ASSURANCE CONTINUITY MAINTENANCE REPORT FOR KLC Group LLC CipherDriveOne Kryptr 1.1.1

KLC Group LLC CipherDriveOne Kryptr 1.1.1

Maintenance Report Number: CCEVS-VR-VID11399-2026

Date of Activity: May 7, 2026

References:

- *Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation*, version 3.0, 12 September 2016
- *KLC Group LLC CipherDriveOne Kryptr 1.1.1 Impact Analysis Report*, Version 1.1, April 2026
- *KLC Group LLC CipherDriveOne Kryptr 1.1.1 Security Target*, Version 2.0, March 2026
- *KLC Group LLC CipherDriveOne Kryptr 1.1.1 Common Criteria Guide*, Version 2.0, March 2026
- *KLC Group LLC CipherDriveOne Kryptr Administrator Guide*, Version 1.1.1 build 1, 1-26-2026
- *collaborative Protection Profile for Full Drive Encryption – Encryption Engine* Version 2.0 + Errata 20190201, February 1, 2019 [CPPFDE_EE]
- *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition* Version 2.0 + Errata 20190201, February 1, 2019 [CPPFDE_AA]

Assurance Continuity Maintenance Report:

KLC Group LLC submitted an Impact Analysis Report (IAR) for the CipherDriveOne Kryptr 1.1.1 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval in March 2026. 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 3.0. 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 Common Criteria Guide (AGD), the Administrator's Guide, and the IAR. The ST, AGD, and Administrator's Guide were updated to the new version of the TOE.

Documentation updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: *KLC Group LLC CipherDriveOne Kryptr 1.1.0 Security Target*, Version 1.5, April 2024	**Maintained Security Target:** See references above. Updated to identify the new TOE version number. ST version references and AGD and Administrative Guide version and date references also updated.
Design Documentation: See ST and Guidance	No changes required
Guidance Documentation: *KLC Group LLC CipherDriveOne Kryptr 1.1.0 Common Criteria Guide*, Version 1.1, April 2024 *KLC Group LLC CipherDriveOne Kryptr Administrator Guide*, Version 1.0.1 build 17, 4-18-2024	**Maintained Guidance Documentation:** See references above. AGD and Administrator Guide updated to identify the new TOE version number. Administrative Guide references also updated in the AGD.
Lifecycle: None	No changes required.
Testing: None	As provided in more detail below, the Vendor's Quality Assurance test reports demonstrate that the TOE continued to perform as expected on all platforms after the implementation of the security patches, feature enhancements, and bug fixes.
Vulnerability Assessment: None	The public search was updated on April 21, 2026. No public vulnerabilities exist in the product. See analysis results below.

Changes to the TOE:
The TOE software has been updated from version 1.1.0 (Build 17) to 1.1.1 (Build 1). Below is a summary of the changes incorporated in the new software version.

Major Changes

None.

Minor Changes

The IAR identified security patches covering 79 CVEs that were applied to the TOE, 15 product enhancements, and 26 bug fixes between versions 1.1.0 and 1.1.1 along with a description and analysis. Changes occurred over a series of Builds: version 1.1.0, Builds 18-25, and version 1.1.1 Build 1. While the majority of the updates impacted all platforms, some of the enhancements were

platform dependent and three bug fixes were specific to Linux. The description and analysis for each security patch, enhancement, and bug fix were inspected, and the overall Minor Change characterization was considered appropriate. None of the changes resulted in the introduction of new TOE capabilities, modification to security functions as defined in the ST, or changes to the TOE boundary. The following table includes a summary of the changes presented in the IAR that impact one or more of the evaluated platforms. The changes have been categorized according to security patches, enhancements, and bug fixes.

