CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer (FDEEEcPP20E/FDEAAcPP20E)

Maintenance Report Number: CCEVS-VR-VID11096-2022

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." August 29, 2014

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

collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0 + Errata 20190201

collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0 + Errata 20190201

Impact Analysis Report for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer Revision 1.3 March 29, 2022

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer version 5.3 (FDEEEcPP20E/FDEAAcPP20E) Security Target (Public) Version 1.3 February 25, 2022

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer version 5.3 (FDEEEcPP20E/FDEAAcPP20E) Security Target (Proprietary) Version 1.3 February 25, 2022

Curtiss-Wright DTS1 CSfC 1-Slot Data Transport System (CSfC) User Guide Part Number: DDOC0099-000-AT Revision AT March 02, 2022

Affected Evidence:

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer version 5.3 (FDEEEcPP20E/FDEAAcPP20E) Security Target (Public) Version 1.3 February 25, 2022

Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer version 5.3 (FDEEEcPP20E/FDEAAcPP20E) Security Target (Proprietary) Version 1.3 February 25, 2022

Curtiss-Wright DTS1 CSfC 1-Slot Data Transport System (CSfC) User Guide Part Number: DDOC0099-000-AT Revision AT March 02, 2022

Updated Developer Evidence:

Code changes included minor bugfixes and extra bounds checking and thus did not have any impact on the developer evidence of the validated TOE. See table below for details.

CC Evidence	Evidence Change Summary
Curtiss-Wright Defense Solutions Data Transport System 1-Slot Hardware Encryption Layer version 5.1 (FDEEEcPP20/FDEAAcPP20) Security Target, version 1.2, 08/13/2020	Updated to identify the new product versions
Design Documentation: See Security Target and Guidance	No changes required
Guidance Documentation: Curtiss-Wright DTS1 Data Transport System (Network File System) User Guide, DDOC0099-000-AH	No changes required but updated with editing corrections/clarifications
Lifecycle: None	No changes required.
Testing: None	Curtiss Wright performs regression testing on each product version. This includes low level testing designed to address any CC related issues.
Vulnerability Assessment: None	The public search was updated from 8/13/2020. No new public vulnerabilities were discovered that are applicable to the TOE.

Description of ASE Changes:

The Security Target was updated to reflect the new product version.

Description of AGD Changes:

The Admin Guidance document was updated to include minor editorial changes.

Changes to TOE:

The changes to the TOE include extra error and bounds checking. The impact of these changes is minor and do not directly impact the assurance. Changes include items such as additional auditing events, minor bug fixes, usability issue fixes, and added security checks beyond those required. The changes are described in the table below.

Change Description	Security Analysis
Fixed an issue at -45C where RNG source would not function correctly.	The EAR claimed the health check bottom range is -40. This is outside the claimed range.
When PSK is erased, the action is logged.	Auditing is not an evaluated function.
Zeroizing the HW-Layer will now log a tamper event.	Auditing is not an evaluated function.
Enhanced validation of ATECC508A to ensure storage unwritten.	During a first ever power-up event (at the manufacturer), the firmware sets the ATECC508A storage portion to all 0's (a known value). What was previously happening was when writing the 0's, it wasn't being verified (write, read, verify). This is an added security check beyond those required.
Payload checksum was previously not calculating the command code nor the payload size. Must have software 3.00.03-fips loaded for this fix.	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.
Fixed a problem where HW-Layer would enter an abort state while clearing sensitive data from the internal RAM.	This was an error condition being handled improperly. This has been corrected and no SFRs are directly impacted by this change
Changed zeroize flag routine in attempt to fix valid PSK flag from getting corrupted.	This was an error condition being handled improperly. This is a usability issue.
Increased size of buffer being passed to system configuration PROM functions.	This is an added bounds feature to ensure proper configuration passed. This is added error checking and no SFRs are directly impacted by this change.
Fixed a problem when powering off the unit during a zeroize would erase the PSK and valid PSK flag.	There was a bug that occurs during zeroization that a single byte in the ATECC508A is getting corrupted. This single byte indicates whether or not the PSK that is stored in the ATECC508A is valid or not. If this flag gets erased, the H/W layer will no longer be able to create a user account because the PSK is no longer valid (i.e.

	the user token/HMAC cannot be encrypted/generated). This is a low level error detection issue and no SFRs are directly impacted by this change.

Assurance Continuity Maintenance Report:

Gossamer Security Solutions, CCTL, on behalf of Curtis-Wright Defense Solutions, submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS). 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 because of those changes, and the security impact of those changes.

Description of Regression Testing:

Curtiss Write performs regression testing on each product version. This includes low level testing designed to address any Common Criteria related issues. Each 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. Curtis Wright ensures that any given release does not break the existing functionality. The tests are also to ensure that developers are not introducing new bugs with each release.

Vulnerability Assessment:

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

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

Gossamer selected the 18 search key words based upon the vendor’s name, the product name, and key platform features the product leverages. 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
- Curtiss Wright Crypto Firmware

- NXP (Phillips) ARM7 Processor P/N LPC2368FBD100
- Maxim Integrated DS3645, Rev A4
- Microchip ATECC508A
- Enova X-Wall MX-256C

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 28, 2022. No vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

> There have been minor product changes to add extra error/bounds checking. The ST has been updated to reflect the new version. The guidance document was updated for editorial changes.
>
> Note that Curtiss Wright Defense Systems 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 Security Target was updated to reflect the new version and the admin guidance was updated to include small editorial changes/clarifications. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.