National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Avocent Cybex SwitchView SC Series Switches SC320, SC340, and SC380

Report Number: CCEVS-VR-VID10397-2010

Dated: 15 December 2010

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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Jandria Alexander

Aerospace Corporation

Columbia, MD

Jean Hung

MITRE Corporation

Bedford, MA

Common Criteria Testing Laboratory

Halvar Forsberg

Gregory Bluher

Computer Sciences Corporation
Hanover, MD

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (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.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Avocent SwitchView SC Series Switches: Avocent Cybex SwitchView SC320 Model 520-633-501, Avocent Cybex SwitchView SC340 Model 520-634-501, and Avocent Cybex SwitchView SC380 Model 520-635-501, the target of evaluation (TOE), performed by Computer Sciences Corporation the Common Criteria Testing Laboratory (CCTL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by Computer Sciences Corporation (CSC) of Hanover, MD in accordance with the United States evaluation scheme and completed on December 2, 2010. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The ST was written by Avocent Corporation. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, version 3.1, dated July 2009 at Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.2, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, July 2009.

The TOE is a device, hereinafter referred to as a Peripheral Sharing Switch (PSS), or simply switch, that permits a single set of human interface devices: DVI-I video, Audio (input and output), USB keyboard, USB mouse, and CAC or SmartCard reader, to be shared among two or more computers. Users who access secure and unsecure networks from one set of peripherals can rely on the Avocent Cybex SwitchView SC series of switches' unique architecture to keep their private data completely separate and secure at all times. There is no software to install or boards to configure.

The Avocent Cybex SwitchView SC series of switches work with IBM PC/AT and Sun systems and have ports for DVI-I video, Audio (input and output), USB keyboard, USB mouse, and CAC or SmartCard reader. Each switch has a "select" button associated with each specific port. For the convenience of the operator, these models have USB ports on both the front and rear of the device.

The TOE is a peripheral sharing switch. The physical boundary of the TOE consists of one Avocent Cybex SwitchView switch (see Table 1: TOE Models and Features), and its accompanying User and Administrator Guidance.

Table 1: Models and Features

Model	TOE Identification Part Numbers	Ports	Interfaces
Avocent Cybex SwitchView SC320	520-633-501	2	Single-head, Dual-link DVI-I, Audio (input and output), USB keyboard, USB mouse and CAC or SmartCard reader
Avocent Cybex SwitchView SC340	520-634-501	4	Single-head, Dual-link DVI-I, Audio (input and output), USB keyboard, USB mouse and CAC or SmartCard reader
Avocent Cybex SwitchView SC380	520-635-501	8	Single-head, Dual-link DVI-I, Audio (input and output), USB keyboard, USB mouse and CAC or SmartCard reader

In addition to having more (8) ports, the SwitchView SC380 also differs from the other two models (4-port SC340 and 2-port SC320) in how the internal hardware architecture controls selection and power indication LEDs; however, this well-documented difference does not alter the fact that all three models provide the same security functionality.

The TOE boundary does not include any peripherals or computer components, to include cables or their associated connectors, attached to the TOE.

1.1. 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 August 13, 2009.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

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;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 2: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Avocent Cybex SwitchView SC320 Model 520-633-501 Avocent Cybex SwitchView SC340 Model 520-634-501 Avocent Cybex SwitchView SC380 Model 520-635-501
Protection Profile	*Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, version 1.2*, dated August 21, 2008
Security Target	*Avocent Cybex SwitchView SC Series Switches Security Target, Document Version 4.0 December 2, 2010*
Dates of evaluation	August 2009 through December 2010
Evaluation Technical Report	*Avocent Cybex SwitchView SC Series: SC320, SC340, SC380*, Version 1.0, December 15, 2010
Conformance Result	Part 2 extended and Part 3 EAL 4 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009
Common Evaluation Methodology (CEM) version	CEM version 3.1R3, July 2009
Sponsor	Avocent Corporation
Developer	Avocent Corporation
Evaluators	Gregory Bluher of Computer Sciences Corporation
Validation Team	Jandria Alexander of Aerospace Corporation and Jean Hung of MITRE Corporation

3. SECURITY POLICY

The TOE enforces the following security policies:

3.1. Data Separation Policy

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 1.2, dated August 21, 2008.

