ASSURANCE CONTINUITY MAINTENANCE REPORT FOR KLC Advantech Drives Firmware Version: SCPB15.0/ECPB15.0

KLC Advantech Drives Firmware Version: SCPB15.0/ECPB15.0

Maintenance Report Number: CCEVS-VR-VID11453-2025

Date of Activity: 10 March 2025

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- KLC Advantech Drives Firmware Version: SCPB15.0/ECPB15.0 Impact Analysis Report, Version 1.1, March 2025
- Collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0, February 1, 2019

Original Documentation:

- KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 Security Target, Version 1.4, June 2024
- KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 Common Criteria Guide, Version 1.1, June 2024

Revised Documentation:

- KLC Advantech Drives Firmware Version: SCPB15.0/ECPB15.0 Security Target, Version 2.0, January 2025
- KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 Common Criteria Guide, Version 2.0, January 2025

Assurance Continuity Maintenance Report:

Lightship Security submitted an Impact Analysis Report (IAR) for the KLC Advantech Drives, Firmware Version: SCPB13.0/ECPB13.0 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 24 January 2025. 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, the Common Criteria Guide, and the Impact Analysis Report (IAR) (see above for a full list of documentation). The ST, CC Guide, and IAR were updated.

The information below has all been pulled from the IAR, updated ST and updated AGDs provided for this assurance maintenance action.

Documentation updated:

Original CC Evaluation Evidence	**Evidence Change Summary**
KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 Security Target, Version 1.3, May 2024	The ST has been revised to update the following: • Title Page • ST Reference • TOE Reference • Guidance document versions • Added new TOE Firmware to 'TOE Hardware / Firmware' table
Design Documentation: See Security Target and Guidance	See Security Target and Guidance changes in this table
Guidance Documentation: KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 Common Criteria Guide, Version 1.0, May 2024	The AGD has been revised to update the following: • Title Page • TOE Reference • Added new TOE Firmware to 'TOE Hardware / Firmware' table
Lifecycle: None	No changes required.
Testing: None	No changes required. The developer successfully performed regression tests as described below.
Vulnerability Assessment: None	Lightship Security performed a search of public information for potential vulnerabilities. The search was in accordance with Labgram #116/Valgram #135 - Vulnerability Evidence. The following public sources were searched on **March 10, 2025**. See more details including search terms below.

Changes to the TOE:
The changes are summarized below.

Major Changes
None.

Minor Changes
The only change to the certified TOE is the following:

- **Firmware.** To support BiCS5 technology, SCPB15.0 and ECPB15.0 firmware was added.

Hardware Changes and Impact
There are no changes to hardware components. The same controller module used in the Validated TOE for the SCPB13.0 firmware (Controller PS3112-S12) and ECPB13.0 firmware (Controller PS5012-E12) is supported for the new firmware composition in the Changed TOE.

Firmware Changes and Impact
The new SCPB15.0 and ECPB15.0 firmware adds support and configuration for Bit Cost Scalable 5 (BiCS5) storage technology. BiCS5 increases storage capacity per unit and improves performance in NAND Flash. Due to the larger physical block size of BiCS5, code changes were made to support Redundant Array of Independent Disks Error Correction Code (RAIDECC) functionality.

The changes to the TOE firmware are assessed as MINOR for the following reasons:

- BiCS5 is a performance enhancement and has no impact on the cryptographic functionality. Cryptographic functionality is provided by the controller, which has not changed.
- The type of NAND supported has not changed (TLC and SLC).
- The most significant code change was support for RAIDECC. RAID is unevaluated functionality that is not touched in any way by the CC testing of SFRs.

All changes to the TOE have been assessed as minor and do not affect the security functionality or claims of the previously evaluated TOE.

As per the previous evaluation documented in "KLC Advantech Drives Firmware Version: SCPB13.0/ECPB13.0 Security Target, Version 1.3, May 2024", together with this assurance continuity activity, the final set of claimed evaluated devices is:

Series	CC Listed P/N & Version	Advantech P/N & Version	Form Factor	Controller	FW Version
840F	SQF-2020-1TSCB	SQFFS25V8-1TSC	2.5" SATA	PS3112-S12	SCPB15.0
840F	SQF-2020-512SCB	SQFFS25V8-512GSC	2.5" SATA		

