CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

ASSURE-Stor™ Solid State Self-Encrypting Drive

Hardware Revision 3.0

Firmware Revision 1.5.1

Maintenance Report Number: CCEVS-VR-VID11041-2022

Date of Activity: 28 February 2022

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

Security Target for ASURRE-Stor™ Solid State Self-Encrypting Drive Version June 6, 2020

Impact Analysis Report for ASURRE-Stor™ Solid State Self-Encrypting Drive, February 25, 2022

Affected Evidence:

None.

Documentation Updated:

There were no changes to the documentation from the original evaluation.

Assurance Continuity Maintenance Report:

Mercury Systems, Inc. submitted an Impact Analysis Report (IAR) and Assurance Continuity package to CCEVS for approval in February 2022. The IAR is intended to satisfy the requirements outlined in

Common Criteria Evaluation and Validation Scheme Publication #6 referenced above. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The purpose of this Assurance Continuity action is to extend the date of the certification beyond the previous expiration date of March 6, 2022. There were no changes to the TOE and hence also no changes to the associated documentation.

Changes to TOE:

There were no changes to the TOE.

Description of Regression Testing:

There was no regression testing performed since there were no changes made to the product.

Vulnerability Assessment:

Mercury Systems 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)

Mercury selected a subset of the key words that were used in the vulnerability search for the original product evaluation. The search terms used were:

- Mercury Systems (formerly Microsemi)
- Asurre-Stor
- Arria II GX
- Drive Encryption, Disk Encryption
- Key Destruction, Key Sanitization
- Self-Encrypting Drive (SED)
- OPAL
- Key caching

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 February 26, 2022. 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 changes to the validated TOE.

Based on this and other information from within this IAR document, the vendor concluded that the assurance impact of these changes is minor.

Validation Team Conclusion:

The validation team reviewed the changes and concurs that the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The Security Target was not changed since there were no changes to the product. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.