptions and Clarifications of Scope

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product’s installation and its operating environment. This will ensure the proper and secure operation of the TOE.

## Usage and Environmental assumptions

The following assumptions are made regarding the use and deployment of the TOE:

* There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE;
* TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner; and
* Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

## Clarification of Scope

* The TOE incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.
* The scope of this evaluation is limited to the specific device models and software versions identified in the ST, as well as the security functionality as specified in the NDPP.

# Evaluated Configuration

The evaluated configuration for the TOE comprises:

the Aruba 2920 Switch Series running ArubaOS version 5.011 on one of the following appliances:

* Aruba 2920-24G;
* Aruba 2920-24G-PoE+;
* Aruba 2920-48G;
* Aruba 2920-48G-PoE+; and
* Aruba 2920-48G-PoE+ 740W.

## Documentation

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

1. HPE Switch Software Management and Configuration Guide KB.15.18;
2. Aruba 2920 Switch Series Version 5.011 CC Configuration Guide version 0.9; and
3. HPE Switch Software Basic Operation Guide, July 2015.

# Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

##  Development

The evaluators analyzed the TOE functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the TOE security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

## Guidance Documents

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

## Life-cycle Support

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

# Testing Activities

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

## Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR.

The evaluators analyzed the developer’s test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification was complete.

## Conduct of Testing

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

## Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

1. PP Assurance Activities: The evaluator performed the assurance actvities listed in the claimed PP;

### Functional Test results

The developer’s tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

## Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

1. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST.

### Penetration Test results

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

# Results of the Evaluation

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

 The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

# Supporting Content

## List of Abbreviations

| Term | Definition |
| --- | --- |
| ASIC  | application-specific integrated circuit |
| BGP  | Border Information Protocol |
| CAVP | Cryptographic Algorithm Validation Program |
| CCEF | Common Criteria Evaluation Facility |
| CCS | Canadian Common Criteria Evaluation and Certification Scheme |
| CM | Configuration Management |
| CMVP | Cryptographic Module Validation Program |
| CSE | Communications Security Establishment |
| EAL | Evaluation Assurance Level |
| ETR  | Evaluation Technical Report |
| GC | Government of Canada |
| IT | Information Technology |
| ITS | Information Technology Security |
| ITSET | Information Technology Security Evaluation and Testing |
| IPV4 | Internet Protocol Version 4 |
| IPV6 | Internet Protocol Version 6 |
| PALCAN | Program for the Accreditation of Laboratories – Canada |
| POE+ | Power over Internet |
| PP | Protection Profile |
| QoS | Quality of Service |
| RIP | Routing Information Protocol |
| SFR | Security Functional Requirement |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |

## References

| Reference |
| --- |
| CCS Publication #4, Technical Oversight, Version 1.8, October 2010. |
| Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012. |
| Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012. |
| Aruba 2920 Switch Series Security Target Version 1.7, 25 August 2016 |
| Evaluation Technical Report for Aruba 2920 Switch Series Evaluation of the ST and the TOE version 0.2, 25 August 2016 |