Certification Report

Curtiss-Wright VPX3-685 Secure Routers v2.0.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-236-CR
Version:	1.0
Date:	05 November 2013
Pagination:	i to iii, 1 to 10

DISCLAIMER

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 Evaluation and Certification Scheme (CCS) – 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, apply 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 CCS, 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 Canada, 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 Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) 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 CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS 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 CGI IT Security Evaluation & Test Facility.

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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 05 November 2013, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

Curtiss-Wright VPX3-685 Secure Routers v2.0.0 (hereafter referred to as VPX3-685), from Curtiss-Wright Controls Defense Solutions, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

VPX3-685 is a single custom 3U VPX form factor blade running a fully-integrated software solution to provide switch, router, firewall, intrusion detection and prevention system, and VPN functionalities. The TOE comprises the entire VPX3-685 Secure Router software image, and all functions of the software image as well as the VPX3-685 secure router hardware.

The VPX3-685 provides several management and configuration interfaces. Remote administrators can connect to a web-based management graphical user interface (GUI) over an SSL session or use the command line interface (CLI) remotely over an SSH connection or SNMP v3. The CLI provides a robust environment that uses commands similar to the existing industry standard. The web GUI provides a subset of the commands that are available from the CLI.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 16 October 2013 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for VPX3-685, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security 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.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 2 *augmented* assurance requirements for the evaluated security functionality. 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.*   The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the VPX3-685 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is Curtiss-Wright VPX3-685 Secure Routers v2.0.0 (hereafter referred to as VPX3-685), from Curtiss-Wright Controls Defense Solutions.

2 TOE Description

VPX3-685 is a single custom 3U VPX form factor blade running a fully-integrated software solution to provide switch, router, firewall, intrusion detection and prevention system, and VPN functionalities. The TOE comprises the entire VPX3-685 Secure Router software image, and all functions of the software image as well as the VPX3-685 secure router hardware.

The VPX3-685 provides several management and configuration interfaces. Remote administrators can connect to a web-based management graphical user interface (GUI) over an SSL session or use the command line interface (CLI) remotely over an SSH connection or SNMP v3. The CLI provides a robust environment that uses commands similar to the existing industry standard. The web GUI provides a subset of the commands that are available from the CLI. Through these connections administrators are able to configure and manage switching rules, access control lists (ACLs) and to create or modify the firewall rules to be enforced.

A detailed description of the VPX3-685 architecture is found in Section 1.6 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for VPX3-685 is identified in Section 1.6 of the ST.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
VPX3-685 Secure Routers	*Pending* [2]

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in VPX3-685:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple DES (TDES)	ANS X9.52	758, 1433
Advanced Encryption Standard (AES)	FIPS 197	963, 2217
Rivest Shamir Adleman (RSA)	FIPS 186-2	1135
Secure Hash Algorithm (SHA-1)	FIPS 180-2	934, 1906, 1907
Keyed-Hash Message Authentication	FIPS 198	538, 1401

[2] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

Code (HMAC)		
ANSI x9.31 PRNG	ANSI x9.31	1111
Digital Signature Algorithm (DSA)	FIPS 186-2	713

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Curtiss-Wright Controls Defense Solutions VPX3-685 Secure Router Security Target
Version: v1.15
Date: 18 October 2013

5 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.*

VPX3-685 is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:

- FAU_STG_EXT.1 - External Audit Trail Storage;
- FCS_CKM_EXT.4 - Cryptographic key destruction;
- FCS_COMM_PRO_EXT.1 - Communication Protection;
- FCS_HTTPS_EXT.1 – HTTPS;
- FCS_IPSEC_EXT.1 – Ipsec;
- FCS_RBG_EXT.1 - Cryptographic Operation (Random Bit Generation);
- FCS_SSH_EXT.1 – SSH;
- FCS_TLS_EXT.1 – TLS;
- FIA_PMG_EXT.1 - Password Management;
- FIA_UAU_EXT.5 - Password-based Authentication Mechanism;
- FIA_UIA_EXT.1 - User Identification and Authentication;
- FPT_PTD_EXT.1 - Management of TSF Data;
- FPT_TST_EXT.1 - TSF self test;
- FPT_TUD_EXT.1 - Trusted Update;
- FTA_SSL_EXT.1 - TSF-initiated session locking;
- IDS_ANL_EXT.1 – Analysis;
- IDS_RCT_EXT.1 - Analyzer react;
- IDS_RDR_EXT.1 - Restricted data review; and

- IDS_SDC_EXT.1 - System data collection

b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and

c. *Common Criteria EAL 2 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

VPX3-685 implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Section 7 of the ST.

