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

Date of Activity: 1 March 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 2.1, February 8, 2019

Seagate Secure ® TCG SSC SED Security Target Version 3.0, Proprietary February 8, 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 3.0 February 8, 2019

Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 3.0 February 8, 2019

Affected Evidence:

Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 3.0, Proprietary February 8, 2019

Updated Developer Evidence:

Seagate Secure ® TCG SSC SED Security Target version 3.0 Proprietary February 8, 2019

Assurance Continuity Maintenance Report:

Seagate Technology, LLC. submitted an Assurance Continuity Maintenance Report (ACMR) to CCEVS for approval to add three new versions of firmware to Common Criteria certified Seagate product models ST500LM033, ST1000LM038, ST2000LM010, ST500LM035, and ST1000LM050.

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.

1. Three new versions of firmware have been added to Common Criteria certified Seagate product models ST500LM033, ST1000LM038, ST2000LM010, ST500LM035, and ST1000LM050. Each model number uses the same three new firmware revision numbers. The new firmware version numbers are RTE2, REE2, and RPE2; they are all based on the existing CC certified firmware revision SDM2.
2. There are a total 55 firmware code changes of which only three are security relevant minor fixes. All other fixes are not security relevant.
    a. The first security relevant fix is an update to response behavior due to a clarification in TCG specification.
    “Fix Sanitize Command Not Aborted Crypto Scramble EXT Command In SD4 State (SED Only)”
    Bug fix: In a particular scenario for the SD4 state (the sanitize operation succeeded state), the Sanitize Crypto Scramble EXT command was not being aborted gracefully. Does not affect underlying security architecture.
    b. The second security relevant fix is a customer requested change to an ATA security related default value. This change does not affect any non-customer specific configurations or underlying system architecture.
    c. The third security relevant fix is to fix an unreliable abort for a valid, authorized issued sanitize command.
    “Invalid Invoking ID - Get - expects NOT_AUTHORIZED instead of empty list”
    Change to replace return of empty list with return of NOT_AUTHORIZED error, as per updated Opal specification clarification. Does not affect any underlying security architecture.

3. The updated Security Target, the Entropy Document, and the Key Management Description were only changed to incorporate the new firmware versions, RTE2, REE2, and RPE2.

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 55 code changes to the product associated with the validated TOE. Of these, three are security relevant but do not affect the underlying security architecture. Based on this and other information from within this IAR document, the assurance impact of these changes is a clear maintenance action.

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 three new firmware versions, RTE2, REE2, and RPE2. Regression testing was successfully conducted for these three firmware releases starting January 9, 2019 and ending February 15, 2019. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.