ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Vertiv CYBEX™ SCMV2160DPH, SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE Firmware Version 44404-E7E7 Peripheral Sharing Devices

Vertiv CYBEX™ SCMV2160DPH, SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE Firmware Version 44404-E7E7 Peripheral Sharing Devices

Maintenance Report Number: CCEVS-VR-VID11122-2022

Date of Activity: 25 January 2022

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Vertiv CYBEX™ SCMV2160DPH, SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE Firmware Version 44404-E7E7 Peripheral Sharing Devices Impact Analysis Report, Version 2.0, 5 January 2022
- Protection Profile for Peripheral Sharing Device Version 4.0, July 19, 2019
- PP-Module for Keyboard/Mouse Devices, Version 1.0, July 19, 2019
- PP-Module for Video/Display Devices, Version 1.0, July 19, 2019

Assurance Continuity Maintenance Report:

Acumen submitted an Impact Analysis Report (IAR) for the Vertiv CYBEX™ SCMV2160DPH, SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE Firmware Version 44404-E7E7 Peripheral Sharing Devices to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 7 January 2022. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consists of the Security Target and the Impact Analysis Report (IAR). The ST and the IAR were updated.

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes

Security Target: Vertiv CYBEX™ SCMV2160DPH, SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE Firmware Version 44404-E7E7 Peripheral Sharing Devices Security Target, Version 1.15, January 4, 2022	The ST was updated with the correct link in section 1.5.2.2. Version 1.14 of the ST contains the error and version 1.15 of the ST contains the fix.

Changes to the TOE:

The fix to the Vertiv CYBEX™ SCMV2160DPH, SC840DVIE, SC940DVIE, SC840HE, SC940HE, SC840DPE, SC940DPE Firmware Version 44404-E7E7 Peripheral Sharing Devices Security Target is summarized below.

Major Changes

None.

Minor Changes

The TOE security target (ST) version 1.14 had an erroneous link in section 1.5.2.2 which has been corrected in version 1.15. This link was: support@highseclabs.com but has been changed to: support.avocent@vertiv.com. No other changes have been made to the TOE or evidence documentation.

Regression Testing:

Not Applicable

NIST CAVP Certificates:

Not Applicable

Vulnerability Analysis:

A public search for vulnerabilities that might affect the TOE was performed on January 5, 2022.

A search of the following national sites was conducted:

- National Vulnerability Database: https://nvd.nist.gov/vuln/search
- Vertiv Support: https://www.vertiv.com/en-ca/support/
- Common Vulnerabilities and Exposures: https://google.com

The terms used to search within the previous websites are several combinations of the following words:

- Vertiv
- Vertiv KVM
- Vertiv Firmware
- Firmware Version 44404-E7E7
- Vertiv Peripheral Sharing Device
- SCMV2160DPH
- SC840DVIE
- SC940DVIE
- SC840HE
- SC940HE
- SC840DPE
- SC940DPE
- Cybex
- AFP0008
- AFP0004
- NAK transaction
- SYNC Signal
- HPD signal
- EDID traffic
- ARC Signal
- HDCP signal
- USB HID traffic
- STMicroelectronics 32-Bit.

Summary of the analysis

National Vulnerability Database

No current vulnerabilities were found.

The term “Vertiv” returned 3 matches for a UMG-4000 product which were found not to be relevant to the TOE.
The term “NAK transaction” returned 3 matches for non-TOE products with a DHCP protocol-specific vulnerability. The TOE is not a networked device.
The term “SYNC signal” returned 4 matches that are not relevant to the TOE technology type.
The term “STMicroelectronics 32-bit” did not return any results. The evaluator augmented this search with the specific proprietary system controller part numbers utilized in each TOE model and also found no results. In researching known vulnerabilities on similar STMicroelectronics controllers, it was found that any exploits would require a physical attacker with access to the interior of the unit, which would be mitigated by the anti-tamper mechanisms available in the TOE.
No other search terms provided any potential matches.

Vertiv Support

No current vulnerabilities were found.

Common Vulnerabilities and Exposures

No current vulnerabilities were found.

Summary of the analysis

All vulnerabilities returned by the search were deemed not applicable to the TOE and no current vulnerabilities were found.

Conclusion:

The overall impact is minor. This is based on the rationale that fix was unrelated to TOE functionality and issued to fix a incorrect vendor link in the ST.

Therefore, CCEVS agrees that the original assurance is maintained for the product.