Swedish Certification Body for IT Security

Certification Report - Oracle DB 19c

Issue: 1.0, 2021-Jun-24

Authorisation: Jerry Johansson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is a relational database management system (RDBMS), which is accessible directly, or through a front end using Structured Query Language (SQL). The TOE is software only, and is designed to run on top of Oracle Linux 8.1 and general purpose computing hardware.

The certified version of the TOE is Oracle Database 19c Enterprise Edition, version 19.11 with Critical Patch Update April 2021.

The evaluation covers the following configurations of the TOE: Standalone, Client-Server, Distributed (with a redundant database instance), and Multi-tier.

The TOE claims demonstrable conformance with the Base Protection Profile for Database Management Systems (DBMS PP), version 2.12, 2017-03-23 with the DBMS PP Extended Package – Access History, version 1.02, 2017-03-23.

The evaluation has been performed by Combitech AB in Stockholm, Sweden, partly with the assistance of Electronic Warfare Associates-Canada Ltd. in Ottawa, Canada.

The evaluation was completed on the 16th of June 2021. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation was performed at the evaluation assurance level EAL 2, augmented by ALC_FLR.2 Flaw reporting procedures.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

Electronic Warfare Associates-Canada Ltd. operates as a Foreign Location for Combitech AB within the scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 2 + ALC_FLR.2.

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by Combitech AB.

2 Identification

Certification Identification	
Certification ID	CSEC2020007
Name and version of the certified IT product	Oracle Database 19c Enterprise Edition (with Database Vault, Multitenant and Label Security) Version 19.11 with Critical patch Update April 2021
Security Target Identification	Oracle Database 19c Enterprise Edition (with Database Vault, Multitenant and Label Security) Security Target, Oracle Corporation, 2021-06-03, document version 1.3
EAL	EAL 2 + ALC_FLR.2
Sponsor	Oracle America Inc.
Developer	Oracle America Inc.
ITSEF	Combitech AB and EWA-Canada
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.24.1
Scheme Notes Release	18.0
Recognition Scope	CCRA, EA-MLA, SOGIS
Certification date	2021-06-24

3 Security Policy

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

3.1 Security Audit

Audit entries are generated for security related events. Audit policies may be created to generate logs based on details such as the user, the object being accessed, event type or success or failure of the operation.

3.2 User Data Protection

The TOE provides a discretionary access control policy to provide fine-grained access control between users and database objects. The TOE implements Oracle Label Security (OLS) to restrict access based on authorization level enforced by labels. The TOE provides a Database Vault access control policy to enforce additional access controls to user data. In a multitenant environment, resources in pluggable databases are logically separate and inaccessible by local users in any other pluggable database or Container Database (CDB). Once data is allocated to a resource, the previous information content is no longer available.

3.3 Identification and Authentication

Users must identify and authenticate prior to gaining TOE access. Attributes are maintained to support the access control policy.

3.4 Security Management

The TOE provides management capabilities via SQL statements. Management functions allow the administrators to:

- configure auditing and access control options (including granting and revoking privileges)
- configure users (including the maximum number of concurrent sessions) and roles
- configure replication options
- configure Database Vault functions
- configure Oracle Label Security
- configure separate domains for pluggable databases within a container database
- assess roles and privileges in use at run-time

Database Vault and Label Security management capabilities are provided through designated Procedural Language Extension to Structured Query Language (PL/SQL) procedures.

3.5 Protection of the TSF

Data may be consistently replicated to a secondary DBMS server.

3.6 TOE Access

The number of concurrent user sessions may be limited by policy. User login may be restricted based on user identity.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes eight assumptions on the usage and the operational environment of the TOE:

A.PHYSICAL

It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

A.AUTHUSER

Authorized users possess the necessary authorization to access at least some of the information managed by the TOE.

A.MANAGE

The TOE security functionality is managed by one or more competent administrators. The system administrative personnel are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.

A.TRAINEDUSER

Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.

