CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Seagate Secure ® TCG SSC Self-Encrypting Drives (CPP FDE EE v2.0)

Maintenance Report Number: CCEVS-VR-VID10857-2019-2

Date of Activity: 15 July 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 Version 3.0, May 30, 2019

Seagate Secure ® TCG SSC SED Security Target Version 4.0, Proprietary May 30, 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 4.0 May 30, 2019

Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 4.0 May 30, 2019

Affected Evidence:

Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 4.0, Proprietary May 30, 2019

Updated Developer Evidence:

Seagate Secure ® TCG SSC SED Security Target version 4.0 Proprietary May 30, 2019

Assurance Continuity Maintenance Report:

Seagate Technology, LLC. submitted an Impact Analysis Report (IAR #3) to CCEVS for approval to update the code on twenty Common Criteria certified Seagate product models and to add fifteen new product models. The twenty modified models have seven new firmware versions based on existing Common Criteria certified versions. The IAR describes code changes the vendor specifies as security relevant; these primarily address intermittent drive hang issues. None of these changes impact the security functional requirements (SFR) against which the product was evaluated.

The ACMR 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, 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 1.0, February 2004.

In accordance with those requirements, the ACMR describes the changes made to the certified TOE, the evidence that was updated because of those changes, and the security impact of those changes.

Changes to TOE:

The TOE has been updated in the following ways.

There are five security relevant/non-SFR impacting firmware code changes involved fixing intermittent drive hang issues.

- The issue "Drive hang when issuing repeated TCG Send commands without retrieving status" occurred due to a missed state check in the TCG packet parser causing the drive to become unresponsive. (Change #6)
- The issue "Incorrect sense data return after invoke sanitize follow by power-cycle" occurred due to an omitted variable check after the sanitization had completed successfully that treated the completion state the same as 'sanitization in progress'. (Change #7)
- The issue "Avoid updating internal state of transaction" occurred due to an internal state of a transaction updating on every transaction, rather than only on successful transactions. (Change #9)
- The issue "Drive returns wrong sense data in response to Read Long command in secure drive" occurred due to a command status field not being appropriately flag-masked for read operations in all cases. (Change #19)
- The issue "Drive may hang while executing TCG Random method in parallel with I/O" occurred due to missing request and release calls to the media scheduler. (Change #32)

One firmware change fixed a TCG Spec violation due to reporting incorrect sense data.

- The issue "Command timeouts after doing I/O while SED Band locking status is changing" occurred due to a state check not being cleared when attempting to unlock a locked band. (Change #34)

The final firmware change fixed an intermittent issue where a sanitize operation caused a drive to fall into an unresponsive but secure state.

- The issue "Sanitize overwrite operation causes data abort and corrupt format" occurred due to a slight misalignment between two security-related subroutines' memory range permissions, which caused an intermittent drive hang waiting for memory access that could not be granted. (Change #46)

The security relevant firmware code changes are included in the following firmware versions (Summarized in the table just below):

- Issues #32, #34, and #46 are included in firmware versions 0001, 0002, A001, 0004, and 0005.
- Issues #6, #7, #9, and #19 are included in firmware versions CF04 and NF04.

Firmware Version	Based on Certified Version	#6	#7	#9	#19	#32	#34	#46
0001	7539					#32	#34	#46
0002	7539					#32	#34	#46
0004	7539					#32	#34	#46
0005	7539					#32	#34	#46
A001	7539					#32	#34	#46
CF04	CK10	#6	#7	#9	#19			
NF04	CKF1	#6	#7	#9	#19			

None of these security relevant changes impacted the underlying security architecture , affected the implementation of the SFRs, or rendered drives into an unsecure or vulnerable state.

Hardware – Model Updates

- The changed model numbers are XS1600ME10023, XS800ME10023, XS400ME10023, XS6400LE70023, XS1600LE10023, XS1920SE10123, XS3840TE10023, XS3200ME70023, XS15360SE70143 (formerly model number XS15360SE70123), XS7680TE70023, ST900MP0166, ST600MP0156, ST900MP0126, ST600MP0026, ST1000LM050, ST500LM035, ST1200MM0069, ST2400MM0149, ST1800MM0149, and ST1200MM0149.
- There are seven new versions of firmware based on existing Common Criteria certified versions. Firmware versions 0001, 0002, 0004, 0005, and A001 are based on the existing certified

firmware revision 7539; firmware version CF04 is based upon existing firmware revision CK10; and firmware version NF04 is based upon existing firmware revision CKF1.

- The new model numbers are XS800LE70024, XS1600LE70024, XS3200LE70024, XS6400LE70024, XS400ME70024, XS800ME70024, XS1600ME70024, XS3200ME70024, XS960SE70024, XS1920SE70024, XS3840SE70024, XS7680SE70024, XS3840TE70024, XS7680TE70024, and XS15360TE70024.
    - The hardware change is minor in scope to replace two types of NAND packages used on the ASIC with one type of NAND package and the accompanying pin differences between the packages.
- The updated Security Target, the Entropy Document, and the Key Management Description were only changed to incorporate the updated and new model numbers and to add the new firmware versions identified above.

Vendor Conclusion:

The IAR indicates that there are no changes to the development environment of the validated TOE. The IAR further indicates that there are a number of minor code changes to the product associated with the validated TOE. Of these, a small number are security relevant but do not affect the underlying security architecture.

Additionally, there is one hardware change associated with a set of new products be ing added to this certification. This hardware change is minor, encompasses only the replacement of one type of component with another from a different vendor, and therefore does not present a risk to the security architecture that would necessitate further testing.
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 incorporate the updated and new model numbers and to add the new firmware versions identified above. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.