ASSURANCE CONTINUITY MAINTENANCE REPORT for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer

---

Maintenance Update for: Data Transport System 1-Slot Hardware Encryption Layer

Maintenance Report Number: CCEVS-VR-VID10861-2019

Date of Activity: 2 May 2019

References:

- Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3, September 12, 2016
- Impact Analysis Report for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer (IAR), Version 1.2, May 2, 2019
- Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0, September 9, 2016 (FDE AA cPP 2.0)
- Collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0, September 9, 2016 (FDE EE cPP 2.0)
- Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019 (FDE AA cPP 2.0E)
- Collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (FDE EE cPP 2.0E)
- Validation Report for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer, Report Number CCEVS-VR-10861-2018, dated October 19, 2018, Version 0.3

Documentation report as being updated:

- Security Target – Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer (FDEEEcPP20/FDEAAcPP20) Security Target, Version 0.6, October 18, 2018. Updated to: Curtiss-Wright Defense Solutions Data Transport System

1-Slot Hardware Encryption Layer (FDEEEcPP20/FDEAAcPP20) Security Target, Version 0.8, May 2, 2019

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 22 April. 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:

The Curtiss-Wright Defense Solutions Data Transport System 1-Slot (DTS1) Hardware Encryption Layer (hereafter referred to as the TOE) was evaluated by Gossamer Security Solutions on October 18, 2018. The product met the requirements specified by the NIAP-approved protection profiles for FDE AA cPP 2.0 and FDE EE cPP 2.0. The validation team also performed evaluations of FDE AA cPP 2.0 and FDE EE cPP 2.0 concurrent with the product evaluation. The initial results by the validation team identified deficiencies in the cPPs, which were resolved in FDE AA cPP 2.0E and FDE EE cPP 2.0E.

The purpose of this document is to summarize and represent CCEVS' analysis and findings regarding Assurance Maintenance Continuity as the CC documentation has been updated.

Summary Description:

The conformance claim has been upgraded from FDE AA cPP 2.0 and FDE EE cPP 2.0 to FDE AA cPP 2.0E and FDE EE cPP 2.0E. The Security Target (ST) has been updated to reflect the new conformance claim, incorporate corrections made in FDE AA cPP 2.0E and FDE EE cPP 2.0E, and update the applicable technical decisions. A new vulnerability scan was also performed.

Changes to TOE:

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

The FDE AA cPP 2.0 was updated to FDE AA cPP 2.0E to account for changes to correct deficiencies identified in the initial validation of the cPPs in conjunction with the TOE evaluation, and incorporate all Technical Decisions. The Full Drive Encryption international Technical Community (FDE iTC) determined the impact of the changes to FDE AA cPP 2.0E

were minor. The majority of the changes were typographical errors related to the conventions for indicating assignments and selections and there was one dependency SFR missing.

FDE AA cPP 2.0E added FMT_SMR.1: Security Roles, a previously missing dependency for FMT_MOF.1: Management of Functions Behavior and FMT_SMF.1: Specification of Management Functions. FMT_SMR.1 adds the requirement that the TOE Security Functionality (TSF) maintains roles for authorized users and be able to associate users with roles. The TOE already had this capability, as necessitated by FMT_MOF.1 and FMT_SMF.1. No additional evaluation activities for FMT_SMR.1 were added, as they were already covered in evaluation activities for FMT_MOF.1 and FMT_SMF.1. Therefore, no changes were required to the product.

The FDE EE cPP 2.0 was updated to FDE EE cPP2.0E The FDE iTC determined the impact of the changes to FDE EE cPP 2.0 E were typographical errors related to the conventions for indicating assignments and selections and did not impact the security functionality of the PP.

Only two technical decisions incorporated into FDE AA cPP 2.0E and FDE EE cPP2.0E were published after the initial evaluation, TD0383 and TD0384. TD0383 is not applicable to this evaluation. TD0384 was the result of a TRRT submitted by this evaluation and its change was already incorporated prior to its publication, as documented in the Validation Report. Therefore, no changes were required to the product.

The corrections to typographical errors were all incorporated into the ST and did not require any changes to the product.

Affected Developer Evidence:

CC Evidence	Evidence Change Summary
Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer (FDEEEcPP20/FDEAAcPP20) Security Target, Version 0.6, October 18, 2018	Updated to reflect the new conformance claim, incorporate typographical error corrections, add an SFR dependency, and update the applicable technical decisions.

Regression Testing:

No regression testing was performed as no changes to the product were required.

Vulnerability Analysis:

A search of national sites was conducted for vulnerabilities related to the TOE. The public search was updated on April 22, 2019. No public vulnerabilities exist in the product.

Conclusion:

CCEVS reviewed the documentation changes and concur the changes are minor and that certificate maintenance is the correct path for assurance continuity as defined in NIAP Publication #6. In addition, the evaluator reported having conducted an updated vulnerability search that located no new applicable vulnerabilities requiring mitigation. Therefore, CCEVS agrees that the original assurance is maintained for the product.