ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.1.0

Maintenance Update of Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.2.0 to 1.3.0

Maintenance Report Number: CCEVS-VR-VID11437-2026

Date of Activity: April 24, 2026

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 Letter #12 "Acceptance Requirements of a product for NIAP Evaluation." 10 February 2025.

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

Impact Analysis Report for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.1.0, Revision 1.4, 20-Apr-2026

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.3.0 Security Target, Version 0.6, December 31, 2025

Assurance Continuity Maintenance Report:

Gossamer Security Solutions submitted an Impact Analysis Report (IAR) for the changes from the certified TOE, Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.2.0 to Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.3.0, to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on December 31, 2025. Addressing some of the comments from the validation team, an updated version of the IAR was submitted on April 20, 2026. 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, any 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) and the Impact Analysis Report (IAR).

The TOE software has been updated from version 1.2.0 to version 1.3.0. See Changes to TOE section for more details. As a result, the following changes were made to the evaluation evidence:

Security Target – The Security Target has been updated to identify the new product version number. No other changes were necessary to the Security Target.

Documentation Updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.2.0 Security Target, Version 0.5, August 19, 2024	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.3.0 Security Target, Version 0.6, December 31, 2025 Updated to identify the new product version number.
Design Documentation: See Security Target and Guidance	No changes required.
Guidance Documentation: • Curtiss-Wright DTS1+ CSfC 1-Slot Data Transport System (CSfC) User Guide, DDOC0199-000-NIAP • Curtiss-Wright DTS1X CSfC 1-Slot Data Transport System 10GbE CSfC User Guide, DDOC0221-000-NIAP • Curtiss-Wright DTS1X-T 1-Slot Data Transport System 10GbE CSfC – Tethered User Guide, DDOC0252-000-NIAP	No changes required.
Lifecycle: None	No changes required
Testing: None	See Description of Regression Testing section.
Vulnerability Assessment: None	The public search was updated from 8/19/2024. No new public vulnerabilities were discovered that are applicable to the TOE. See below for results. Added the KEV database to address new NIAP requirements

Changes to TOE:

The changes to the TOE are divided into two categories: hardware and software.

Hardware Changes

There are no changes to Hardware

Software Changes

The TOE software has been updated from version 1.2.0 to version 1.3.0. This update includes two bug fixes to security relevant features, and one bug fix for a non-security relevant feature related to usability that is outside of scope of the TOE.

Description of Regression Testing:

The CCTL reported that Curtiss Wright performs regression testing on each product version. That includes low level testing designed to address any CC related issues. Each CC requirement is verified to ensure that the product still meets the requirements.

Each SW release has to go through a series of tests that 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. Furthermore, drives encrypted with the predecessor are decrypted with the current release (and vice-versa) to ensure encryption compatibility between releases. The vendor, thus ensures 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.

Equivalency:

Processor, components, circuitry, entropy source, software, and firmware are identical between the different variants; the crypto boundary is unchanged, and the identified software bug fixes have been verified to not impact any of the claimed SFRs. Products originally evaluated are running on all TOE variants.

NIST CAVP Certificates:

The CAVP certificate to SFR mappings in Table 4 of the ST are unchanged and remain valid in version 1.3.0 of Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer TOE.

Vulnerability Assessment:

The evaluator searched the MITRE CVE Database, National Vulnerability Database, and CVE details (https://www.cve.org/, https://web.nvd.nist.gov/vuln/search, and https://www.cvedetails.com/vulnerability-search.php, ref CVE) and Known Vulnerability Exploit Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog, ref KEV), Vulnerability Notes Database

(http://www.kb.cert.org/vuls/, ref VND) on 4/8/2026 (from 8/1/2024) with the following search terms: "Disk&encryption", "Drive&encryption", "Key&destruction", "Key&sanitization", "Opal&management&software", "SED&management&software", "Password&caching", "Key&caching", "Curtiss&Wright", "DTS1-Slot&Plus", "Defense&Solutions&Data&Transport&System", "Curtiss&Wright&Crypto&Firmware", "ARM7&Processor", "P/N&LPC4367JET100E", "Cyprus&FM24V05", "ATECC608B", "Enova&X-Wall MX+", "Linux&8.8", "AES&XTS", and "DTS1".

A total of 76 vulnerabilities were identified. Of all the sources searched, the following terms identified matches: Linux&8.8, Key&destruction, AES&XTS, Key&sanitization, Disk&encryption, Drive&encryption, Key&caching, Password&caching. The breakdown of individual matches is as follows:

- 20 CVE matches (4 not applicable, 16 issue mitigated) for: Linux&8.8.
- 2 CVE matches (2 issue mitigated) for: Key&destruction.
- 1 CVE matches (1 issue mitigated) for: AES&XTS.
- 32 CVE matches (32 not applicable) for: Key&sanitization.
- 9 CVE matches (9 not applicable) for: Disk&encryption.
- 2 CVE matches (2 not applicable) for: Drive&encryption.
- 8 CVE matches (8 not applicable) for: Key&caching.
- 2 CVE matches (2 not applicable) for: Password&caching

All of these vulnerabilities are either resolved or deemed not applicable by the CCTL.

Vendor Conclusion:

There have been two **minor** product changes to address evaluated functionality that improved product usability by eliminating failed updates and corrected the advertised password length limits.

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 the analysis of the impact upon security, 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 1.2.0 to 1.3.0 to address minor usability issues that do not change related security functionality of the TOE. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.