Signals processed by the TOE are shared peripheral device data, Data Display Channel information, and video signals. Specific versions of the TOE accommodate subsets of the listed signals to support popular types of computers. In all cases, the TOE ensures data separation for all signal paths using both hardware and firmware.

The basic arrangement of the microprocessors used for shared peripheral data ensures data separation in hardware by physical separation of the microprocessors connected to the user's peripheral devices from the microprocessors connected to the attached computers. In operation, the main processor moves data received from the shared peripherals to the microprocessor corresponding to the selected computer. The processor dedicated to the selected computer sends data to the computer. Separation is ensured in hardware by use of separate microprocessors for each of the computers and for the shared user peripheral devices.

Separation in firmware is ensured by firmware design consisting of dedicated functions and static memory assignment with no third-party library functions or multitasking executives.

In operation, the TOE is not concerned with the content of user information flowing between the shared peripherals and the switched computers. It only provides a single logical connection between the shared peripheral group and the one selected computer supporting the Data Separation Security Functional Policy – "the TOE shall allow peripheral data and state information to be transferred only between peripheral port groups with the same ID." The TOE interfaces ensure that confidentiality of information is not violated by isolating signals electrically and through firmware modules that ensure that information is passed only between the user peripherals and the selected computer.

Shared peripheral status for each computer is stored by the processor associated with each computer. The TOE does not have software to install, or boards to configure. The logic contained within the TOE is protected from unauthorized modification through the use of discrete components.

3.2. Security Management Policy

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The green LEDs over each channel will light, indicating that the attached computer is powered on. To select or switch computers, the TOE provides port-specific switches that allow the human user to explicitly determine to which computer the shared set of

peripherals is connected. This connection is visually displayed by an amber LED over the selected channel.

4. ASSUMPTIONS

4.1. Physical Security Assumptions

A key environmental assumption is physical security, for it is assumed appropriate physical security protection will be applied to the TOE hardware commensurate with the value of the IT assets. Specifically, the TOE is assumed to be located within a facility providing controlled (i.e., employee-only) access to prevent unauthorized physical access to internal parts of the TOE.

4.2. Personnel Security Assumptions

It is assumed that an authorized user possesses the necessary privileges to access the information transferred by the TOE – users are authorized users. It is also assumed that the TOE is installed and managed in accordance with the manufacturer's directions. It is assumed that the authorized user is non-hostile and follows all usage guidance.

4.3. Operational Security Assumptions

It is assumed that the TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, Part 15 of the FCC Rules for Class B digital devices.] It is also assumed that only the selected computer's video channel will be visible on the shared monitor. It is assumed that vulnerabilities associated with the attached devices (shared peripherals or switched computers), or their connection to the TOE, are a concern of the application scenario and not of the TOE.

4.4. Threats Countered and Not Countered

The TOE is designed to fully or partially counter the following threats:

T.BYPASS	The TOE may be bypassed, circumventing nominal SWITCH functionality
T.INSTALL	The TOE may be delivered and installed in a manner which violates the security policy.
T.LOGICAL	The functionality of the TOE may be changed by reprogramming in such a way as to violate the security policy.
T.PHYSICAL	A physical attack on the TOE may violate the security policy.
T.RESIDUAL	RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs.
T.SPOOF	Via intentional or unintentional actions, a USER may think the set of SHARED PERIPHERALS are CONNECTED to one COMPUTER when in fact they are connected to a different one.

T.STATE	STATE INFORMATION may be transferred to a PERIPHERAL PORT GROUP with an ID other than the selected one.
T.TRANSFER	A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.

4.5. Organizational Security Policies

The *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008, identifies no organization security policies (OSPs) to which the TOE must comply.

