CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Software Encryption Layer v1.03.00

Maintenance Report Number: CCEVS-VR-VID11438-2025

Date of Activity: April 29, 2025

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." 29 August 2014.

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 ((FDEEEcPP20E)

collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019 (FDEAAcPP20E)

Impact Analysis Report for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Software Encryption Layer v1.03.00, version 1.1, April 29, 2025

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Software Encryption Layer v1.03.00 Security Target, version 0.5, April 29, 2025

Assurance Continuity Maintenance Report:

Gossamer Security Solutions submitted an Impact Analysis Report (IAR), on behalf of Curtiss-Wright, for the changes from the certified TOE, Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Software Encryption Layer v1.02.00 to Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Software Encryption Layer v1.03.00. This was accomplished per the requirements of the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on March 17, 2025. The IAR is intended to

satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Reevaluation, version 3.0. 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 evaluation evidence submitted for consideration consists of the Security Target (ST), the User Guide DDOC0199-000-NIAP, and the Impact Analysis Report (IAR).

RHEL 8.10 has been added as a new underlying Linux version to the TOE and the TOE software has been updated from version 1.02.00 to version 1.03.00. See Changes to TOE section for more details. As a result, the following changes were made to the evaluation evidence:

1. Security Target – The Security Target has been updated to identify the new underlying Linux version addition. It has also been updated to identify the new User Guide.
2. Guidance Document -- User Guide (DDOC0199-000-NIAP) was updated to add a reference to RHEL.

Documentation Updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Software Encryption Layer version 1.02.00 Security Target, Version 0.4, August 19, 2024	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Software Encryption Layer v1.03.00 Security Target, Version 0.5, April 29, 2025 Updated to identify the new underlying Linux version addition and one updated User Guide
Design Documentation: See Security Target and Guidance	No changes required
Guidance Documentation: 1. Curtiss-Wright DTS1+ CSfC 1-Slot Data Transport System (CSfC) User Guide, DDOC0199-000-NIAP 2. Curtiss-Wright DTS1X CSfC 1-Slot Data Transport System 10GbE CSfC User Guide, DDOC0221-000-NIAP **3.** Curtiss-Wright DTS1X-T 1-Slot Data Transport System 10GbE CSfC – Tethered User Guide, DDOC0252-000-NIAP	The first User Guide (DDOC0199-000-NIAP) was updated to add a reference to RHEL
Lifecycle: NONE	No changes required
Testing: NONE	See also Description of Regression Testing section.

	Curtiss Wright performs regression testing on each product version. This includes low level testing designed to address any CC related issues. Each SW release has to go through a series of tests which Curtiss Wright terms ATP or Acceptance Test Procedure which tests all supported capability/features (NAS, PXE, iSCSI, PCAP, etc.) and operations, utilizing both encryption layers: HWFDE and SWFDE, to ensure that they maintain the integrity of the product. In other words, Curtiss Wright wants to ensure that any given release complies with customer expectation and does not break the existing functionality. It is also tested to ensure that developers are not introducing new bugs with each release.
Vulnerability Assessment: NONE	The public search was updated on April28, 2025. No new public vulnerabilities were discovered that are applicable to the TOE. See analysis of results below. Note the term Linux 8.10 was added to address the new underlying Linux. The terms Rocky and RHEL were also added.

Changes to TOE:

The change to the TOE was to add support for RHEL 8.10 in addition to the evaluated configuration with Rocky Linux 8.8. No SFRs are directly impacted by this change as the exact same software runs on RHEL as runs on Rocky Linux. Rocky Linux is binary and bug-for-bug compatible with RHEL. This change has no security impact.

The CAVP certificates are still valid as the tested model is listed on the certificate and the RHEL addition simply adds an equivalent software environment. The Crypto libraries used in the RHEL version are identical to the libraries used in Rocky Linux (kernel 4.18.0, OpenSSL 1.1.1, and libgcrypt 1.8.5). To support the claim that the crypto libraries are the same, the IAR details the checking that the vendor performed on OpenSSL 1.1.1, and libgcrypt 1.8.5, and notes the kernels are the same so that one algorithm is the same.

Description of Regression Testing:

Curtiss Wright performs regression testing on each product version. This includes low level testing designed to address any CC related issues.

Each SW release has to go through a series of tests which Curtiss Wright terms ATP or Acceptance Test Procedure which tests all supported capability/features (NAS, PXE, iSCSI, PCAP, etc.) and operations, utilizing both encryption layers: HWFDE and SWFDE, to ensure that they maintain the integrity of the

product. In other words, Curtiss Wright wants to ensure that any given release complies with customer expectation and does not break the existing functionality. It is also tested to ensure that developers are not introducing new bugs with each release.

NIST CAVP Certificates

The CAVP certificates are still valid as the tested model is listed on the certificate and the RHEL addition simply adds an equivalent software environment. The Crypto libraries used in the RHEL version are identical to the libraries used in Rocky Linux (kernel 4.18.0, OpenSSL 1.1.1, and libgcrypt 1.8.5).

Vulnerability Assessment:

The IAR contains the output from the vulnerability search updated on 4/28/2025, as well as the rationale why the vulnerabilities identified in the search results are not applicable to the TOE.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), and the Vulnerability Notes Database (http://www.kb.cert.org/vuls/, using the following search terms.

- "disk encryption "
- "driver encryption "
- "key destruction "
- "key sanitization "
- "Opal management software "
- "SED management software "
- "Password caching "
- "Key caching "
- "Curtiss Wright DTS1-Slot Plus Data Transport System "
- "Linux Unified Key Setup "
- "LUKS "
- "Libgcrypt "
- "openssl "
- "Linux 8.8 "
- "kernel cryptography"
- "dts1"
- "Linux 8.8 "
- "Linux 8.10"
- "RHEL"
- "Rocky".

The vulnerability search returned 38 results. The results of the vulnerability assessment were included in the IAR. No new vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

There have been minor product changes to include a new underlying version of Linux. The evaluated version of the TOE runs on the new addition. The ST has been updated to reflect the added Linux version and reference the one updated User Guide.

Note that Curtiss Wright 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.

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 TOE has been updated from version 1.02.00 to 1.03.00 to include a new underlying version of Linux. This update to add support for RHEL 8.10, in addition to Rocky Linux 8.8, isn't a significant operating system change. The kernels and crypto libraries are identical. Therefore this change can be considered minor and is not security relevant. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.