Category	Number of Changes	Assessment
Security Patches – Version 1.1.0, Build 22 and Version 1.1.1 Build 1	79 total CVEs	There were two Builds that covered security patches. Build 22 covered 24 CVEs. Build 1 covered 55 CVEs. The security patches updated various libraries, utilities, and package versions. None of the security patches affected the security functionality and none of the changes resulted in changes to the ST or guidance documentation. These changes were either unrelated to SFRs or outside the scope of the evaluated configuration. Thus, the original evaluation testing still holds, and any testing was covered by vendor non-evaluation regression testing.
Enhancements – Version 1.1.0, Builds 19, 22 - 25	15	There were five Builds that covered product enhancements. Enhancements were made that: • Added information to logs and detection/reporting capabilities • Updated drivers and driver setup • Added shortcut keys and updated command line options/the GUI and install templates • Improved licensing capabilities • Added support for RedHat 9.5 and 9.6 configurations • Improved the Shrink LVM process None of the Enhancements were SFR related or covered by the SFR functionality claimed. Thus, the original evaluation testing still holds,

		and any testing was covered by vendor non-evaluation regression testing.
Bug Fixes – Version 1.1.0, Builds 18 – 25	26	26 Bug fixes were made that impacted the: • Mouse cursor and keyboard input • Licenses, to include evaluation licenses • Sleep times • Installation • Boot and automatic boot issues • Partitions and directories • Build errors None of the Big fixes were SFR related or had impacted SFR claims. Thus, the original evaluation testing still holds, and any testing was covered by vendor non-evaluation regression testing.

Regression Testing:
The Vendor performed regression testing on the updated TOE on the claimed platforms. Regression testing included installation, configuration, and login to management console and the protected OS; verification of full disk encryption; multi-user configuration with all user roles; change password parameters; smartcard multifactor authentication; failed login lockout thresholds; log message visibility; and uninstallation and boot into OS. The successful completion of all these tests provided the Vendor with confidence regarding the proper behavior of the new firmware. The Lab reviewed the test evidence and confirmed that the updated TOE operates as expected and maintains all claimed functionality.

Equivalency:
The security functionality of the software version update to 1.1.1 remains the same as the prior evaluated version. The changes do not introduce new cryptographic functionality, modify the security boundary of the TOE, or change the Security Functionality Requirements of the TOE. The overall security functionality and operational behavior of the TOE remain unchanged.

The host platforms have been updated to include RedHat 9.5 and 9.6; however, this is a minor version variation that does not impact either the originally evaluated version of the TOE or its interfaces.

NIST CAVP Certificates:
The cryptographic functions validated under the CAVP certificate numbers remain unchanged and as noted in the Equivalency subsection, no TOE cryptographic interfaces have changed. The operating environment remains covered by those certificates. The CAVP certificate numbers referenced during the original 1.1.0 evaluation remain applicable to the TOE.

Vulnerability Analysis:
A new search was performed for vulnerabilities on April 21, 2026. The search was conducted against the following databases:

- NIST National Vulnerability Database: https://nvd.nist.gov

- MITRE CVE Search: https://cve.mitre.org/cve/search_cve_list.html
- CISA - Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

The search used the same terms as the original evaluation, with the exception of the OpenSSL and Linux kernel versions which were updated: CipherDriveOne, Kryptr, CipherDriveOne Kryptr, KLC CipherDriveOne Kryptr, Key sanitization, Opal management software, Password caching, Key destruction, Key caching, SED management software, Disk Encryption, Drive Encryption, Linux Crypto API, Windows CryptoAPI, BoringSSL, OpenSSL fips object module, Libgcrypt, Cryptsetup, OpenSSL 3.2.2, Opensc, Linux Kernel 6.6.105.

The results of the vulnerability assessment were included in the IAR. No new TOE vulnerabilities were found.

Conclusion:

The overall impact is minor. This is based on the rationale that the patches, enhancements, and bug fixes do not change any security policies of the TOE and are unrelated from SFR claims. The updates described above were made to support the updated TOE software.

Regression testing was done and was considered adequate based on the scale and types of changes made. The vendor also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. In addition, the host platform changes were minor version variations and there were no necessary alterations to the NIST cryptographic certificates. Therefore, CCEVS agrees that the original assurance is maintained for the product.