5. ARCHITECTURAL INFORMATION

5.1. Logical Scope and Boundary

The TOE logical scope and boundary consists of the security functions/features provided/controlled by the TOE.

The TOE provides the following security features:

- Data Separation (TSF_DSP),
- Security Management (TSF_MGT), and
- Tamper Detection (TSF_TMP).

5.1.1. Data Separation (TSF_DSP)

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 2 of *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*, Version 1.2, dated August 21, 2008. In operation, the TOE is not concerned with the user information flowing between the shared peripherals and the switched computers. It only provides a single logical connection between the shared peripheral group and the one selected computer (TSF_DSP).

5.1.2. Security Management (TSF_MGT)

The TOE allows for the connected computers to be powered-up all-at-once or one at a time. The green LEDs over each channel will light, indicating that the attached computer is powered on. To select or switch computers, the TOE provides *select* switches, that allow the human user to explicitly determine to which computer the shared set of peripherals is connected (TSF_MGT). This connection is visually displayed by an amber LED over the selected channel.

5.1.3. Tamper Detection (TSF_TMP)

Any attempt to open the TOE by removing the security screw will activate a tamper-detection "suicide" switch. If one of these models has been physically tampered with in this manner, the lights on the front of the TOE will all flash in unison to alert an administrator to the interference, and all TOE functions will be permanently disabled.

5.2. Physical Scope and Boundary

The TOE is a peripheral sharing switch. The physical boundary of the TOE consists of one Avocent Cybex SwitchView switch, and its accompanying User and Administrator Guidance.

In addition to having more (8) ports, the SwitchView SC380 also differs from the other two models (4-port SC340 and 2-port SC320) in how the internal hardware architecture

controls selection and power indication LEDs; however, this well-documented difference does not alter the fact that all three models provide the same security functionality.

The TOE boundary does not include any peripherals or computer components, to include cables or their associated connectors, attached to the TOE. USB type-enforcement must be mandated by policy; only human interface and CAC or smart card reader devices are permitted in the evaluated configuration because type checking was not included in the PP to which this product claims conformance. The evaluated TOE configuration excludes the usage of a proprietary USB target selection / indication device if such device becomes available for purchase. The following figure depicts the TOE and its environment.

