**CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT**

**ASSURANCE CONTINUITY MAINTENANCE REPORT FOR**

---

**Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer**

(CPP_FDE_AA_V2.OE, CPP_FDE_EE_V2.OE)

**Maintenance Report Number:** CCEVS-VR-VID11097-2022

**Date of Activity:** March 29, 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." 29 August 2014.

Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019 (cpp_fde_aa_v2.0e)

Collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (cpp_fde_ee_v2.0e)

Impact Analysis Report for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer version 3.0.1 (IAR), Version 1.3, March 29, 2022

Common Criteria Evaluation and Validation Scheme Validation Report Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer, Version 0.3, September 02, 2020

**Affected Evidence:**

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer version 3.0.1 (FDEEEcPP20E/FDEAAcPP20E) Security Target, Version 1.2, August 13, 2020

- Updated to: Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer version 3.0.3 (FDEEEcPP20E/FDEAAcPP20E) Security Target, Version 1.3, February 25, 2022

Curtiss-Wright DTS1 Data Transport System (Network File System) User Guide, DDOC0099-000-AH

- Updated to: Curtiss-Wright DTS1 Data Transport System (Network File System) User Guide, DDOC0099-000-AT

**Development Environment Changes:**

No development environment changes occurred that impacted the product.

**Assurance Continuity Maintenance Report:**

Gossamer Security Solutions, CCTL, on behalf of Curtiss-Wright Defense Solutions, submitted an Impact Analysis Report to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 29 March, 2022. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3, September 12, 2016. In accordance with those requirements, the IAR describes the changes made to the certified Target of Evaluation (TOE), the evidence that was updated as a result of those changes, and the security impact of those changes.

**Introduction:**

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer (hereafter referred to as the TOE) was evaluated by Gossamer Security Solutions on August 13, 2020. The product met the requirements specified by the NIAP approved protection profiles for CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E.

The purpose of this document is to summarize and represent CCEVS' analysis and findings regarding Assurance Maintenance Continuity as minor product changes to add extra error/bounds checking were incorporated.

**Summary Description:**

The Security Target (ST) has been updated to reflect the new software versions. The Guidance Documentation has been updated with editing corrections and clarifications. There was no change to Design Documentation. Curtiss Wright performed regression testing on each product version. This includes low level testing designed to address any CC related issues. A new vulnerability scan was also

performed on 2/24/2022, where no new public vulnerabilities were discovered that are applicable to the TOE.

**Changes to TOE:**

The following table presents the changes incorporated into the TOE For each change, a description is provided and an analysis as to why it is not a major change.

| Change Description | Security Analysis |
|---|---|
| Fix to prevent accidental cmkey –zpsk operation (requires crypto firmware version 5.2 or later) | Added extra error checking to the interaction between the layers. There exists a checksum of the payload being sent from the S/W layer to the H/W layer. In previous versions, the command byte was not being included in this calculation. If a bit error occurred on the I2C bus, then instead of one command (updating the sensors) it would then perform a zeroize PSK command. This is an added function and no SFRs are directly impacted by this change. |
| Fix error reporting in cmkey and cmlogin | This is an error reporting clarification issue and not directly related to any claimed SFR. |
| Add the cmlog command | Auditing is not an evaluated function |
| Fix for rmcctl –wipe to be allowed when boot flash is write protected | This is a bug fix where the customer couldn't wipe the RMC configuration if the write protect switch was enabled. For example, if the customer configured the RMC with 4 partitions and wanted to re-configure the RMC with 2 partitions, they would need to run the `--wipe` command first to change from 4 to 2 partitions. The customer could always wipe the drive but this allows more flexibility. |
| Fix sens -p issues | The sens command is health test related. This fixes a display error and no SFRs are directly impacted by this change. |
| Fix rmcpurge issue where missing functions were reported when purging an actively mounted software image | This is an error reporting issue and not directly related to any claimed SFR. |
| Update iSCSI feature to support iSCSI target exports of SW Encrypted drives and SW Encrypted partitions | Fixed software bug in iSCSI export routine not directly related to any claimed SFR. |
| Fix cmkey issues where the HMAC wasn't being written to RMC with the --force option | This is just a change to the command line interface options. The documented and evaluated process works as described. Additional options have been added. |
| Fix cmkey key loaded status | This is a status reporting clarification issue and not directly related to any claimed SFR |

| | |
|---|---|
| Fix issue with nfsctl | Fixed software bug related to nfsctl CLI arguments not directly related to any claimed SFR |

These changes were software bug fixes, addition of error/bound checking and reporting, and changes to command line interface options. No SFRs are directly impacted by an added function, added flexibility, or software bug fixes.

**Affected Developer Evidence:**

| CC Evidence | Evidence Change Summary |
|---|---|
| Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer (FDEEEcPP20/FDEAAcPP20) Security Target, version 1.2, 08/13/2020 | Updated to identify the new software versions |
| **Design Documentation:**<br>See Security Target and Guidance | No changes required |
| **Guidance Documentation:**<br>Curtiss-Wright DTS1 Data Transport System (Network File System) User Guide, DDOC0099-000-AH | No changes required but updated with editing corrections/clarifications |
| **Lifecycle:**<br>None | No changes required. |
| **Testing:**<br>None | Curtiss Wright performs regression testing on each product version. This includes low level testing designed to address any CC related issues. |
| **Vulnerability Assessment:**<br>None | The public search was updated from 8/13/2020. No new public vulnerabilities were discovered that are applicable to the TOE. |

**Description of Regression Testing:**

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**:

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

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

The CCTL selected the 17 search key words. 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
- Defense Solutions Data Transport System
- Linux Unified Key Setup
- LUKS
- Libgcrypt
- Openssl
- CentOS
- kernel cryptography

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 March 29, 2022. No vulnerabilities applicable to the TOE were found.

**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 Security Target has been updated to identify the new product version. Editorial changes were made to the Guidance document. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.