CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Seagate Secure ® TCG SSC Self-Encrypting Drives (CPP FDE EE V2.0E)

Maintenance Report Number: CCEVS-VR-VID10857-2019-5

Date of Activity: 11 December 2019

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." March 20, 2013

Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements" Version 1, February 2004

Seagate Secure ® TCG SSC Self-Encrypting Drives Impact Analysis Report #5 Version 1.0 November 27, 2019

Seagate Secure ® TCG SSC SED Security Target Version 6.0, Proprietary November 27, 2019

Seagate Secure® TCG Enterprise SSC Self-Encrypting Drive and TCG Opal SSC Self-Encrypting Drive Common Criteria Full Drive Encryption – Encryption Engine Key Management Description, Version 6.0 November 27, 2019

Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 6.0 November 27, 2019

Affected Evidence:

Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 6.0 Proprietary November 27, 2019

Updated Developer Evidence:

Code change did not have any impact on the developer evidence of the validated TOE.

Description of ASE Changes:

Seagate Technology, LLC. submitted an Impact Analysis Report (IAR #5) to CCEVS for approval to add one new version of firmware, based on an existing Common Criteria certified version, to four Common Criteria certified Seagate product models. The new firmware version EF02 is based on the existing certified firmware revision EF01. The IAR specifies that the update to the firmware is one non-security relevant code change to improve 2MB/4MB random read and write performance which does not impact the underlying security architecture.

Changes to TOE:

A new firmware version EF02, which is based on the existing certified firmware revision EF01, was added to 4 validated hardware version models. The update to the firmware is one non-security relevant code change to improve 2MB/4MB random read and write performance which does not impact the underlying security architecture.

The hardware models use the firmware versions as shown in the following table.

Validated Hardware Versions	New Firmware Versions
ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	EF02

Description of ALC Changes:

Changes to the following documents were made, going from version 5.0 to 6.0:

- Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 6.0 Proprietary November 27, 2019
- Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 6.0 Public November 27, 2019
- Seagate Secure® TCG Enterprise and TCG Opal SSC Self-Encrypting Drive Common Criteria Configuration Guide, Version 6.0 Dated: November 27, 2019.
- Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 6.0 Dated: November 27, 2019
- Seagate Secure® TCG Enterprise SSC Self-Encrypting Drive and TCG Opal SSC Self-Encrypting Drive Common Criteria Full Drive Encryption – Encryption Engine Key Management Description Report Version 6.0 Dated: November 27, 2019

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR) for the four Common Criteria certified models listed above

- The IAR specifies that the update to the firmware is one non-security relevant code change to improve 2MB/4MB random read and write performance which does not impact the underlying security architecture.
- There are no changes to the development environment.
- Code change did not have any impact on the developer evidence of the validated TOE.
- The changes to the ST and other documents were limited to document version with the addition of the new firmware version.

Description of Regression Testing:

For all storage products, Seagate performs a lengthy and rigorous suite of regression tests before releasing any firmware revisions. Regression testing performs a comprehensive set of security and non-security related test cases, including tests for device I/O throughput and performance, device read/write verification, servo performance, shock and vibration, environmental, secure port locking, firmware updates, secure boot signature verification and roll back protection. In addition, secure SED and FIPS or CC certified secure storage products are tested for all aspects of security including all TCG commands, ATA commands, FDE encryption modes, credentials, retry limits, band creation and deletion, and FIPS and CC mode testing. The entire regression test process takes about 21 days to complete. Regression testing was conducted for these firmware releases starting September 6, 2019 and ending October 12, 2019.

Vulnerability Assessment:

Seagate searched 3 vulnerability databases, National Vulnerability Database (NVD, https://nvd.nist.gov/), MITRE Common Vulnerabilities and Exposures (CVE, http://cve.mitre.org/cve/), and United States Computer Emergency Readiness Team (US-CERT, http://www.kb.cert.org/vuls/html/search) for a large number of terms, on November 20, 2019. No new vulnerabilities were found.

Vendor Conclusion:

The 'Description of Changes' section (Chapter 2) of the IAR indicates that there are no changes to the development environment of the validated TOE. That section of the IAR further indicates that there is one code change to the product associated with the validated TOE and is not security relevant. Based on this and other information from within this IAR document, the assurance impact of these changes is minor.

Validation Team Conclusion:

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. The updated Security Target, the Entropy Document, and the Key Management Description were only changed to add the new firmware version identified above. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.