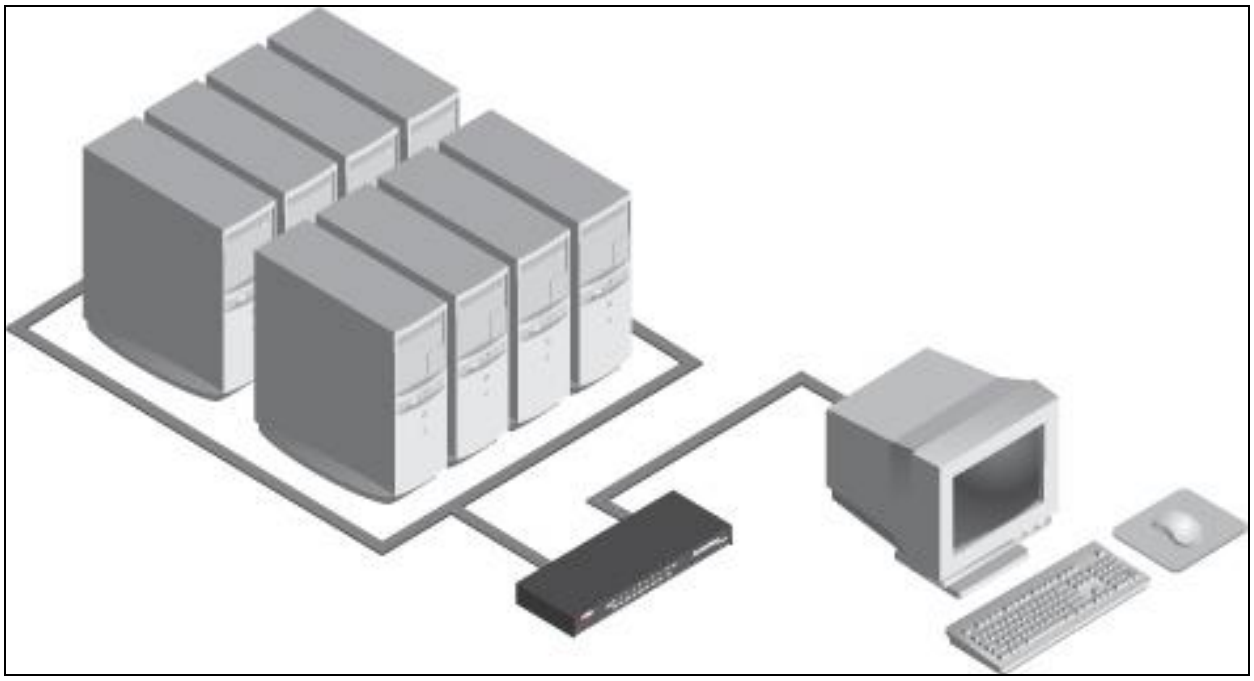


Figure 1: Depiction of TOE Deployment

6. DOCUMENTATION

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Avocent Cybex SwitchView SC Series Switches SC320, SC340, and SC380. Note that not all evidence is available to customers. The following documentation is available to the customer:

- Quick Installation Guide, SwitchView SC320/340 (AGD- 590979501C (SC320 and SC340 guidance).pdf)
- Quick Installation Guide, SwitchView SC380 (AGD- 5901011501C (SC380 guidance).pdf)

The remaining evaluation evidence is described in the Evaluation Technical Report developed by Computer Sciences Corporation.

7. IT PRODUCT TESTING

This section describes the testing efforts of the Developer and the evaluation team.

