Certification Report

Avocent Cybex SwitchView SC Series Switches

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-312-CR
Version:	1.0
Date:	19 November 2014
Pagination:	i to iii, 1 to 9

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, 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 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, 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.

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.

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 CSC Security Testing/Certification Laboratories.

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.

This certification report is associated with the certificate of product evaluation dated 19 November 2014, 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

Avocent Cybex SwitchView SC Series Switches (hereafter referred to as Avocent SwitchView SC), from Avocent Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that Avocent SwitchView SC meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

Avocent SwitchView SC is a Peripheral Sharing Switch that permits a single set of human interface devices such as DVI-I video, audio (input and output), USB keyboard, USB mouse, and USB Smart Card reader to be shared among two or more computers. The Avocent SwitchView SC architecture enables users to access secure and non-secure networks from one set of peripherals while keeping the data separate.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 23 October 2014 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 Avocent SwitchView SC, 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 CCS Certification Body, declares that the Avocent SwitchView SC 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).

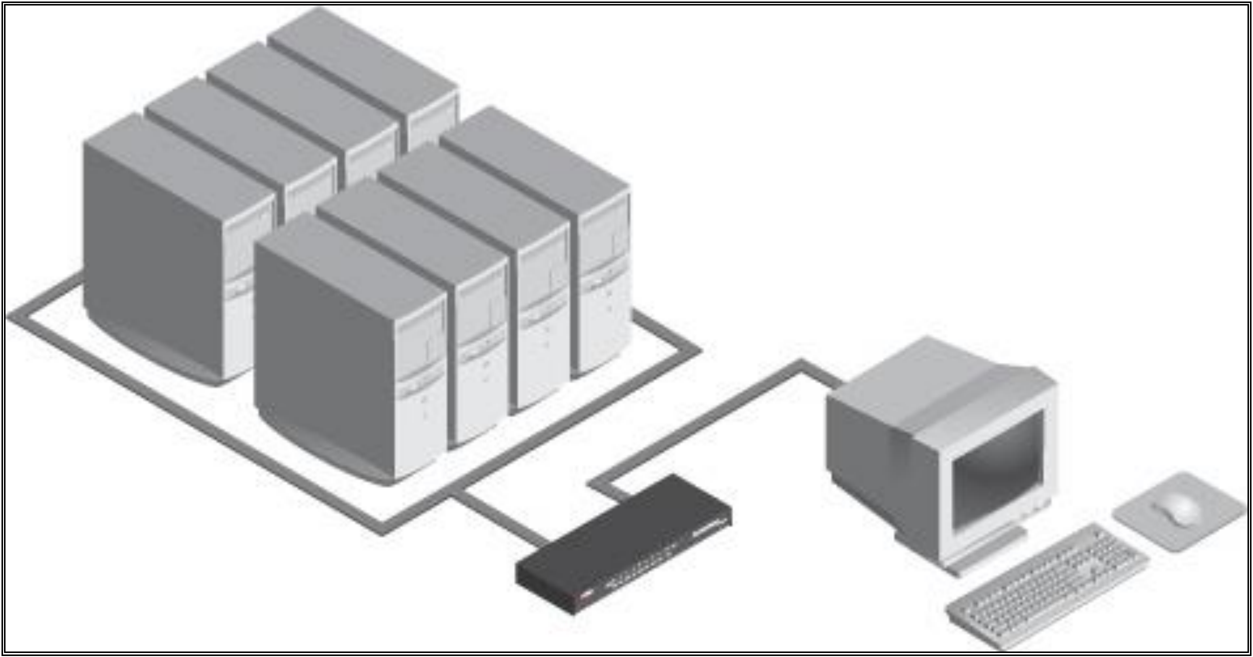
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is Avocent Cybex SwitchView SC Series Switches (hereafter referred to as Avocent SwitchView SC), from Avocent Corporation.

2 TOE Description

Avocent SwitchView SC is a Peripheral Sharing Switch that permits a single set of human interface devices such as DVI-I video, audio (input and output), USB keyboard, USB mouse, and USB Smart Card reader to be shared among two or more computers. The Avocent SwitchView SC architecture enables users to access secure and non-secure networks from one set of peripherals while keeping the data separate.

