Common Criteria Certification Report

Crunchy Certified PostgreSQL 17.9

CAN-674-LSS

7 July 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 certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Program, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

This report, and its associated certificate, are 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, and its associated certificate, and 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, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification 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)

Overview

The Canadian Common Criteria Program provides a third-party evaluation service for evaluating the security of IT products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target (ST). A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the ST, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCTL.

The certification report, certificate of product evaluation and ST are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

Executive Summary CAN-674-LSS

Crunchy Certified PostgreSQL 17.9 (hereafter referred to as the Target of Evaluation, or TOE), from **Crunchy Data Solutions, Inc.** , was the subject of this Common Criteria evaluation . The results of this evaluation demonstrate that the TOE meets the following conformance claim: **collaborative Protection Profile for Database Management Systems v1.3, March 13, 2023**

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on **7 July 2026** and was conducted in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to consider the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

Identification of Target of Evaluation

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Crunchy Certified PostgreSQL 17.9
Developer	Crunchy Data Solutions, Inc.

See the Evaluated Configuration section for more details on the evaluated configuration of the TOE.

Common Criteria Conformance

The evaluation was conducted using the following methodology:

Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5

The TOE claims the following conformance:

collaborative Protection Profile for Database Management Systems v1.3, March 13, 2023

TOE Description

The TOE is an open source relational database management system (DBMS). The TOE includes PostgreSQL and tools for clients, developers and administrators. It is a computerized repository that stores information and allows authorized users to retrieve and update that information.

The TOE may be operated as a single-user system, in which only one user may access the DBMS at a given time, or as a multi-user system, in which many users may access the DBMS simultaneously.

TOE Architecture

A diagram of the TOE architecture is as follows:

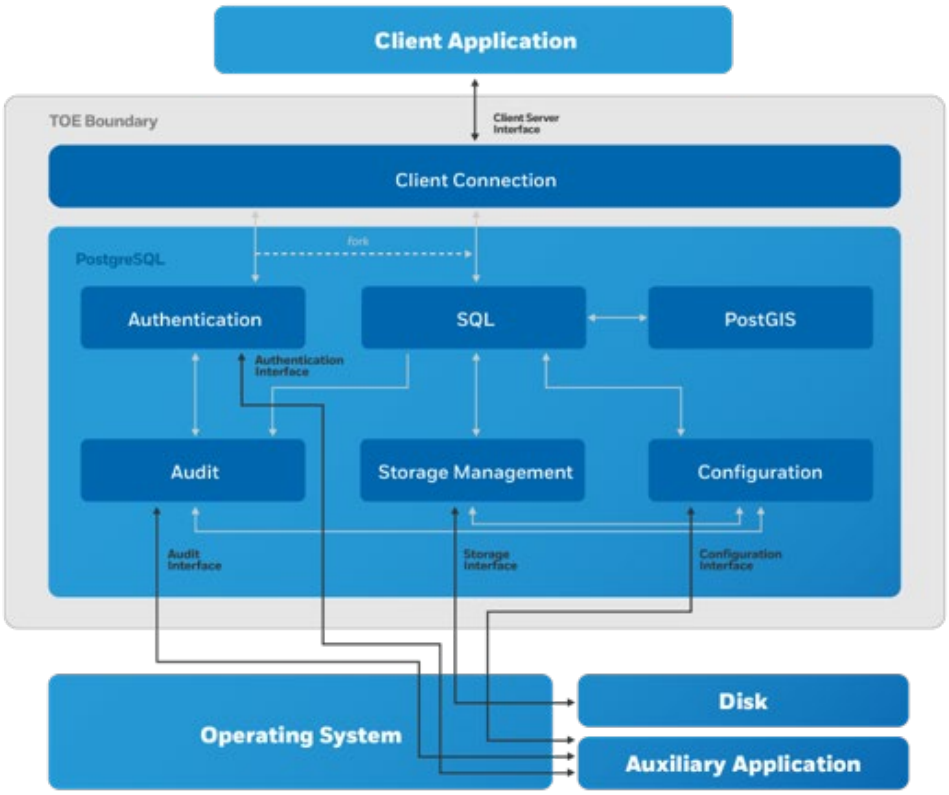

Figure 1: TOE Architecture

Security Policy

The TOE implements and enforces policies pertaining to the following security functionality:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access

Complete details of the security functional requirements (SFRs) can be found in the Security Target.