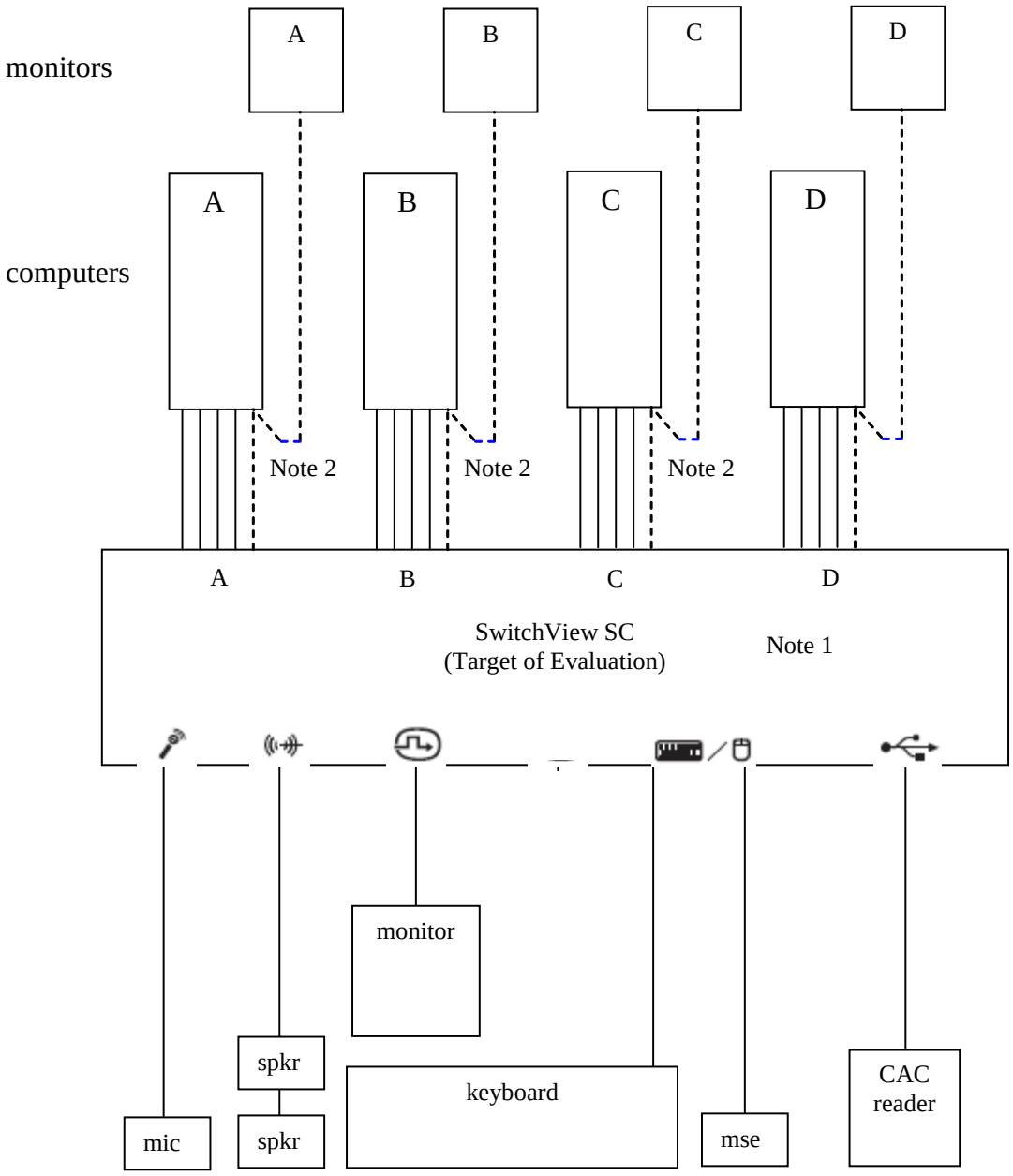
7.1. Developer testing

Test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces. The developer tested all of the interfaces to the TOE and in doing so tested all TSFs.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included with each of the tests in the TOE Test Procedures. Each test case was assigned an identifier that was used to reference it throughout the testing evidence.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 4. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

The following diagram depicts the test environment that was used by the Developers. The Evaluators assessed that the test environment used by the Developers was appropriate and mirrored a portion of this test configuration during Independent testing.



Note:

1. SC340 model is illustrated. Omit ports C and D for the two-port model. Add ports E-H for the eight-port model.

2. Connect computer video directly to monitors where dictated by test procedure – Smart Card Reader tests, otherwise connect computer video to TOE. It is also acceptable to use a single monitor, moving it from computer to computer during the test.

7.2. Evaluation team independent testing

The evaluation team conducted independent testing both at the CCTL and the Developer's facilities. For the testing at the CCTL, the TOE was delivered by common carrier, UPS, and a signature receipt was required. The evaluation team installed and configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target. The evaluation team then tested the tamper detection security functionality.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team repeated all of the Sponsor's test cases and designed additional independent tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

The evaluators examined the ADV evidence listed in Section 1.2 above as well as a subset of the implementation representation and selected to run the developer's tests for all three models under evaluation.

Each TOE Security Function was exercised at least once, and the evaluation team verified that each test passed.

7.3. Vulnerability analysis

The evaluation team gained assurance that the TOE does not contain exploitable flaws or weaknesses in the TOE based on the evaluation team's Vulnerability Analysis.

The Developer performed a Vulnerability Analysis of the TOE to identify any obvious vulnerability in the product and to show that it is not exploitable in the intended environment for the TOE operation. In addition, the evaluation team conducted a search of the public vulnerability sites to determine the thoroughness of the analysis.

Based on the results of the team's Vulnerability Analysis and an in-depth analysis (to the code level) of the TOE design evidence, the evaluation team came to the conclusion that

obvious penetration attempts are not possible through the TOE external interfaces. As indicated in the design documentation, direct access to the TOE security functions is not possible without disassembly of the TOE, thus penetration is not possible via the product control, i.e., user/administrator interfaces. Additionally, no configuration items are provided for the security functionality of the TOE thus it cannot be configured in an insecure state. The security functionality is inherent in the design and internal functioning of the TOE.

