ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Scalar and Express P-series SSD, version NV.R1900

Scalar and Express P-series SSD, version NV.R1900

Maintenance Report Number: CCEVS-VR-VID11262-2024

Date of Activity: 16 April 2024

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Impact Analysis Report for Scalar and Express P-series SSD, version NV.R1900, version 1.1, 5 April 2024
- Scalar and Express P-series SSD, version NV.R1900 Security Target, version 1.2, 19 February 2024
- Non-Proprietary Administrative Guidance, version 1.2, 16 February 2024
- collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0e, February 1, 2019
- collaborative Protection Profile for Full Disk Encryption – Authorization Acquisition, Version 2.0e, February 1, 2019

Assurance Continuity Maintenance Report:

UL submitted an Impact Analysis Report (IAR) for the Scalar and Express P-series SSD, version NV.R1900 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 11 April 2024. 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 Administrator's Guide, and the Impact Analysis Report (IAR). The ST, Admin Guide, and IAR were updated.

The updated documentation table, the minor change breakdown and the vulnerability analysis have all been pulled directly from the IAR.

Documentation updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Scalar and Express P-series SSD, version NV.R1900 Security Target, version 1.0, 06 June 2022	*Security Target Assurance Activity changes:* ASE_INT.1-8 rationale is affected by the inclusion of the new form factors in the maintained TOE. *Security Target Documentation Changes:* ST Cover page and ST Section 1.1 changed version of ST to v1.2, and the date of document changed to 'February 19, 2024'. The 'footer' in the ST changed 'Version 1.1' to "Version 1.2". Sections 1.2, Table1 and Section 1.3.1 were updated to include the proposed models in the maintained TOE. Section 1.3.4. was updated to include descriptions of the proposed models in the maintained TOE, in terms of their form factor and with regards to the operational environment that the proposed models are compatible with. Section 2.2 was updated to include the latest TDs. These include TD0767 and TD0760. Section 6.1.3.2 – FMT_SMF.1.1(AA) was updated to apply TD0767. Section 9, Table 14 was updated to include the updated title/version/date of the Guidance Documentation.
Design Documentation: See Security Target and Guidance	No changes required
Guidance Documentation: Non-Proprietary Administrative Guidance, version 1.0, 03 March 2022	*Guidance Documentation Assurance Activity changes:* AGD_PRE.1-3-PP is affected by the inclusion of the new models into the rationale of this specific work unit. *Guidance Documentation Changes:* Document version changed to v1.2. Multiple sections were updated to improve grammar, spelling and overall readability without modifying meaning. These changes are numerous

	and have not be identified with greater fidelity than this. Section 1 was updated to describe the form factors supported in the maintained TOE (RMM and R-SATA). Section 2 was updated to reiterate the new form factors that are supported in the maintained TOE (RMM and R-SATA). Section 3 was updated to include the list of the 10 new models proposed for the maintained TOE. Figure 5 was updated to include the images of the new R-SATA model for the maintained TOE. Figures 6 through 7 were shifted up in figure number to make room for the new Figure 5. Figure 8 was added to include images of the new RMM model. Figures 9 through 13 were shifted up in figure number to make room for the new Figure 8. Section 4 was updated to include new models for the maintained TOE; providing details with regards to the connector/pinouts for the new RMM and R-SATA form factors. New part numbers were added to account for the proposed models for the Maintained TOE. Figure 15 was added to describe the R-SATA connector in detail – subsequent figures were incremented to make room for Figure 15. Figure 18 was added to describe the RMM connector in detail – subsequent figures were incremented to make room for Figure 18. Figure 26 was updated to show the tamper-evident label locations for the SATA and R-SATA models. Section 10 was updated to include the new models of the maintained TOE. This section clarifies that the RMM form factor does not support the 'optional' method of invoking TSF. The implications of this is described in detail in the "TSFI Interfaces" row of this table.

	Table 10 was updated to include the R-SATA and RMM form factors; clarifying the accessibility of the secure erase TSF on a per-form-factor basis. Section 12 was updated to fix grammar. Section 19 was updated to include installation instructions for new models in the maintained TOE. Section 30 included an updated table to include the new models.
Lifecycle: None	No changes required.

