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-VID10857-2020-4

Date of Activity: 21 December 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 #9 Version 1.0 November 25, 2020

Seagate Secure ® TCG SSC Self-Encrypting Drives Security Target Version 10.0, November 25, 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 10.0 November 25, 2020

Affected Evidence:

Seagate Secure ® TCG SSC Self-Encrypting Drives Security Target Version 10.0, November 25, 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 #9) to CCEVS for approval to add four firmware revision to four CC certified hardware versions as shown here:

- add EF03 based on firmware versions EF01 and EF02
- add NF03 based on firmware versions NF01 and NF02
- add TF03 based on firmware versions TF01 and TF02 and
- add SF03 based on firmware versions SF01 and SF02

The table below shows the model numbers and the new firmware version.

Changes to TOE:

In the updated ST, version 10, Tables 1 and 2 were updated to show the four new firmware versions.

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 firmware versions.

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

Product Name	Model Number	New FW *Version in Italics*
Exos™ 7E8, SAS Interface	ST4000NM014A ST8000NM010A ST6000NM033A	EF01, EF02, ***EF03***
Exos™ 7E8, SAS Interface	ST4000NM015A ST3000NM005A	NF01, NF02, ***NF03***
Exos™ 7E8, SATA Interface	ST3000NM004A ST4000NM013A	TF01, TF02, ***TF03***
Exos™ 16, SAS Interface	ST10000NM010G ST12000NM008G ST14000NM012G	SF01, SF02, ***SF03***

Code changes to the firmware were made to the validated TOE to support the new firmware versions. These changes were bug fix and performance improvements; in this case most of the changes were fixes for incorrect error/sense data reporting, log page errors, and drive hangs, and for performance optimization.

Section 2.3. “Assurance Impact Determination” of the IAR specifies that there are a 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 TSF interface, no hardware changes, no SFR changes, no new security features, no changes to assumptions and objectives, no changes that require updates to assurance evidence, and no new non-security

features. There are only non-security-relevant bug fixes and changes included in this firmware update. None of the changes were security relevant.

The IAR shows the FW Version(s) in Table 9, Validated TOE Product Code Changes. For each FW change, the FW Version(s) cell lists the FW releases that include the change. Many of the changes are included in all 4 releases. In other cases, the change is only relevant to SATA devices and in the remaining cases, the change is only relevant to SAS devices. As Table 9 indicates, none of the changes in this update are security relevant. All changes are to address non-security issues. For further detail, see table below.

#	Change Description	Security Relevant?	Comments	FW Version(s)
1	Performance drop in SAS Sequential Transfer	No	Performance optimization	EF03 NF03 SF03
2	SMART (Self-Monitoring, Analysis, and Reporting Technology) Attribute 10h counter incremented incorrectly, causing SMART trips	No	Fix for a SMART error	EF03 NF03 SF03
3	Drive Hang during SAS error injection testing	No	Fix for drive hang issue	EF03 NF03 SF03
4	Unexpected Mode Page value after firmware download	No	Fix for Mode Page error	EF03 NF03 SF03
5	In Drive Diagnostics (IDD) SAS BER Calculations Incorrect	No	Fix for log page error	EF03 NF03 SF03
6	Pin 11 Activity LED not functioning if pin 11 is pulled low at power on.	No	Update LED behavior to comply with revision 3.2 of the SATA specification	TF03
7	Drive not spin up on power up after PHY initialization is completed	No	Fix to address infrequent initialization issue	TF03
8	NCQ Command Timeouts in regression testing command never gets processed, causing a timeout	No	Fix for command (I/O) timeout	TF03
9	SATA: SanitizeAntifreezeLockExt Is incorrectly accepted when drive is depoping	No	Fix to address incorrect error/sense code data reporting	TF03
10	Assert while running read after incomplete normal ATA erase	No	Fix for drive hang (Assert)	TF03
11	Drive reports zero phy speed in Identify device data	No	Address Inquiry / Identify device error	TF03
12	Assert during Write Same command processing	No	Fix for drive hang (Assert)	EF03 NF03 SF03 TF03
13	Drive becomes unresponsive following Hard Reset during Write command workload	No	Fix for drive hang	EF03 NF03 SF03 TF03
14	Aligned Write Command Timeout Due to Dynamic WCD (Write Cache Disabled) Streaming	No	Fix for command (I/O) timeout	EF03 NF03 SF03 TF03
15	Flash led were reported during sequential write	No	Fix for drive hang (Assert)	EF03 NF03