8. EVALUATED CONFIGURATION

The evaluated configuration of the Avocent Cybex SwitchView SC Series Switches SC320 Model 520-633-501, SC340 Model 520-634-501, and SC380 Model 520-635-501, as defined in the Security Target, consists of one of the evaluated models.

The Avocent Cybex SwitchView SC Series Switches SC320, SC340, and SC380 must be configured in accordance with the following Guidance Documents:

- Quick Installation Guide, SwitchView SC320/340 (AGD- 590979501C (SC320 and SC340 guidance).pdf)
- Quick Installation Guide, SwitchView SC380 (AGD- 5901011501C (SC380 guidance).pdf)

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 3.1R3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R3.

Computer Sciences Corporation (CSC) has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 4 augmented with ALC_FLR.2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on November 8, 2010. A final Validation Oversight Review (VOR) was held on December 1, 2010.

9.1. Evaluation of the Security Target (ASE)

The evaluation team applied each EAL4 appropriate ASE CEM work unit.

The evaluation of the ST introduction demonstrated that the ST and the TOE were correctly identified, that the TOE was correctly described at three levels of abstraction (TOE reference, TOE overview and TOE description) and that these three descriptions were consistent with each other.

The evaluation demonstrated the validity of the conformance claims including the one with the PP reference in Table 2 above.

The evaluation of the security problem definition demonstrated that the security problem intended to be addressed by the TOE and its operational environment, was clearly defined.

The evaluation of the security objectives demonstrated that the security objectives adequately and completely addressed the security problem definition, and that the division of this problem between the TOE and its operational environment was clearly defined.

The evaluation of the definition of extended components determined that they were clear and unambiguous, and that they were necessary, i.e. they could not be clearly expressed using existing CC Part 2 or CC Part 3 components.

The evaluation of the security requirements ensured that they were clear, unambiguous and well-defined.

The evaluation of the TOE summary specification determined that it was adequately described how the TOE: met its SFRs; protected itself against interference, logical tampering and bypass; and that the TOE summary specification was consistent with other narrative descriptions of the TOE.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the

evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2.Evaluation of the Development (ADV)

The evaluation team applied each EAL4 appropriate ADV CEM work unit.

The evaluation of the ADV_ARC.1 evidence determined that the TSF was structured such that it could not be tampered with or bypassed, and that TSFs that provided security domains isolated those domains from each other.

The evaluation of the ADV_FSP.4 evidence determined that the developer had provided a description of the TSFIs in terms of their purpose, method of use, and parameters. In addition, the actions, results and error messages of each TSFI were also described sufficiently that it could be determined whether they were SFR-enforcing, with the SFR-enforcing TSFI being described in more detail than other TSFIs. The evaluation ascertained that the developer completely described all of the TSFI in a manner such that the evaluator was able to determine that the TSFI were completely and accurately described, and appeared to implement the security functional requirements of the ST.

The evaluation of the ADV_IMP.1 evidence ascertained that the developer made available the implementation representation of the TOE in the form that could be and was analyzed by the evaluator. The implementation representation was used in analysis activities for other families to demonstrate that the TOE conformed to its design and to provide a basis for analysis in other areas of the evaluation. The implementation representation consisted of firmware source code and detailed hardware diagrams.

The evaluation of the ADV_TDS.3 evidence determined that the TOE design provided a description of the TOE in terms of subsystems sufficient to determine the TSF boundary, and provided a description of the TSF internals in terms of modules and subsystems. It provided a detailed description of the SFR-enforcing modules and enough information about the SFR-supporting and SFR-non-interfering modules for the evaluator to determine that the SFRs were completely and accurately implemented; as such, the TOE design provided an explanation of the implementation representation.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3.Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit.

The evaluation of the AGD_OPE.1 evidence determined that the user guidance described for each user role the security functionality and interfaces provided by the TSF, provided

instructions and guidelines for the secure use of the TOE, addressed secure procedures for all modes of operation, and facilitated prevention and detection of insecure TOE state.