Testing:
None
	No changes required.
	
	All functional tests performed previously in the validated TOE were reperformed by the developer on the following models from the set of proposed models, with no testing failures:
	- NS361P500GCC0-1S
	  o R-SATA form factor
	- NS369P500GVR3-1F
	  o RMM form factor

Vulnerability Assessment: None	The public search was updated on 3/5/2024. No public vulnerabilities exist in the product. See analysis results below.

Changes to the TOE:
The changes are summarized below.

Major Changes
None.

Minor Changes
No changes were made to the individual products within the validated TOE.

Additional models are proposed containing new form factors (in terms of size and connectors) but with the same protocols (SATA and PCIe/NVMe) which were fully evaluated in the Assurance Baseline. No hardware components are being added to the models in the validated TOE outside of the form factor / connector changes explicitly described in tables below. The changes in hardware are not considered to be security relevant. Ten models of storage drives are proposed for addition.

As per the previous evaluation documented in the "Scalar and Express P-series SSD, version NV.R1900 Security Target, version 1.1, 22 February 2023", together with this assurance continuity activity, the final set of claimed supported evaluated devices is:

TOE developer Original Part No.	HW Ver.	Description (Form factor & Interface)	Firmware Ver.	User Capacity	Certification Sponsor Reseller Part No.
Previously Validated TOE Models					
NS361P500GCCR-1F	04MB3	2.5" SATA 7mm	NV.R1900_1000	500GB	AMP25T500-IM02AI
NS371P01T0CC1-1F	04MN3	2.5" SATA 7mm	NV.R1900_1000	1TB	AMP2500T0T10-IM020CP
NS371P02T0CC1-1F	08MN3	2.5" SATA 7mm	NV.R1900_1000	2TB	AMP25TT20-IM02AI
NS371P04T0CC1-1F	16MN3	2.5" SATA 7mm	NV.R1900_1000	4TB	AMP25TT40-IM02AI
NS371P08T0CC0-1F	16MN3	2.5" SATA 9.5mm	NV.R1900_1000	8TB	AMP2500T08T0-IM020CP
NS371P10T0CC0-1F	16MN3	2.5" SATA 9.5mm	NV.R1900_1000	10TB	AMP25TT10-IM02AI
NS379P16T0VC0-1F	32MN1	2.5" SATA 9.5mm	NV.R1900_1000	16TB	AMP2500T16T0-IM020CP
NS379P20T0VC0-1F	32MN1	2.5" SATA 9.5mm	NV.R1900_1000	20TB	AMP2500T20T0-IM020CP
NS361P125GCM7-1F	04MBB	M.2 2242, SATA	NV.R1900_1000	125GB	AMPW300T0125-IM020CP
NS369P250GVM7-1F	04MBA	M.2 2242, SATA	NV.R1900_1000	250GB	AMPW300T0250-IM020CP
NS369P500GVM7-1F	04MBA	M.2 2242, SATA	NV.R1900_1000	500GB	AMPW300T0500-IM020CP
NS369P01T0VE7-1F	04MB1	M.2 2280, SATA	NV.R1900_1000	1TB	AMPW500T0T10-IM020CP
NS369P01T0VA7-1F	04MB1	mSATA SATA	NV.R1900_1000	1TB	AMPV500T0T10-IM020CP
NS569P500GVM7-1F	04MBA	M.2 2242, PCIe/NVMe	NV.R1900_1000	500GB	AMPW300D0500-IM020CP
NS561P500GCE7-1F	02MB3	M.2 2280 PCIe/NVMe	NV.R1900_1000	500GB	AMPW5D500-IM02AI
NS571P02T0CK7-1F	16SN3	M.2 22110 PCIe/NVMe	NV.R1900_1000	2TB	AMPW6DT20-IM02AI
NS579P04T0VK7-1F	16SN1	M.2 22110, PCIe/NVMe	NV.R1900_1000	4TB	AMPW600D04T0-IM020CP
NS571P08T0CC0-1F	16MN3	2.5” PCIe/NVMe (U.2)	NV.R1900_1000	8TB	AMP2UDT80-IM02AI
New TOE Models					
NS571P01T0CC0-1F	16MN3	2.5” PCIe/NVMe (U.2)	NV.R1900_1000	1TB	AMP2U00D0T10-IM020CP

