CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Cybex SwitchView SC Series Switches SC 680 and SC 780

Maintenance Report Number: CCEVS-VR-VID10471-2014

Date of Activity: 18 August 2014

References:

Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 2, September 8, 2008

Common Criteria Document CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements” Version 2.1, June 2012

Avocent Corporation Impact Analysis Report (IAR) for the SwitchView SC Series for models SC680 and SC780 with revised firmware Version 1.0.

Cybex SwitchView SC Series Switches Security Target Document Version 7.0 Revision 1.1.

Cybex SwitchView SC Series Switches Security Target Document Version 7.0 Revision 1.2.

Affected Evidence:

Cybex SwitchView SC Series Switches Security Target Document Version 7.0 Revision 1.2.

Updated Developer Evidence:

Cybex SwitchView SC Series Switches Security Target Document Version 7.0 Revision 1.2.

Assurance Continuity Maintenance Report:

Introduction:

This Impact Analysis Report (IAR) for the Cybex SwitchView SC Series Switches, also called the TOE, is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 2.1, June 2012. In accordance with those requirements, it describes the changes made to the certified TOE, the evidence updated because of the changes and the security impact of the changes.

Configuration Control Identifiers

The Validation Report Number is CCEVS-VR-010471-2011.

The Validated TOE is identified as follows:

Avocent Cybex SwitchView SC680, part number 520-865-501
Avocent Cybex SwitchView SC780, part number 520-867-501

The Security Target (ST) is identified as *Cybex SwitchView SC Series Switches Security Target Document Version 7.0 Revision 1.2.* The Security Target for the original validation is *Cybex SwitchView SC Series Switches Security Target Document Version 7.0 Revision 1.1*.

Changes to TOE:

The following modifications were made:

- Unit tamper-evident labels were modified to include an 8-digit, unique serial number for both units.
- Firmware on the mainboard was revised for both units.
- Hardware and firmware on the video board was revised for both units.
- New TOE identifications were assigned
  From:
    - Avocent Cybex SwitchView SC680, part number 520-865-501
    - Avocent Cybex SwitchView SC780, part number 520-867-501

  To:
    - Avocent Cybex SwitchView SC680, part number 520-865-502
    - Avocent Cybex SwitchView SC780, part number 520-867-502

Reason for Change

- **Tamper Evident Labels**: The revised tamper-evident label was in response to a specific DoD customer request
- **Main board firmware**: It has been observed that switching channels while hot-plugging an invalid USB device may cause the units to restart
- **Video board hardware and firmware:** Both units are currently capable of supporting displays with an Extended Display Identification Data (EDID) size of 128 bytes. Some newer displays are appearing on the market with larger 256 byte EDIDs. In order to support these displays, a change to the hardware and firmware was required.

Security Impact Analysis

- **Tamper Evident Labels**: The addition of a unique serial number to the tamper evident labels has no impact of the security enforcing functions of the units.

Firmware: The firmware changes on the main board occurred in the “PlusOne” processor of the Controller subsystem. The HLD and LLD maps these to the TSF_DSP (data separation) security function. The mapping was included in **Table 1** to show the specific interface involved and the related TOE Security Function.

Subsystem	External Interface	TOE Security Function	Security Functional Requirement(s)
Controller	User Keyboard Interface	TSF_DSP TSF_IUC	FDP_ETC.1 FDP_IFC.1 FDP_IFF.1 FDP_ITC.1 EXT_IUC.1
	User Mouse Interface	TSF_DSP TSF_IUC	FDP_ETC.1 FDP_IFC.1 FDP_IFF.1 FDP_ITC.1 EXT_IUC.1

Table 1 - High-level Design Correspondence for Main Board Firmware Change

The changes to the firmware were confined to the User Keyboard Interface and User Mouse Interface within the Controller Subsystem. The changes add a more graceful recovery mechanism in response to an error during enumeration. These changes do not result in any changes to the evaluated evidence of the controller subsystem and do not impact upon the enforcement of TSF_DSP (Data Separation) or TSF_IUC (Invalid USB Connection). Regression testing was performed to confirm that the changes did not impact the security profile of the device.

- **Video board hardware and firmware**: The video board hardware and firmware changes occurred in the Video/Audio Switch subsystem within the Computer DDC Interfaces and User DDC Interface modules. No user information passes through the DDC path; hence, these modules do not have any security related functions.

Subsystem	External Interface	TOE Security Function	Security Functional Requirement(s)
Video/Audio Switch	Computer DDC Interfaces	none	none
	User DDC Interfaces	none	none

Table 2 - High-level Design Correspondence for Video Board Hardware and Firmware Change

Affected Evidence

Evidence already on file has been revised as indicated below.

Class	Document	Changes
ADV	Design document	identify changed TOE
ADV	Security Architecture Description	identify changed TOE
ATE	Test Procedure	identify changed TOE in section 3

		add test results for changed TOE to section 3
ATE	Functional Test Plan	identify changed TOE in section 2
ST	Security Target	identify changed TOE in sections 1.1, 1.4, Table 1
		Revised tamper-evident label in section 7 Corrected typos
ALC	CI list	updated to reflect changes

Vendor Conclusion:

The revised tamper evident labels on both the units have all of the functionality of the previous tamper evident labels in addition to a unique serial number. The impact of this change is judged to be minor and not impact the security enforcing functions of the device.

The changes to the firmware were confined to the User Keyboard Interface and User Mouse Interface within the Controller Subsystem. The changes add a more graceful recovery mechanism in response to an error during enumeration. These changes do not result in any changes to the evaluated evidence of the controller subsystem and do not impact upon the enforcement of TSF_DSP (Data Separation) or TSF_IUC (Invalid USB Connection). Regression testing was performed to confirm that the changes did not impact the security profile of the device Thus, the change is judged to be minor as it does not impact the security enforcing functions of the device.

The changes to the hardware and firmware on the video board were confined to a section that has no role in the TOE Security Function nor any associated Security Functional Requirements.

Consideration of the nature of the changes leads to the conclusion that they should be classified as minor changes and that certificate maintenance is the correct path to continuity of assurance.

Validation Team Conclusion:

The vendor asserts that regression testing was performed and no impacts to the security profile were detected. The validation team reviewed the changes and concur the changes are minor and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.