840F	SQF-2020-256SCB	SQFFS25V4-256GSC	2.5" SATA		
840F	SQF-2020-128SCB	SQFFS25V2-128GSC	2.5" SATA		
840F	SQF-2020-1TSCM	SQFFSM8V4-1TSC	M.2 SATA		
840F	SQF-2020-512SCM	SQFFSM8V4-512GSC	M.2 SATA		
840F	SQF-2020-256SCM	SQFFSM8V4-256GSC	M.2 SATA		
840F	SQF-2020-128SCM	SQFFSM8V2-128GSC	M.2 SATA		
920F	SQF-2040-1TECM	SQFFCM8V4-1TEC	M.2 NVMe	PS5012-E12	ECPB15.0
920F	SQF-2040-512ECM	SQFFCM8V4-512GEC	M.2 NVMe		
920F	SQF-2040-256ECM	SQFFCM8V4-256GEC	M.2 NVMe		

Developer Testing

The developer has provided QA testing reports for both ECPB15.0 and SCPB15.0 firmware versions. These reports contain testing evidence that demonstrate nominal functionality and confirms the TOE performs as expected on claimed models. Lightship Security has reviewed this testing evidence and confirms the TOE operates as expected and maintains claimed functionality.

The Developer successfully performed the following regression tests:

- **Device Information Check.** Checks DUT's Identify/Smart information.
- **NVME Protocol Test.** Tests the PCIe NVMe protocol for SSD products.
- **ULINK NVME Regression Test.** Regression testing of the PCIe protocol for SSD products by Drive Master Tool.
- **Burn-In Test.** Verifies the firmware can correctly handle different combinations of Read/Write processes.
- **SPOR Test.** Verifies DUT can still function normally after a sudden power-off and recovery.
- **Production Flow Test.** Verifies production flow on different devices.
- **FIPS Test.** Verifies FIPS certification for SSD products by performing FIPS command patterns.

Assurance Activity Requirements
No changes were made to the Security Functional Requirements or Security Assurance Requirements, therefore no updates to the Assurance Activities were necessary.

NIST CAVP Certificates:
No CAVP changes.

Vulnerability Analysis:
Lightship Security performed a search of public information for potential vulnerabilities. The search was in accordance with Labgram #116/Valgram #135 - Vulnerability Evidence. The following public sources were searched on **March 10, 2025**.

- NIST National Vulnerability Database: https://nvd.nist.gov
- MITRE CVE Search: https://cve.mitre.org/cve/search_cve_list.html

The search terms listed below were used from the initial evaluation:

- Drive encryption
- Disk encryption
- Key destruction
- Key sanitization
- Self Encrypting Drive
- SED
- OPAL
- SQFFS25V4-256GSC
- SQFFS25V2-128GSC
- SQFFSM8V4-1TSC
- SQFFSM8V4-512GSC
- SQFFSM8V4-256GSC
- SQFFSM8V2-128GSC
- SQFFCM8V4-1TEC
- KLC Advantech
- SQFFS25V8-1TSC
- SQFFS25V8-512GSC
- SQFFCM8V4-512GEC
- SQFFCM8V4-256GEC
- PS3112-S12
- PS5012-E12
- cpe:2.3:h:arm:arm7:-:*:*:*:*:*:*:*:*
- cpe:2.3:h:arm:cortex-r:-:*:*:*:*:*:*:*:*
- ARM Cortex-R5

The following search terms were removed due to the changed TOE:

- SCPB13.0
- ECPB13.0

The following search terms were added due to the updated TOE:

- SCPB15.0
- ECPB15.0

The vulnerability search was performed on 10th March 2025. No open vulnerabilities applicable to the TOE were identified. All known public security vulnerabilities are mitigated in the TOE version. KLC asserts that there are no known exploitable public vulnerabilities in the changed TOE as of the publication date of this Assurance Maintenance Action.

Conclusion:
The evaluation evidence consists of the Security Target and CC-specific Guidance Documentation. Both the Security Target and Guidance Documentation were revised to include the updated firmware versions. The overall impact is minor. This is based on the rationale that updates do not change any security policies of the TOE and are unrelated from SFR/SAR claims.

There are no changes to TSF Interfaces, no SFR changes, no changes to assumptions threats or objectives and no CAVP changes. Regression testing was done to verify that the TOE performs as expected on the claimed models. Lightship Security has reviewed this testing evidence produced by the developer and confirms the TOE operates as expected and maintains claimed functionality. The reasoning is considered adequate based on the scale and types of changes made. The vulnerability search also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. The impact of all TOE changes on the assurance baseline is assessed to have an impact of minor severity and is within the parameters of the Assurance Continuity Framework.

In review of the changes between TOE versions, no change has been made that impacts the evaluated configuration of the TOE. The product properly maintained conformance to the protection profile and no changes made to the product firmware impacts the functionality claimed within the original Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.