ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Seagate® Secure NVMe Self-Encrypting Drives

---

Seagate® Secure NVMe Self-Encrypting Drives

Maintenance Report Number: CCEVS-VR-VID11416-2026

Date of Activity: April 6, 2026

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Seagate® Secure NVMe Self-Encrypting Drives Impact Analysis Report, Version 1.2, April 2, 2026
- Seagate® Secure NVMe Self-Encrypting Drives Security Target, Version .26, March 18, 2026
- Seagate Secure® NVMe Self-Encrypting Drive Common Criteria Configuration Guide, Version 1.3, March 27th, 2026
- Seagate® Secure NVMe Self-Encrypting Drives Common Criteria Full Drive Encryption – Encryption Engine Key Management Description, Version 1.0, March 27, 2026
- collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 + Errata 20190201, February 1, 2019 [CPPFDE_EE]

Assurance Continuity Maintenance Report:

Seagate® Technology LLC. submitted an Impact Analysis Report (IAR) for the Seagate Secure® NVMe Self-Encrypting Drives to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on March 2, 2026. 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 (ST), the Administrator's Guide (AGD), the Key Management Description (KMD), and the IAR. The ST, AGD, and KMD were updated to the new version of the TOE.

Documentation updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Seagate® Secure NVMe Self-Encrypting Drives Security Target, Version 0.24, March 7, 2024	**Maintained Security Target:** See references above. Updated to identify the new Firmware version number and removed firmware version SGEBHG02. Removal of SGEBHG02 also required removal of try limits related to the firmware. ST also updated AGD version and date references.
Design Documentation: See ST, KMD, and Guidance	No changes required
Guidance Documentation: Seagate Secure® NVMe Self-Encrypting Drives Common Criteria Configuration Guide, Version 1.3, March 27th, 2024	**Maintained Guidance Documentation:** See references above. Updated to identify the new Firmware version number and removed firmware version SGEBHG02. Removal of SGEBHG02 also required removal of try limits related to the firmware.
Key Management Description: Seagate® Secure NVMe Self-Encrypting Drives Common Criteria Full Drive Encryption – Encryption Engine Key Management Description, Version 0.95, March 7, 2024	**Maintained Key Management Description:** See references above. Updated to identify the new Firmware version number and removed firmware version SGEBHG02. Removal of SGEBHG02 also required removal of try limits related to the firmware. Updates also made to integrity check values and DRAM. ST and AGD version and date references also updated.
Lifecycle: None	No changes required.
Testing: None	As provided in more detail below, the Vendor's Firmware Quality and Assurance and Validation team performed the regression testing. Automated test cases from the initial evaluation were re-run. Additional ULink TCG OPAL and NVME protocol test patterns were run, and interface integrity and power-cycling stress tests were run. All tests were successful.

Vulnerability Assessment: None	The public search was updated on March 30, 2026. No public vulnerabilities exist in the product. See analysis results below.

Changes to the TOE:
The TOE firmware has been updated from revision SE4SA530 to revision SE4SA550. The SGEBHG02 firmware version included in the evaluated TOE has been removed from the maintained TOE. Below is a summary of the changes incorporated in the new firmware version.

Major Changes

None.

Minor Changes

Five updates were identified in the IAR from versions SE4SA530 to SE4SA550 along with a description and given rationale. The description and rationale for each enhancement were inspected and the overall Minor Change characterization was considered appropriate. None of the changes resulted in the introduction of new TOE capabilities, modification to security functions as defined in the ST, or changes to the TOE boundary. The following table includes a summary of the detailed changes presented in the IAR.

Change Description	Impact
Firmware improvement - TCG Storage protocol fix for TCG ACE structure.	No change to the TOE security functionality. TCG Storage protocol functionality is not in the scope of the evaluation.
Firmware improvement - TCG Storage protocol fix for internal table logic.	No change to the TOE security functionality. TCG Storage protocol functionality is not in the scope of the evaluation.
Compliance - Tighter DRBG settings and startup check for FIPS140-3 compliance.	No change to the TOE security architecture.
Reporting - FIPS 140-3 compliance reporting name change and indicator enhancement.	No impact to the TOE security functionality.
Self-test refinement - PBKDF2 power-on self-test iteration count update.	No change to evaluated security functionality.

Regression Testing:
The Vendor's Firmware Quality and Assurance and Validation team performed the regression testing on all hardware variants. Applicable test cases from the automated test script used in the initial evaluation were re-run. Additionally, ULink TCG OPAL test patterns were run to verify TCG OPAL compliance, NVMe protocol test patterns were run to test protocol and interface integrity, and power-cycling stress tests were run to determine performance and reliability. The successful completion of

all these tests provided the Vendor with confidence in the proper behavior of the new firmware.

Equivalency:
The security functionality of the firmware version update to SE4SA550 remains the same as the prior evaluated version. The changes do not introduce new cryptographic functionality, modify the security boundary of the TOE, or change the Security Functionality Requirements of the TOE. The overall security functionality and operational behavior of the TOE remain unchanged except that Try Limits beyond 5 are no longer supported. That change is a result of the removal of the SGEBHG02 firmware. The hardware platforms are unchanged from the original evaluation version.

NIST CAVP Certificates:
The CAVP certificate numbers referenced during the SE4SA530 evaluation have not changed and remain applicable to the maintained TOE.

Vulnerability Analysis:
A new search was performed for vulnerabilities from the time of the original evaluation (April 4, 2024) to May 9, 2024. The search was conducted against the same vulnerability databases and used the same terms as the original evaluation, with the exception of the firmware version: "Seagate", "Phison", "Nytro", "PS5020-E20", "SE4SA550", "Arm Cortex-R5", "ARMv7-R", "self encrypting drive", "opal", "drive encryption", "disk encryption", "key destruction", and "key sanitization".

The results of the vulnerability assessment were included in the IAR. No new TOE vulnerabilities were found.

Conclusion:

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 to SFR claims. The updates described above were made to support the updated TOE firmware.

Regression testing was done and was considered adequate based on the scale and types of changes made. The vendor also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. In addition, the platforms did not change and there were no necessary alterations to the NIST cryptographic certificates. Therefore, CCEVS agrees that the original assurance is maintained for the product.