
**CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT**

**ASSURANCE CONTINUITY MAINTENANCE REPORT FOR**

---

**Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.2.0**

**Maintenance Report Number:** CCEVS-VR-VID11437-2024

**Date of Activity:** October 15, 2024

**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

Impact Analysis Report for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.1.0, version 1.1, October 15, 2024

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.2.0 Security Target, version 0.5, August 18, 2024

**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 1.1.0 to Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.2.0, to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on August 23, 2024. 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 Administrator's Guide (AGD), and the Impact Analysis Report (IAR).

Two additional TOE hardware models/variants of the same product have been added to the TOE (DTS1X and DTS1X-T) and the TOE software has been updated from version 1.1.0 to version 1.2.0. 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 product variants and version number as well as adding references to the new AGDs. No other changes were necessary to the Security Target.
2. Guidance document – The User Guide has been expanded to include a document for each variant of the TOE. The documents are similar except for the hardware descriptions.

**Documentation Updated:**

| Original CC Evaluation Evidence | Evidence Change Summary |
|---|---|
| **Security Target:**<br>Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer version 1.0 Security Target, Version 0.4, April 12, 2024 | 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<br><br>Updated to identify the new product variants and version number. |
| **Design Documentation:**<br>See Security Target and Guidance | No changes required. |
| **Guidance Documentation:**<br>Curtiss-Wright DTS1+ CSfC 1-Slot Data Transport System (CSfC) User Guide, DDOC0199-000-A9 | 1. Curtiss-Wright DTS1+ CSfC 1-Slot Data Transport System (CSfC) User Guide, DDOC0199-000-NIAP<br>2. Curtiss-Wright DTS1X CSfC 1-Slot Data Transport System 10GbE CSfC User Guide, DDOC0221-000-NIAP<br>3. Curtiss-Wright DTS1X-T 1-Slot Data Transport System 10GbE CSfC - Tethered User Guide, DDOC0252-000-NIAP<br><br>Updated so there is one guidance document per product variant.<br><br>The evaluated DTS1+ User Guide has been updated to add section 5.2 HWFDE Layer Definitions – it defines some terms used in Section 5. |

| | |
|---|---|
| | The evaluated AGD Section B, Migration, has been removed from the end of the DTS1X and DTS1X-T User Guides since these are new models.<br><br>The evaluated AGD section 1.4, CE Conformity, has been removed from the DTS1X and DTS1X-T User Guides because these devices do not need European certifications.<br><br>Lastly, there are minor differences between the evaluated DTS1+ AGD and the added DTS1X and DTS1X-T User Guides related to hardware. The connectors replaced would be the HyperTronic connector identified above in the evaluated TOE and evolved to support the higher bandwidth and tethered design. The secondary Ethernet was also changed to support 10GbE. Both connector changes are outside the crypto boundary and has no security implication.<br><br>Between the AGDs, the differences would be seen in the Connectors/Cables section. J1 (Power) and J2 (Utility) cables are identical. J3 for the DTS1+ is for 1GbE operation, DTS1X and DTS1X-T uses connector/cable for 10GbE operation. There is also a D-MAG Connector for the DTS1X-T in the Connectors/Cables section. |
| **Lifecycle:**<br>NONE | No changes required |
| **Testing:**<br>NONE | See Description of Regression Testing section. |
| **Vulnerability Assessment:**<br>NONE | The public search was updated on October 15, 2024. No new public vulnerabilities were discovered that are applicable to the TOE. See analysis of results below. |

**Changes to TOE:**

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

**Hardware Changes**

Two additional TOE hardware models/variants of the same product have been added (DTS1X and DTS1X-T). The difference between the original product (DTS1+) and its variants are as follows:

DTS1X – 1x1GbE and 1x10GbE instead of 2x1GbE interface and removable storage connector type is changed to support higher SATA III speeds. The connector was changed from HyperTronics PN: KA17/127BEFB21TAH to Amphenol PN: HSB-D 4-05DM022X high density connector to support the higher frequency signals. The former was used for the evaluated TOE. The connector in question is between the ciphertext side of the inline SATA encryptor and storage cartridge. However, these connectors are outside the crypto boundary and data is already encrypted through both layers before getting to this point. Hence it is non-security relevant.

DTS1X-T -- 1x1GbE and 1x10GbE instead of 2x1GbE interface, 2x eNova encryptor instead of 1 to support a 2nd storage, and RMC replaced with eSATA drivers to support external tethered application. Tethered design and connectors are outside the crypto boundary. There are no security relevant changes. The tethered device is externally powered however data going in and out of the tethered storage are already encrypted.

**Software Changes**

The TOE software has been updated from version 1.1.0 to version 1.2.0. This update includes 1 bug fix for a non-security relevant feature related to usability that is outside of scope of the TOE.

**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 must 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.

**Equivalency:**

Processor, components, circuitry, entropy source, software, and firmware are identical between the different variants, with the exception of the components identified in the Changes to TOE section above, but the crypto boundary is unchanged, and the differences identified do not impact any of the claimed SFRs.

Products originally evaluated are already running on all variants.

**NIST CAVP Certificates:**

The new variants do not impact the CAVP certificates – the same certificates from the evaluated TOE apply to all additional variants. The CAVP certificate to SFR mappings in Table 4 of the ST are unchanged

and remain valid in version 1.2.0 of Curtiss-Wright Defense Solutions Data Transport System 1-Slot Plus Hardware Encryption Layer TOE.

**Vulnerability Assessment**:

The IAR contains the output from the vulnerability searches since the time of the original evaluation search (4/23/2024) to 10/15/2024, as well as the rationale why the vulnerabilities identified in the search results are not applicable to the TOE.

The same vulnerability databases and search terms listed in the assurance activities were used with one exception. The term “DTS1” was added to address all new models/variants.:

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

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"
- "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"
- "DTS1"

The vulnerability search returned 5 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 address a non-evaluated functionality and to add additional models. The ST has been updated to reflect the new models and version. The Guidance document was updated to include a separate document for each model.

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 1.1.0 to 1.2.0 to address a minor usability issue that is not related to security functionality and outside the scope of the TOE. This assurance maintenance also adds two additional TOE models, DTS1X and DTS1X-T, that vary only in minor hardware differences that are not security relevant. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.