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-VID10857-2020-3

Date of Activity: 28 September 2020

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 #8 Version 1.0 August 10, 2020

Seagate Secure ® TCG SSC Self-Encrypting Drives Security Target Version 9.0, Proprietary August 10, 2020

Seagate Secure ® TCG SSC Self-Encrypting Drives Security Target Version 9.0, Public August 10, 2020

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 9.0 August 10, 2020

Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 9.0 August 10, 2020

Affected Evidence:

Seagate Secure ® TCG SSC Self-Encrypting Drives Security Target Version 9.0, Proprietary August 10, 2020

Seagate Secure ® TCG SSC Self-Encrypting Drives Security Target Version 9.0, Public August 10, 2020

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 #8) to CCEVS for approval to add twenty-three new Seagate product models and one new firmware version, 0001. The sole hardware change is replacing the NAND BIC53 with BIC54. The hardware change is minor in scope to achieve a more compact physical PCB layout. The table below shows the new model numbers and the new firmware version.

Changes to TOE:

In the updated ST, version 9, Table 2 shows the two new Product Names (Nytro® 2032 SSD and Nytro® 3032 SSD), with the 23 new models split between them, Balto ASIC, new firmware version 0001, and 'Firmware implementations (for each model) as identified by CAVP'. This table shows only 4 firmware implementations, all Balto ASIC. Table 3 shows that the 23 new models are in the first column/group of models select 11 different firmware implementations. It appears that the other 7 firmware implementations are for the older models. The IAR is silent on the firmware implementations but does specify the new firmware version 0001. It should also be noted that the 4 firmware implementations for the 23 new models in the two new products are not new and are used in older models.

These code changes did not impact the crypto software and, therefore, did not require update to the CAVP certificates. There were no changes to the EAR except to add the new hardware models and the new firmware version.

The products, models, and firmware versions are shown in the table below.

Product Name	Model Number	New FW Version
Nytro® 2032 SSD, 15mm, SAS Interface	XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	0001
Nytro® 3032 SSD, 15mm, SAS Interface	XS400ME70104 XS800ME70104 XS1600ME70104	0001

Product Name	Model Number	New FW Version
	XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104	

Code changes to the firmware were made to the validated TOE to support the new version. These changes included changes to comply with a customer request, to fix a bug for a hang condition, a logging reliability issue, and a drive hang condition. None of the changes were security relevant.

Description of ALC Changes:

Changes to the following documents were made, going from version 8.0 to 9.0:

- Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 9.0 Proprietary August 10, 2020
- Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 9.0 Public August 10, 2020
- Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 9.0 Dated: August 10, 2020
- 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 9.0 Dated: August 10, 2020

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR #8) for the 23 new hardware models listed above
- The IAR specifies that there are no security relevant firmware changes
- There are a relatively small number of changes to the validated TOE, and none of the changes impact the secure operation of the TOE. The assurance impact of these changes is minor. 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 3 weeks to complete. Regression testing was conducted for these firmware releases starting June 6, 2020 through June 15, 2020

Vulnerability Assessment:

Seagate searched the Internet for potential vulnerabilities in the TOE using the three web sites listed below.

- 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)

Seagate selected the 26 search key words based upon the vendor name, the product name, and key platform features the product leverages. The search terms used were:

- Seagate
- Seagate Secure TCG Opal SSC
- Seagate Secure TCG Enterprise SSC
- ARMv7
- ARM Cortex-R
- ARM Processor
- 800-90 DRBG 1.0 Firmware
- ARMv7 AES in Firmware
- ARMv7 AES Key Wrap in Firmware
- ARMv7 GCM in Firmware
- ARMv7 HMAC in Firmware
- ARMv7 RSA in Firmware
- ARMv7 SHS in Firmware
- Hash_Based DRBG 2.0 Firmware
- Balto
- Cheops
- Myna

- drive encryption
- disk encryption
- key destruction
- key sanitization
- self-encrypting drive
- sed
- opal
- enterprise ssc
- tcg ssc

The IAR contains the output from the vulnerability searches and the rationale why the search results are not applicable to the TOE. This search was performed on August 10, 2020. No vulnerabilities applicable to the TOE 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. The 'Description of Changes' section of the IAR further indicates that there are no security relevant firmware changes to the validated TOE.
>
> 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 hardware models and the new firmware version identified above. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.