#	Change Description	Security Relevant?	Comments	FW Version(s)
				SF03 TF03
16	Zero values on FARM (Field-Accessible Reliability Metrics) Log: RV (Rotational Vibration) Abs Mean, RV Max Abs Mean	No	Address system level error logging issue	EF03 NF03 SF03 TF03
17	Assert after DOS (Direct Offline Scan) rewrites the last user track	No	Fix for drive hang (Assert)	EF03 NF03 SF03 TF03
18	Assert seen during performance testing	No	Fix for drive hang (Assert)	EF03 NF03 SF03 TF03
19	Unrecoverable read errors seen post highly localized write intensive workload	No	Fix incorrect error/sense data reporting	EF03 NF03 SF03 TF03
20	Assert condition due to divide by zero calculation	No	Fix for drive hang (Assert)	EF03 NF03 SF03 TF03
21	After depop/repop, DOS (Direct Offline Scan) Ought/Need to Occurs Immediately	No	Fix for command (I/O) timeout	EF03 NF03 SF03 TF03
22	Get Element Status Encounters WFI (Wait for Interrupt) During Reman/Depopulation	No	Fix for command (I/O) timeout	EF03 NF03 SF03 TF03
23	Servo positional error information is invalid in the UDS (Unified Debug System)	No	Address system level error logging issue	EF03 NF03 SF03 TF03
24	Sanitize Portion of Depop Does Not Resume after Host Reset	No	Address a protocol violation	EF03 NF03 SF03 TF03
25	Improve robustness of H2SAT BIE (Bits in Error) measurements by adding conditional retries phase	No	Improve robustness of H2SAT measurements	EF03 NF03 SF03 TF03
26	Format failed with resident DST (Drive Self-Test) full	No	Fix to address incorrect error/sense code data reporting	EF03 NF03 SF03 TF03
27	Assert Encountered During WCD Sequential Write	No	Fix for drive hang (Assert)	EF03 NF03 SF03 TF03
28	Uncorrectable Errors in Write Intensive Workload	No	Fix to address incorrect error/sense code data reporting	EF03 NF03 SF03

#	Change Description	Security Relevant?	Comments	FW Version(s)
				TF03
29	Drive hang during recovery of a corrupted system file	No	Fix for drive hang issue	EF03 NF03 SF03 TF03
30	Run to Run Performance Variation in Random Write Workload	No	Performance optimization	EF03 NF03 SF03 TF03
31	Assert due to thread timing issue	No	Fix for drive hang (Assert)	EF03 NF03 SF03 TF03
32	Unexpected abort during read H2SAT log	No	Remove unnecessary drive readiness check	EF03 NF03 SF03 TF03
33	Incorrect collection of parity during RAW write recovery operations	No	Fix for drive hang (Assert)	EF03 NF03 SF03 TF03
34	0B/09/04/00 error reported by the drive after a power cycle	No	Fix to address infrequent initialization issue	EF03 NF03 SF03 TF03
35	Possible Assert during DST (Drive Self-Test)	No	Fix for drive hang (Assert)	EF03 NF03 SF03 TF03
36	Corrupted location not found by background parity scan in time	No	Address incorrect error/sense data reporting	EF03 NF03 SF03 TF03
37	Super Parity recovery fails if there is ALT (Accelerated Life Testing) at the last sector	No	Address incorrect error/sense data reporting	EF03 NF03 SF03 TF03
38	Bit Error Rate Calculation Missing Invalid Measurement	No	Address a log page error	EF03 NF03 SF03 TF03
39	DOS (Directed Off-Line Scan) logging: "Worst Need to scan counter" value can appear to be 0xFFFF	No	Address log page error	EF03 NF03 SF03 TF03
40	Assert encountered during Send Diagnostics command with Rebuild Assist	No	Fix for drive hang (Assert)	EF03 NF03 SF03 TF03
41	Update the RW progress to match the Super Parity RAM progress	No	Address issue with reporting incorrect error/sense data	EF03 NF03 SF03 TF03

Description of ALC Changes:

Changes to the following documents were made, going from version 9.0 to 10.0:

- Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 10.0, November 25, 2020
- Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 10.0 Dated: November 25, 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 10.0 Dated: November 25, 2020

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR #8) to add the four new firmware versions 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 12, 2020 through June 22, 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 22 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 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
- Myna
- drive encryption
- disk encryption
- key destruction
- key sanitization
- self-encrypting drive
- sed
- 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 November 23, 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.