Cryptographic Functionality

The TOE makes use of the following CMVP validated cryptographic module:

Table 2: Cryptographic Implementation(s)

Cryptographic Implementation	Certificate Number
Red Hat Enterprise Linux 9 - OpenSSL FIPS Provider v3.0.7-395c1a240fbfffd8	CMVP #4857

Assumptions and Clarification of Scope

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

Usage and Environmental Assumptions

The following assumptions are made regarding the use and deployment of the TOE:

- The operational environment is assumed to provide the TOE with appropriate physical protection such that the TOE is not subject to physical attack that may compromise the security and/or interfere with the platform's correct operation. This includes protection for the physical infrastructure on which the TOE depends for correct operation and hardware devices on which the TOE is executing.
- Authorized users possess the necessary authorization to access the information managed by the TOE in accordance with organization information access policies.
- The TOE security functionality is managed by one or more competent, authorized administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
- Authorized users are sufficiently trained to accomplish a task or group of tasks within a secure IT environment by exercising complete control over their user data.
- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.
- All external IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.
- Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.

- All connections to and from remote trusted IT systems and between separate parts of the TSF not protected by the TSF itself are physically and/or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

Clarification of Scope

The TOE relies on the operating system, which is part of the operational environment, to provide cryptographic support for communications, such as SSL encryption. Thus, cryptographic functionality is outside the scope of this evaluation. Specifically, support for secure communication channels and certificate-based authentication was not evaluated.

Crunchy PostgreSQL provides synchronous streaming replication as a way to replicate changes to data on one database server to the other database servers within a cluster. The evaluated TOE architecture is a stand-alone system running a single PostgreSQL server. Thus, streaming replication functionality is outside the scope of this evaluation.

The following TOE configuration options are not included within the scope of the evaluation:

- "Trust" authentication option
- "Ident" authentication option
- "SSPI" authentication option
- Certificate authentication option
- GSSAPI Authentication
- Peer Authentication
- Streaming Replication Configuration
- Logical Replication Configuration

Evaluated Configuration

The evaluated configuration for the TOE comprises:

Table 3: Evaluated Configuration

TOE Software/Firmware	PostgreSQL 17.9 with the following client connectors: • Java Database Connectivity (42.7.7-0Crunchy.el9) • Libpq (postgresql17-libs-17.6-0Crunchy.el9.x86_64) And the following extensions: • PostgreSQL Audit Extension (17.1-1Crunchy.el9) • PostGIS Spatial Extensions (3.5.5-0Crunchy.el9)
Environmental Support	• Red Hat Enterprise Linux Version 9.4 • LDAP/Radius server

Documentation

The following documents are available to the consumer to assist in the configuration and installation of the TOE:

a) The PostgreSQL Global Development Group; PostgreSQL 17 Documentation, Version 17.9
b) The PostgreSQL JDBC Interface v42.7.9
c) PostgreSQL Audit Extension User Guide 17.1
d) PostGIS 3 Manual 3.5.5
e) Secure Installation and Configuration Guide – Crunchy Certified PostgreSQL 17, Version 1.6

Evaluation Analysis Activities

The evaluation activities comprised a structured assessment of the TOE. Documentation and processes related to Development, Guidance Documentation, and Life-Cycle Support were reviewed and analyzed.

Development

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

Guidance Documents

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators exercised the preparative and operational guidance and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all the procedures required to maintain the integrity of the TOE during distribution to the consumer.

Testing Activities

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

Conduct of Testing

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate proprietary test results document.

Independent Testing

During this evaluation, the evaluator developed independent functional & penetration tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP;
b. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests; and
c. Cryptographic implementation verification: The evaluator verified that the claimed cryptographic implementation was present in the TOE.

Independent Testing Results

The testing produced the expected results, supporting the conclusion that the TOE correctly implements the functional requirements specified in the ST and the TOE functional specification.

Vulnerability Analysis

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases, and technical community sources. Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities. Based upon this review, the evaluators formulated flaw hypotheses , which they used in their vulnerability analysis.

Public domain searches were conducted on **1 May 2026** and included the following search terms:

Crunchy Certified PostgreSQL 17	PostGIS	Libpq
Crunchy DBMS	PgAudit	Openssl 3.0.7
PostgreSQL 17	JDBC 42.7	Red Hat Enterprise Linux 9.4

Vulnerability searches were conducted using the following sources:

CrunchyData Security Blog: https://www.crunchydata.com/blog/topic/security	National Vulnerability Database https://nvd.nist.gov/vuln/search
PostgreSQL security postings: https://www.postgresql.org/support/security	CISA Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Vulnerability Analysis Results

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

Results of the Evaluation

The Information Technology product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

Recommendations/Comments

It is recommended that all guidance be followed to configure the TOE in the evaluated configuration.

The evaluator was impressed by the developer's commitment to flaw remediation. The developer has a commitment to open-source development and is well staffed monitoring and fixing bugs.

Supporting Content

List of Abbreviations

Term	Definition
ACVP	Automated Cryptographic Validation Protocol
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ESV	Entropy Source Validation
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

References

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5.
Evaluation Technical Report Crunchy Certified PostgreSQL 17.9, 2026-07-07, v1.4.
Security Target Crunchy Certified PostgreSQL 17.9, 2026-07-06, v1.9.
Assurance Activity Report Crunchy Certified PostgreSQL 17.9, 2026-07-07, v1.3.