The evaluation of the AGD_PRE.1 evidence determined that the procedures and steps for the secure preparation of the TOE had been documented and resulted in a secure configuration.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4. Evaluation of the Life-cycle Support (ALC)

The evaluation team applied each EAL4 appropriate ALC CEM work unit and ALC_FLR.2.

The evaluation of the ALC_CMC.4 evidence determined that the developer had clearly identified the TOE and its associated configuration items, and that the ability to modify these items was properly controlled by automated tools, thus making the CM system less susceptible to human error or negligence.

The evaluation of the ALC_CMS.4 evidence determined that the configuration list included the TOE, the parts that comprise the TOE, the TOE implementation representation, security flaws, and the evaluation evidence. These configuration items were controlled in accordance with CM capabilities (ALC_CMC).

The evaluation of the ALC_DEL.1 evidence determined that the delivery documentation described all procedures used to maintain security of the TOE when distributing the TOE to the user.

The evaluation of the ALC_DVS.1 evidence determined that the developer's security controls on the development environment were adequate to provide the confidentiality and integrity of the TOE design and implementation that was necessary to ensure that secure operation of the TOE was not compromised.

The evaluation of the ALC_FLR.2 evidence determined that the developer had established flaw remediation procedures that described the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users. Additionally, the evaluation determined that the developer's procedures provided for the corrections of security flaws, for the receipt of flaw reports from TOE users, and for assurance that the corrections introduced no new security flaws.

The evaluation of the ALC_LCD.1 evidence determined that the developer had used a documented model of the TOE life-cycle.

The evaluation of the ALC_TAT.1 evidence determined that the developer had used well-defined development tools that yield consistent and predictable results.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5.Evaluation of the Test (ATE)

The evaluation team applied each EAL4 appropriate ALC ATE work unit.

The evaluation of the ALC_COV.2 evidence determined that the developer had tested all of the TSFIs, and that the developer's test coverage evidence showed correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification.

The evaluation of the ALC_DPT.2 evidence determined that the developer had tested all the TSF subsystems and SFR-enforcing modules against the TOE design and the security architecture description.

The evaluation of the ALC_FUN.1 evidence determined that the developer correctly performed and documented the tests in the test documentation.

The performance of the ALC_IND.2 work determined, by having independently tested a subset of the TSF, that the TOE behaved as specified in the functional specification, guidance documentation, and the design documentation; and enabled the evaluators to gain confidence in the developer's test results by having performed a sample of the developer's tests.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6.Evaluation of the Vulnerability Assessment (AVA)

The evaluation team applied each EAL4 appropriate ALC ATE work unit.

The performance of the AVA_VAN.3 work determined that the TOE, in its operational environment, did not have vulnerabilities exploitable by attackers possessing Enhanced-Basic attack potential.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10. VALIDATOR COMMENTS

USB type-enforcement must be mandated by policy; only human interface and CAC or smart card reader devices are permitted in the evaluated configuration because type checking was not included in the PP to which this product claims conformance.

11. ANNEXES

None.

12. SECURITY TARGET

Avocent Cybex SwitchView SC Series Switches Security Target, Version 4.0, December 2, 2010

13. GLOSSARY

- **Administrator:** Role applied to user with full access to all aspects of the Cybex SwitchView SC Series Switches.
- **Attack:** An attack is an exploited threat or an attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.
- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. BIBLIOGRAPHY

1.) Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1, Revision 3.

2.) Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated July 2009, Version 3.1, Revision 3.

3.) Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated July 2009, Version 3.1, Revision 3.

4.) Common Evaluation Methodology for Information Technology Security Evaluation, dated July 2009, Version 3.1, Revision 3.

5.) Avocent Corporation/Computer Sciences Corporation. *Avocent Cybex SwitchView SC Series Switches Security Target, Version 4.0,* December 2, 2010.

6.) Computer Sciences Corporation (CSC). *Evaluation Technical Report Avocent Cybex SwitchView SC Series: SC320, SC340, and SC380,* Version 1.0, December 15, 2010.