NS571P02T0CC0-1F	16MN3	2.5" PCIe/NVMe (U.2)	NV.R1900_1000	2TB	AMP2U00D0T20-IM020CP
NS571P04T0CC0-1F	16MN3	2.5" PCIe/NVMe (U.2)	NV.R1900_1000	4TB	AMP2U00D0T40-IM020CP
NS361P250GCC0-1S	04MB3	2.5" SATA 9.5mm R-SATA	NV.R1900_1000	250GB	AMP2500F0250-IM020CP
NS361P500GCC0-1S	04MB3	2.5" SATA 9.5mm R-SATA	NV.R1900_1000	500GB	AMP2500F0500-IM020CP
NS369P01T0VC0-1S	04MB3	2.5" SATA 9.5mm R-SATA	NV.R1900_1000	1TB	AMP2500F0T10-IM020CP
NS369P02T0VC0-1S	04MB3	2.5" SATA 9.5mm R-SATA	NV.R1900_1000	2TB	AMP2500F0T20-IM020CP
NS361P125GCR3-1F	04MBB	RMM form factor	NV.R1900_1000	125GB	2026640-003
NS369P250GVR3-1F	04MBA	RMM form factor	NV.R1900_1000	250GB	2026640-003
NS369P500GVR3-1F	04MBA	RMM form factor	NV.R1900_1000	500GB	2026640-003

The table below identifies each of the ten proposed models, the differences between the proposed models and those within the validated TOE, and a determination as to whether the differences are considered security relevant.

Identifying Delta Between the Validated TOE and proposed TOE Models			
Identifier of the proposed model *(This identifier is a.k.a. the "TOE developer Original Part No.")*	Description	Changes	Security Relevant Change?
(Group A) NS361P250GCC0-1S; NS361P500GCC0-1S; NS369P01T0VC0-1S; NS369P02T0VC0-1S	Proposed models are functionally equivalent to all models of the Validated TOE. The following models of the Validated TOE share the highest degree of similarity in terms of form factor, specifically, the following models of the Validated TOE are characterized as "2.5 SATA 9.5mm" form factor whereas the proposed models are characterized as "2.5" SATA 9.5mm R-SATA" where "R-SATA" denotes a 'ruggedized' SATA connector: - NS371P08T0CC0-1F - NS371P10T0CC0-1F - NS379P16T0VC0-1F	*Storage Capacity:* - Proposed models have the new storage capacities of 250GB, 500GB, 1TB and 2TB, as compared to the capacities of 500GB, 2TB and 4TB in comparable models of the validated TOE. *Connector Form factor:* - Proposed models have a ruggedized connector for the '2.5" SATA' drive form factor (maintaining the EIA	No.

		SFF-8201 specification). The ruggedization is provided by structural form of the physical connector mating pairs while maintaining identical pinout morphology and logic.	
(Group B) NS361P125GCR3-1F; NS369P250GVR3-1F; NS369P500GVR3-1F	Proposed models are functionally equivalent to all models of the Validated TOE, with the following exception: - Proposed models do not have access to GPIO pins. As such, the 'secure erase' security functionality cannot be initiated via GPIO; however, 'secure erase' TSF is still accessible via the normal SATA data pins, identical to all other models in the Validated TOE. For these proposed models, initiating the 'secure erase' TSF operates identically to the 'secure erase' TSF in the Validated TOE, regardless if initiated by an ATA/NVM command via the typical data pinout, or from a voltage signal on the specific GPIO pin. Thus, the absence of the GPIO interface is not considered an impact to the Assurance Baseline. The following models of the Validated TOE share the highest degree of similarity in terms of form factor, specifically, the following model of the Validated TOE is characterized as a "2.5" PCIe/NVMe (U.2)" formfactor whereas the proposed models are characterized as "RMM Form Factor" where "RMM" denotes a 'ruggedized' SATA connector, without GPIO access: - NS371P08T0CC0-1F - NS371P10T0CC0-1F - NS379P16T0VC0-1F - NS379P20T0VC0-1F	*Storage Capacity:* - Proposed models have 8TB, 16TB, and 20TB capacity as compared to the capacity of 10TB for the previously validated comparable model. *Connector Form factor:* - Proposed models have a ruggedized connector for the '2.5" SATA' drive form factor (maintaining the EIA SFF-8201 specification). The ruggedization is provided by structural form of the physical connector mating pairs. SATA pinout is rearranged in a novel configuration. New pinout houses 7 total pins – maintaining the 7 SATA power/data pins present on all Validated TOE models while excluding the GPIO pins.	No.