In addition, VPX3-685 implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of VPX3-685 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- 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; and
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment; and
- The TOE router controls the single access point to the trusted network and that there are no hostile entities on the trusted network side.

8 Evaluated Configuration

The evaluated configuration for VPX3-685 comprises:

- The TOE software running on;
- a VPX-compliant/custom chassis
  - VPX3-685-A13014-FC;
  - VPX3-685-C23014-FC;
  - VPX3-685-A13020-FC; or
  - VPX3-685-C23020-FC.
- a power supply
- an administrator workstation with an SSH/HTTPS client
- an external syslog server

The publication entitled Curtiss-Wright Controls Defense Solutions VPX3-685Secure Routers Guidance Documentation Supplement, version 0.9, October 16, 2013 describes the procedures necessary to install and operate VPX3-685 in its evaluated configuration.

9 Documentation

The Curtiss-Wright Controls Defense Solutions documents provided to the consumer are as follows:

a. Curtiss-Wright Controls Defense Solutions VPX3-685 Secure Routers Security Target, version 1.15, October 18, 2013;

b. Curtiss-Wright Controls Defense Solutions VPX3-685 Secure Routers Guidance Documentation Supplement, version 0.8, July 9, 2013;

c. Curtiss-Wright Controls Defense Solutions VPX3-685 Secure Ethernet Router User’s Manual, Document Number: 825947, Version 4, June 2012;

d. Curtiss-Wright Controls Defense Solutions VPX3-685 Command Line Interface (CLI) Software Reference Manual, Document Number: 826390, Version 3, June 2012;

e. Curtiss-Wright Controls Defense Solutions VPX-685 Web Interface Software Reference Manual, Document Number: 826391, Version 2, May 2012;

f. Curtiss-Wright Controls Defense Solutions VPX3-685 14/17/20 Port Secure Ethernet Router Controlled Information User’s Manual, Document Number: 828333, Version 2, June 2012; and

g. Curtiss-Wright Controls Defense Solutions, IPMI User Guide, Document Number: 826691, Version 2, May 2012.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of VPX3-685, including the following areas:

Development: The evaluators analyzed the VPX3-685 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 VPX3-685 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 VPX3-685 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.

Life-cycle support: An analysis of the VPX3-685 configuration management system and associated documentation was performed. The evaluators found that the VPX3-685 configuration items were clearly marked. The developer’s configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of VPX3-685 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the VPX3-685. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of VPX3-685. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify VPX3-685 potential vulnerabilities. The evaluators identified potential vulnerabilities; subsequent to follow-on penetration testing (ref: section 11.3) it was verified that none of the potential vulnerabilities were exploitable in the operational environment for VPX3-685.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

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

11.1 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[3].

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.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of CGI IT Security Evaluation & Test Facility test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. VPN functionality: The objective of this test goal is to verify the functionality of the VPN and demonstrate either the correct functionality of the VPN endpoint and show that the TOE logs the appropriate messages when an event occurs;

c. SSH Testing: The objective of this test goal is to verify the functionality of the Secure Shell (SSH);

d. Firewall (IPv6): The objective of this test goal is to verify the IPv6 firewall functionality;

e. Information Flow Control Rules: The objective of this test goal is to verify the flow control rule enforcement of the TOE; and

f. IDS: The objective of this test goal is to test the IDS functionality of the TOE.

[3] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

11.3 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:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;

b. Attempting to lock out the administrator account by forcing multiple failed SSH logins; and

c. Attempting to trick the router into routing packets from a trusted network to an untrusted network.

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

11.4 Conduct of Testing

VPX3-685 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place onsite at the developer’s site in Ottawa, Canada. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, providing assurance that VPX3-685 behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

The TOE is not intended to be deployed as a standalone router in an enterprise. Consumers are expected to be experienced in integrating modular embedded components into larger IT products. The documentation has been written for such an audience.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation

15 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Curtiss-Wright Controls Defense Solutions VPX3-685 Secure Router Security Target, v1.15, 18 October 2013.

e. Evaluation Technical Report (ETR) for VPX3-685 Secure Routers, v1.2, 18 October 2013.