A.NO_GENERAL_ PURPOSE

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.

A.PEER_FUNC_&_ MGT

All remote trusted 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.

A.SUPPORT

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.

A.CONNECT

All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality if the data transmitted and to ensure the authenticity of the communication end points.

4.2 Clarification of Scope

The Security Target contains seven threats, which have been considered during the evaluation:

T.ACCESS_TSFDATA

A threat agent may read or modify TSF data using functions of the TOE without the proper authentication.

T.ACCESS_TSFFUNC

A threat agent may use or manage TSF, bypassing protection mechanisms of the TSF.

T.IA_MASQUERADE

A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.

T.IA_USER

A threat agent may gain access to user data, TSF data, or TOE resources with the exception of public access objects without being identified and authenticated.

T.RESIDUAL_DATA

A user or a process acting on behalf of a user may gain unauthenticated access to user or TSF data through reallocation of TOE resources from one user or process to another.

T.TSF_COMPROMISE

A user or a process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.

T.UNAUTHORIZED_ ACCESS

A threat agent may gain unauthenticated access to user data for which they are not authorized according to the TOE security policy.

The Security Target contains three Organisational Security Policies (OSPs), which have been considered during the evaluation:

P.ACCOUNTABILITY

The authorized users of the TOE shall be held accountable for their actions within the TOE.

P.ROLES

Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.

P.USER

Authority shall only be given to users who are trusted to perform the actions correctly.

5 Architectural Information

The TOE security functionality is implemented in two subsystems:

• the Oracle Net Subsystem, and

• the Kernel Subsystem.

The Oracle Net Subsystem, which is SFR-supporting, provides session establishment, communications, and network management.

The Kernel Subsystem, which is SFR-enforcing, performs all of the necessary tasks for managing a database.

6 Documentation

The following documents are included in the scope of the TOE:

CCADM	Oracle® Database 19c Enterprise Edition (with Database Vault, Multitenant and Label Security) Common Criteria Guidance Supplement
INST	Oracle® Database Database Installation Guide 19c for Linux
ADM	Oracle® Database Database Administrator's Guide 19c
MULTI	Oracle® Multitenant Administrator's Guide 19c
SQL	Oracle® Database SQL Language Reference 19c
PL/SQL	Oracle® Database PL/SQL Language Reference 19c
SEC	Oracle® Database Security Guide 19c
DG	Oracle® Data Guard Concepts and Administration 19c
VAULT	Oracle® Database Vault Administrator’s Guide 19c
LABEL	Oracle® Label Security Administrator's Guide 19c

7 IT Product Testing

Full testing was first performed on version 19.10 with the January 2021 Critical Patch Update. After updating the TOE to version 19.11 with the April 2021Critical Patch Update, all the developer tests, and 70 percent of the evaluator tests, were repeated. All the penetration tests were rerun.

7.1 Developer Testing

The developer testing was done using automated test scripts, launched one by one or in test sequences. The developer's testing covers all SFRs.

Testing was performed in 3rd-4th June 2021 in the developer's premises in USA, UK and India. All tests were successful.

7.2 Evaluator Testing

The evaluators repeated a subset of the developer tests and performed independently devised complementary tests.

The evaluator testing was performed 1st-4th of June 2021. The repeated developer tests were performed remotely from the evaluator's premises in Stockholm, Sweden, and the independent tests were performed in the evaluator's premises in Stockholm, Sweden. All tests were successful.

7.3 Penetration Testing

Some negative tests were performed as part of the ATE testing. The network interface was scanned for unexpected open ports using NMAP. A vulnerability scan was made using Nessus.

The tests were performed 1st-4th of June 2021 in the evaluator's premises in Stockholm, Sweden. No unexpected behaviour or vulnerabilities were discovered.

