CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Curtiss-Wright Defense Solutions Compact Network Storage 4-Slot Software Encryption Layer (FDEEEcPP20E/FDEAAcPP20E)

Maintenance Report Number: CCEVS-VR-VID10968-2021

Date of Activity: 26 January 2021

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

collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201

collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0 + Errata 20190201

Impact Analysis Report for Curtiss-Wright Defense Solutions Compact Network Storage 4-Slot Software Encryption Layer Revision 1.0 January 14, 2021

Curtiss-Wright Defense Solutions Compact Network Storage 4-Slot Software Encryption Layer (FDEEEcPP20E/FDEAAcPP20E) Security Target Version 0.5 April 15, 2019

Curtiss-Wright CNS4 CSfC Common Airborne Recorder CSfC Encrypted Data Storage User Guide Part Number: DDOC0108-000-A2 Revision A2 March 20, 2019

Affected Evidence:

Curtiss-Wright Defense Solutions Compact Network Storage 4-Slot Software Encryption Layer (FDEEEcPP20E/FDEAAcPP20E) Security Target Version 0.5 April 15, 2019

Updated Developer Evidence:

There have been no changes to the product and no changes to the development environment.

Description of ASE Changes:

There have been no changes to the product and no changes to the development environment.

Changes to TOE:

There have been no changes to the product and no changes to the development environment.

Assurance Continuity Maintenance Report:

Gossamer submitted an Impact Analysis Report (IAR) on behalf of Curtiss-Wright Defense Solutions that updates the vulnerability search. There are no changes to the product or to the development environment.

Description of Regression Testing:

Given that there were no changes to the product or development environment, no regression testing was noted in the IAR.

Vulnerability Assessment:

Gossamer searched the Internet for potential vulnerabilities in the TOE using the two web sites listed below.

- National Vulnerability Database (NVD, https://nvd.nist.gov/)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)

Gossamer selected the 16 search key words based upon the vendor name, the product name, and key platform features the product leverages. The search terms used were:

- disk encryption
- drive encryption
- key destruction
- key sanitization
- Opal management software
- SED management software

- Password caching
- Key caching
- Curtiss Wright
- CNS4
- Compact Network Storage 4-Slot
- Linux Unified Key Setup
- LUKS
- Libgcrypt
- Openssl
- CentOS

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 January 14, 2021. 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 product and no changes to the development environment of the validated TOE.

The TOE has not been changed nor has the Full Disk Encryption PPs changed. The IAR only updates the public search for vulnerabilities.

Note that Curtiss Wright Defense Systems continually tracks bugs, vulnerabilities, and other defects reported in the public domain and at the time of this report there are no known outstanding security-related vulnerabilities in the 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. Neither the Security Target nor the Common Criteria Guide were changed. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.