Group C) NS571P01T0CC0-1F; NS571P02T0CC0-1F; NS571P04T0CC0-1F	Proposed models are functionally equivalent to all models of the Validated TOE. The following models of the Validated TOE share the highest degree of similarity in terms of form factor, specifically, the following models of the Validated TOE are characterized as "2.5" PCIe/NVMe (U.2)" form factor which is identical to the following Validated TOE model: - NS571P08T0CC0-1F The only difference between the proposed model and the Validated TOE model is in terms of storage capacity.	*Storage Capacity:* - Proposed models have the new storage capacities of 1TB, 2TB, and 4TB as compared to the capacity of 8TB in the listed Validated TOE model. *Connector Form factor:* - Proposed models have identical form factor.	No.

Regression Testing:
All functional tests performed previously on the validated TOE were reperformed by the developer on the following models from the set of proposed models, with no testing failures:

- NS361P500GCC0-1S
  - R-SATA form factor
- NS369P500GVR3-1F
  - RMM form factor

TSF Interfaces:
Proposed models in Group B have identical TSFI with the exception that GPIO pins are not accessible owing to the smaller footprint of the ruggedized connector. The GPIO pins that are accessible in Validated TOE models are present for redundancy and/or as an alternative method of invoking the 'secure erase' TSF. The method of invoking the 'secure erase' TSF has no impact on the TSF itself and therefore the Evaluation team sees no impact to the Assurance Baseline.

NIST CAVP Certificates:
The new TOE models are covered under the original CAVP certificates.

Vulnerability Analysis:
The evaluation team performed each AVA_VAN.1 CEM work unit (as refined by the SD) and each AVA_VAN evaluation activity defined in the SD. A vulnerability analysis was performed following the processes described in the PP. The vulnerability analysis included a public domain search for potential vulnerabilities. This search was performed on March 5, 2024. The following public vulnerability repositories were utilized:

- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/
- National Vulnerability Database: https://nvd.nist.gov/
- US-CERT http://www.kb.cert.org/vuls/html/search

The following search terms were utilized:

- Novachips

- ASIC
- Scalar and Express
- NVS3800
- drive encryption
- disk encryption
- "SED"
- NVMe
- NV.R1900
- SSD
- self-encrypting

The search resulted in no vulnerabilities that are applicable to the TOE. No residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

Conclusion:
The changes to the validated TOE are in form factor and/or storage capacity, with the consideration pertaining to TSFI as described in the "TSF Interfaces" section above. While storage capacity rarely, if ever, has security implications pertaining to Full Drive Encryption products, the form factor may have security relevant differences with regards to communication protocols between the host and device, if new protocols are introduced. However, no new protocols are introduced with the addition of the proposed models and form factors.

Testing performed in the assurance baseline covered both PCIe/NVMe and SATA; two host expansion bus protocols. The proposed models are either of PCIe/NVMe or SATA protocol.

The remaining difference between the proposed models and validated TOE pertain to storage capacity, which again, the CCTL considers to be non-security relevant. There was no impact to the CAVP certificates.

Furthermore, each of the proposed models/form factors utilize the identical microcontroller and firmware as the models within the validated TOE. There are no SFR changes, no new security features, no changes to assumptions and objectives, no ATE changes, no ALC changes, no ADV_FSP changes, no new assurance evidence, no new non-security features and no bug fixes.

Full coverage in Functional Testing evaluation activities performed in the assurance baseline is maintained with the proposed changes.

Given this, the CCTL determined that the proposed changes are not security relevant and thus the quality of the impact is considered 'minor'.

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