Common Criteria Maintenance Report

CipherDriveOne 2.1.0

CAN-648-LAB

3 June 2026

v1.0

Communications Security Establishment Canada
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité
Canada

Foreword

This maintenance report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this report has been previously evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This report applies only to the identified version and release of the product in its evaluated configuration.

This report is not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report. Furthermore, no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report is either expressed or implied.

If your organization has identified a requirement for this report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security

Contact Centre and Information Services

contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

TABLE OF CONTENTS

Executive Summary CAN-648-LAB

The purpose of this document is to summarize and present the Canadian Common Criteria program's findings regarding the assurance maintenance of **CipherDriveOne 2.1.0**, hereafter referred to as the maintained Target of Evaluation, or maintained TOE.

An Impact Analysis Report was submitted to the Canadian Common Criteria Program to extend the validity of the Common Criteria certificate previously awarded to **CipherDriveOne 2.0.1** from **KLC Group LLC** .

The process to achieve this is described in Assurance Continuity: CCRA Requirements, version 3.0, March 2023. In accordance with the requirements of this process, the Impact Analysis Report describes all changes made to the product and/or its IT environment, all resulting changes made to the evaluation evidence, and the security impact of the changes.

The Canadian Centre for Cyber Security, as the Certification Body, declares that the assurance gained during the original certification has been preserved.

Description of Changes

The following characterizes the changes implemented in the maintained TOE and/or the environment. For each change, it was verified that there were no required changes to the security functional requirements in the Security Target.

Original TOE	CipherDriveOne 2.0.1
Maintained TOE	CipherDriveOne 2.1.0
Developer	KLC Group LLC

Description of Changes in the Maintained Target of Evaluation

The changes in the maintained TOE comprise the following:

- Security updates: Updates to third-party and system software components to address known vulnerabilities. These include package upgrades, targeted patches, and removal of unused vulnerable packages. The following CVEs were patched:

CVE-2026-31431	CVE-2025-4598	CVE-2025-0840	CVE-2025-5244
CVE-2025-5245	CVE-2025-69644	CVE-2025-69647	CVE-2025-69648
CVE-2025-69649	CVE-2025-69650	CVE-2025-69651	CVE-2025-69652
CVE-2026-3441	CVE-2026-3442	CVE-2026-4647	CVE-2025-46394
CVE-2025-60876	CVE-2024-28757	CVE-2024-45490	CVE-2024-45491
CVE-2024-45492	CVE-2024-50602	CVE-2025-59375	CVE-2025-66382
CVE-2026-24515	CVE-2026-25210	CVE-2026-32776	CVE-2026-32777
CVE-2026-32778	CVE-2025-27363	CVE-2023-4156	CVE-2023-4911
CVE-2023-5156	CVE-2024-2961	CVE-2024-33599	CVE-2024-33600
CVE-2024-33601	CVE-2024-33602	CVE-2025-4802	CVE-2025-15281
CVE-2026-0861	CVE-2026-0915	CVE-2026-4046	CVE-2026-4437
CVE-2026-4438	CVE-2026-5435	CVE-2026-5450	CVE-2026-5928
CVE-2026-6238	CVE-2025-32988	CVE-2026-22693	CVE-2020-12825

CVE-2024-7264	CVE-2025-0725	CVE-2023-29499	CVE-2023-32611
CVE-2023-32636	CVE-2023-32643	CVE-2023-32665	CVE-2024-34397
CVE-2024-52533	CVE-2025-4056	CVE-2025-13601	CVE-2025-14087
CVE-2025-14512	CVE-2018-11813	CVE-2020-14152	CVE-2020-14153
CVE-2024-6119	CVE-2025-64505	CVE-2025-64506	CVE-2025-64720
CVE-2025-65018	CVE-2025-66293	CVE-2026-22801	CVE-2026-25646
CVE-2025-5318	CVE-2025-5351	CVE-2025-5372	CVE-2025-5987
CVE-2025-8114	CVE-2026-3731	CVE-2024-34402	CVE-2024-34403
CVE-2024-25062	CVE-2024-34459	CVE-2024-40896	CVE-2024-56171
CVE-2025-6021	CVE-2025-24928	CVE-2025-27113	CVE-2025-32414
CVE-2025-32415	CVE-2026-6732	CVE-2025-6170	CVE-2024-55549
CVE-2025-24855	CVE-2026-22184	CVE-2026-27171	CVE-2022-44370
CVE-2025-23419	CVE-2014-4550	CVE-2021-4336	CVE-2024-45615
CVE-2024-45616	CVE-2024-45617	CVE-2024-45618	CVE-2024-45619
CVE-2024-45620	CVE-2022-44940	CVE-2023-24056	CVE-2022-42969
CVE-2025-47273	CVE-2026-35094	CVE-2023-27043	CVE-2023-36632
CVE-2024-6232	CVE-2024-7592	CVE-2024-9287	CVE-2025-6075
CVE-2025-12084	CVE-2025-12781	CVE-2025-13836	CVE-2025-13837
CVE-2026-3087	CVE-2026-4519	CVE-2019-15845	CVE-2019-16201
CVE-2019-16254	CVE-2019-16255	CVE-2020-5247	CVE-2020-25613
CVE-2021-28965	CVE-2021-28966	CVE-2021-31810	CVE-2021-41819
CVE-2022-28739	CVE-2023-28756	CVE-2025-3277	CVE-2025-6965
CVE-2025-29087	CVE-2024-29038	CVE-2024-29039	CVE-2023-22745
CVE-2024-28085	CVE-2026-3184	CVE-2026-27456	CVE-2023-3138
CVE-2023-43785	CVE-2023-43786	CVE-2023-43787	CVE-2022-1271

CVE-2026-34743			

- User-interface, and operational usability enhancements: Added or revised installation modes, automated installer support, generic/clandestine UI option, virtual/on-screen keyboard support, and related UI behavior improvements.
- Bug fixes and operational corrections: Resolved installer, boot, GUI/console formatting, error-message, logging, disk-space, and configuration-handling issues.

Description of Changes to the IT Environment

The changes to the IT environment comprise the following:

- Installation-environment changes: support was added for automated Windows installer, console/GUI installation selection, and temporary disabling of BlockSID for the next boot from the installer.

Affected Developer Evidence

Modifications to the product necessitated changes to the following developer evidence that was previously submitted in support of the original evaluation:

- KLC Group LLC CipherDriveOne 2.0.1 Security Target, Version 1.3, June 2024 was updated with the new TOE reference
- The KLC Group LLC CipherDriveOne 2.0.1 Common Criteria Guide, Version 1.3, June 2024 was updated to reflect the maintained TOE reference, CipherDriveOne 2.1.0.

Conclusion

As all changes to the maintained TOE were classified as minor, the Certification Body has determined that assurance maintenance is appropriate and that re-evaluation is not required. The assurance maintenance for the TOE was conducted in accordance with the provisions of the Canadian Common Criteria Program, and the conclusion reached is consistent with the evidence presented.

Functional and regression testing of the maintained TOE confirmed that the assurance gained during the original certification has been preserved.

References

Reference
Assurance Continuity: CCRA Requirements, V3.0, March 2023
Common Criteria Certification Report CipherDriveOne 2.0.1, V1.0, 27 June 2024
KLC Group LLC CipherDriveOne 2.1.0 Security Target, Version 2.0, May 2026
KLC Group LLC CipherDriveOne 2.1.0 Impact Analysis Report, Version 1.0, May 2026