8 Evaluated Configuration

The following operating system and hardware components are required for operation of the TOE (Oracle Database 19c), as well as database clients (non-TOE), in the evaluated configuration:

- Oracle Enterprise Linux 8.1
- General Purpose Computing Hardware

The deployment configurations considered in the evaluation are:

- Standalone Database Configuration
- Distributed Database Configuration
- Client Server Database Configuration
- Multi-tier Database Configuration

as defined in the ST.

Installation and configuration of the TOE shall be done in accordance with the guidance documentation, in particular with the Guidance Supplement [CCADM].

The following features are excluded from this evaluation:

- Authentication features
  - Although Oracle Database 19c supports several authentication mechanisms, including Kerberos and Public Key Infrastructure, only Oracle password authentication was demonstrated for the purposes of this evaluation.
- Real Application Clusters (RAC)
- External clients
- Autonomous Database
  - The autonomous database, which is the Oracle Database Enterprise Edition deployed in the cloud and offered as a service, was not evaluated.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class/Family	*Class/ Component*	*Verdict*
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.2	PASS
TOE Design	ADV_TDS.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.2	PASS
CM Scope	ALC_CMS.2	PASS
Delivery	ALC_DEL.1	PASS
Flaw Remediation	ALC_FLR.2	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria for Information Technology Security, a set of three documents describing different aspects of Common Criteria evaluations
CDB	Container Database
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
DBMS	Database Management Security
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
OLS	Oracle Label Security
PP	Protection Profile
RDBMS	Relational Database Management System
SFR	Security Functional Requirement. A requirement on the TOE in the ST.
SQL	Structured Query Language
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation

12 Bibliography

CC	Common Criteria for Information Technology Security Evaluation, CCMB-2017-04-001 through 003, document versions 3.1 revision 5
CEM	Common Methodology for Information Technology Security Evaluation, CCMB-2017-04-004, document version 3.1 revision 5
ST	Oracle Database 12c Enterprise Edition, Security Target, Oracle, 2021-06-03, document version 1.3
DBMS PP	Base Protection Profile for Database Management Systems Base Package, BSI, 2017-03-23, document version 2.12
EP	DBMS PP Extended Package - Access History, BSI, 2017-03-23, document version 1.02
CCADM	Oracle® Database 19c Enterprise Edition (with Database Vault, Multitenant and Label Security) Common Criteria Guidance Supplement, Oracle Corporation, 2021-06-03, document version 0.6
INST	Oracle® Database Database Installation Guide 19c for Linux, Oracle Corporation, April 2021, document version E96432-15
ADM	Oracle® Database Database Administrator's Guide 19c, Oracle Corporation, April 2021, document version E96348-12
MULTI	Oracle® Multitenant Administrator's Guide 19c, Oracle Corporation, April 2021, document version E96136-11
SQL	Oracle® Database SQL Language Reference 19c, Oracle Corporation, April 2021, document version E96310-09
PL/SQL	Oracle® Database PL/SQL Language Reference 19c, Oracle Corporation, August 2020, document version E96448-03
SEC	Oracle® Database Security Guide 19c, Oracle Corporation, May 2021, document version E96299-11
DG	Oracle® Data Guard Concepts and Administration 19c, Oracle Corporation, February 2021, document version E96244-04
VAULT	Oracle® Database Vault Administrator’s Guide 19c, Oracle Corporation, March 2021, document version E96302-15
LABEL	Oracle® Label Security Administrator's Guide 19c, Oracle Corporation, March 2019, document version E96303-05

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used:

Version	Introduced	Impact of changes
1.24.1	2020-12-03	None - *the new requirements in SP-002 already fulfilled*
1.24	2020-11-19	None
1.23.2	2020-05-11	Original version

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in "Ändringslista CSEC QMS 1.24.1".

The certifier concluded that, from QMS 1.23.2 to the current QMS 1.24.1, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- SN 15 - Testing
- SN 18 - Highlighted requirements on the ST
- SN-22 - Vulnerability assessment
- SN 28 - Updated procedures

The applicable versions are part of Scheme Note release 18.0.