A diagram of the Avocent SwitchView SC deployment is as follows:



3 Security Policy

Avocent SwitchView SC implements a data separation security policy to allow peripheral data to be transferred only between peripheral port groups with the same ID; details of this security policy can be found in Section 6 of the ST.

In addition, Avocent SwitchView SC implements policies pertaining to the following security functional classes:

- Security Management; and
- Protection of the TSF.

4 Security Target

The ST associated with this Certification Report is identified below:

Avocent Cybex SwitchView SC Series Switches Security Target, Version 6.0 Revision 2.6, August 12, 2014.

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.*

Avocent SwitchView SC is:

a. *EAL 2 augmented, containing all security assurance requirements listed, as well as the following:*
   - ALC_FLR.2 – Flaw Reporting Procedures

b. *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:*
   - EXT_VIR.1-Visual Indication Rule
   - EXT_IUC.1 - Invalid USB Connection
   - EXT_ROM.1- Read-only ROMs

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

6 Assumptions and Clarification of Scope

Consumers of Avocent SwitchView SC 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- Authorized users possess the necessary privileges to access the information transferred by the TOE.
- The TOE is installed and managed in accordance with the manufacturer's directions.
- Authorized users are non-hostile and follow all usage guidance.

6.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- The TOE is physically secure.

6.3 Clarification of Scope

The TOE is intended for use by non-hostile and trained users that have followed the installation and configuration guidance provided in the product's user manual.

7 Evaluated Configuration

The evaluated configuration for Avocent SwitchView SC comprises the following hardware models:

- Avocent Cybex SwitchView SC620 520-866-503
- Avocent Cybex SwitchView SC640 520-869-503
- Avocent Cybex SwitchView SC740 520-868-503
- Avocent Cybex SwitchView SC620C 520-903-503
- Avocent Cybex SwitchView SC640C 520-904-503
- Avocent Cybex SwitchView SC740C 520-905-503

8 Documentation

The Avocent Corporation documents provided to the consumer are as follows:

a. Quick Installation Guide SwitchView SC620/640 2/4-Port DVI-I/USB Switches with Audio (590-1050-501A)

b. Quick Installation Guide SwitchView SC740 4-Port, Dual-Head DVI-I/USB Switch with Audio (590-1051-501A)

c. Quick Installation Guide SwitchView SC620C/640C 2/4-Port DVI-I/USB Switches with Audio (590-1137-501A)

d. Quick Installation Guide SwitchView SC740C 4-Port, Dual-Head DVI-I/USB Switch with Audio (590-1138-501A)

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Avocent SwitchView SC, including the following areas:

Development: The evaluators analyzed the Avocent SwitchView SC 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 Avocent SwitchView SC 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 Avocent SwitchView SC 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 Avocent SwitchView SC configuration management system and associated documentation was performed. The evaluators found that the Avocent SwitchView SC 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 Avocent SwitchView SC during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Avocent SwitchView SC. 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.

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

10 ITS Product Testing

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

10.1 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[1].

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.

10.2 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. Resulting from this test coverage approach is the following list of 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. Verification of Read Only Memory: The objective of this test goal is to determine that the processor used in the TOE is able to protect its internal flash memory which is used to store the TSF software;

c. Separation of Audio Output Data: The objective of this test goal is to verify that the audio output data from each computer is separated; and

d. Initial Value on Start Up: The objective of this test goal is to determine if port A is initially connected to a shared peripheral whether computer A powers up or not.

10.3 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. Misuse: The objective of this test goal is to concurrently push more than one port selection button in an attempt to cause to the TOE to malfunction; and

[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.

b. Undocumented External Interfaces: The objective of this test goal is to enter shortcut key sequences to verify that undocumented external interfaces are not present and/or exploitable within the TOE.

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

10.4 Conduct of Testing

Avocent SwitchView SC was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test Facility. 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.

10.5 Testing Results

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

11 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.

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
API	Application Programming Interface
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DVI	Digital Video Interface
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
TSF	TOE Security Function
USB	Universal Serial Bus

13 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. Avocent Cybex SwitchView SC Series Switches Security Target, Version 6.0 Revision 2.6, August 12, 2014.

e. Evaluation Technical Report Avocent Corporation Avocent Cybex SwitchView SC Series Switches EAL2+, Version 0.4, October 23, 2014.