CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Avocent Cybex SwitchView SC Series Switches SC320, SC 340, and SC 380

Maintenance Report Number: CCEVS-VR-VID10397-2014

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 SC320, SC340 and SC380 with revised firmware and hardware Version 1, July 16, 2014

Cybex SwitchView SC Series Security Target, Version 4.0

Cybex SwitchView SC Series Security Target, Version 4.0, Revision 1.11

Affected Evidence:

Cybex SwitchView SC Series Security Target, Version 4.0

Updated Developer Evidence:

Cybex SwitchView SC Series Security Target, Version 4.0, Revision 1.11

Assurance Continuity Maintenance Report:

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.

Changes to TOE:

The following modifications were made:

- Unit tamper-evident labels were modified to include an 8-digit, unique serial number for all three units.
- Firmware on the Main Board was revised for the SC320 and SC340. Firmware on the Main Board of the SC380 is unchanged.
- Hardware of the Video Board was revised for the SC380. Hardware on the Video Board of the SC320 and SC340 is unchanged.
- New TOE identifications were assigned

  From:
  - Avocent Cybex SwitchView SC320, part number 520-870-502
  - Avocent Cybex SwitchView SC340, part number 520-871-502
  - Avocent Cybex SwitchView SC380, part number 520-872-502

  To:
  - Avocent Cybex SwitchView SC320, part number 520-870-503
  - Avocent Cybex SwitchView SC340, part number 520-871-503
  - Avocent Cybex SwitchView SC380, part number 520-872-503

The firmware is the same source and object for the SC320 and SC340 main board. The firmware is the same source and object for all three video boards.

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 change occurred in the "N" processor of the Controller subsystem. The HLD and LLD maps these to the TSF_DSP (data separation) security function. Within encoreVKM.c the following changes were made to prevent unselected target computers from entering sleep mode:
  - A flag, *TargetDeselected,* was added to indicate the state of the channel, selected or deselected.
  - The call to *DeselectTarget()* is now only made when the communication with the "PlusOne" processor is ended and the *TargetDeselected* flag indicates that the channel is selected. The flag is then updated to indicate the new state of the channel. This has the net effect of only calling *DeselectTarget()* once when the channel is deselected instead of repeatedly while the channel is deselected.
- **Hardware:** The hardware change occurred in the Video/Audio switch subsystem within the DDC circuits module. No user information passes through the DDC path; hence, DDC circuits do not have any security related functions.

Evidence Modifications

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
ALC	CI list	updated to reflect changes

Vendor Conclusion:

The revised tamper evident labels on all 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 within the Computer Keyboard Interface of the "N" processors in the Controller subsystem to prevent unselected target computers from entering sleep mode. Although the Controller subsystem enforces data separation (TSF_DSP) the "N" processor firmware plays no part in this enforcement. TSF_DSP is achieved by physical separation between "N" processors. Testing confirmed that data separation is maintained. Thus, the change is judged to be minor as it does not impact the security enforcing functions of the device.

The change in the hardware was 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:

Note that although firmware changes were applied to two of the devices (the SC320 and SC340) the firmware used to update those devices is the same firmware version that was previously subject to testing in the SC380 platform. The change to the SC380 video hardware was to expand EDID support. The vendor asserts that regression testing was performed and that no security related functions were impacted by the changes made.

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.