Reference: 2019-32-INF-3664- v1
Target: Limitada al expediente
Date: 25.03.2022

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2019-32**
TOE	**Huawei GaussDB 200 version 6.5.1 build e3690037**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**

References

[EXT-5296] Certification request

[EXT-7074] Evaluation technical report

Certification report of the product Huawei GaussDB 200 version 6.5.1 build e3690037, as requested in [EXT-5296] dated 12/07/2019, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-7074] received on 15/07/2021.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei GaussDB 200 version 6.5.1 build e3690037.

The TOE is a DBMS. It provides a relational database engine providing mechanisms for access control, identification and authentication, and security audit. It mainly focuses on online data analysis-processing scenarios with large data volumes. This TOE is a software-only TOE.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: DEKRA Testing and Certification S.A.U.

Protection Profile: [DBMSPP]: Protection Profile for Database Management Systems (Base Package), Version 2.12 dated March 23rd, 2017. BSI-CC-PP-0088-V2.

Evaluation Level: Common Criteria for Information Technology Security Evaluation Version 3.1 R5 – EAL2 + ALC_FLR.2.

Evaluation end date: 21/10/2021

Expiration Date[1]: 22/03/2027

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.2) have been assigned a “PASS” verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2 (augmented with ALC_FLR.2), as defined by the Common Criteria for Information Technology Security Evaluation Version 3.1 R5 and the Common Methodology for Information Technology Security Evaluation Version 3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Huawei GaussDB 200 version 6.5.1 build e3690037, a positive resolution is proposed.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

TOE SUMMARY

The TOE is a DBMS. It provides a relational database engine providing mechanisms for access control, identification and authentication, and security audit. It mainly focuses on online data analysis processing scenarios with large data volumes. The TOE can restrict the access of authorized users to the TOE, implement free access control on objects controlled by the DBMS based on users or roles, and can clarify users' responsibilities by their behaviour. This TOE is a software-only TOE.

The database provides the following functions:

- Supports standard SQL.

  Supports standard SQL92 and SQL2003, GBK and UTF-8 character sets, SQL standard functions, analytical functions, and SQL Procedural Language.

- Provides database storage management.

  Supports tablespaces and online scaling.

- Provides component management and high availability (HA) of data nodes.

  Supports atomicity, consistency, isolation, and durability (ACID) features of database transactions, recovery from single node failure, and load balancing.

- Provides data analysis capabilities.

  Supports full-text index, unified management of structured and semi-structured data,unified SQL access, and collaborative analysis between homogeneous clusters across data centers.

- Supports APIs.

  Supports standard JDBC 4.0 and ODBC 3.5.

- Provides security functions.

  Provides functions including security audit, user data protection, identity identification and authentication, security management, data backup and restoration, and session management, ensuring database security.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidences required by the additional component ALC_FLR.2, according to Common Criteria for Information Technology Security Evaluation Version 3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1

AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
	ALC_FLR.2
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria for Information Technology Security Evaluation Version 3.1 R5:

FAU: Security Audit	FAU_GEN.1. Audit data generation
	FAU_GEN.2. User identity association
	FAU_SEL.1. Selective audit
FDP: User Data Protection	FDP_ACC.1. Subset access control
	FDP_ACF.1. Security attribute based access control
	FDP_RIP.1. Subset residual information protection
FIA: Identification and Authentication	FIA_ATD.1. User attribute definition
	FIA_UAU.1. Timing of authentication
	FIA_UID.1. Timing of identification
	FIA_USB_(EXT).2. Enhanced user-subject binding
FMT: Security Management	FMT_MOF.1. Management of security functions behaviour
	FMT_MSA.1. Management of security attributes
	FMT_MSA.3. Static attribute initialization
	FMT_MTD.1. Management of TSF data
	FMT_REV.1(1). Revocation (user attributes)
	FMT_REV.1(2). Revocation (subject, object attributes)
	FMT_SMF.1. Specification of Management Functions
	FMT_SMR.1. Security roles

FPT: Protection of the TSF	FPT_TRC.1. Internal TSF consistency
FTA: TOE Access	FTA_MCS.1. Basic limitation on multiple concurrent sessions
	FTA_TAH_(EXT).1. TOE access information
	FTA_TSE.1. TOE session establishment

IDENTIFICATION

Product: Huawei GaussDB 200 version 6.5.1 build e3690037

Security Target: Huawei GaussDB 200 6.5.1 Security Target (version: 0.7, date: 2021-07-02).

Protection Profile: [DBMSPP]: Protection Profile for Database Management Systems (Base Package), Version 2.12 dated March 23rd, 2017. BSI-CC-PP-0088-V2.

Evaluation Level: Common Criteria for Information Technology Security Evaluation Version 3.1 R5 – EAL2 + ALC_FLR.2.

SECURITY POLICIES

The use of the product Huawei GaussDB 200 version 6.5.1 build e3690037 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 4.4 ("Organizational Security Policies").

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 4.5 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei GaussDB 200 version 6.5.1 build e3690037, although the agents implementing attacks have the attack potential according to the basic attack potential of EAL2+ ALC_FLR.2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Database Management Systems Protection Profile and they are documented in the Security Target, section 4.3 (“Threats”).

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 5.2 (“Operational Environment Security Objectives”).

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE consists of the following subsystems:

- **Kernel Subsystem** provides interfaces for external applications, authorizes and authenticates external requests, optimizes global execution plans, distributes the execution plans to Datanode instances, stores service data, executes data query tasks, and returns execution results.
- **Cluster Management** Subsystem provides management interfaces and tools for routine cluster O&M and configuration management. It manages and monitors the running status of functional units and physical resources in the distributed system, ensuring stable running of the entire system.

The following list describes the logical scope of the TOE. For details about each function, see the section *8.1 TOE Security Function* in the Security Target.

- **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.
- **User Data Protection**. The TOE provides a discretionary access control policy to provide access control between users and database objects (such as tables, columns, views, triggers, functions, and procedures) or metadata. Residual Information Protection (RIP) is used to ensure that the previous content of a resource is no longer available once the resource is allocated to a table, row, or other database object.
- **Identification and Authentication**. Users must be identified and authenticated prior to TOE access. Authentication modes are configured to implement the access control policy.
- **Security Management**. The TOE provides the management function by executing SQL statements on the client and using server tools. The management function allows

administrators to configure audit and access control options (including granting and revoking permissions), and the security attributes of users and roles.

- **Protection of the TSF**. The TSF is protected through backup and restoration solutions and data reliability assurance mechanisms, ensuring fault recovery consistency and replication consistency.
- **TOE Access**. The Session Handling mechanism, which limits the possibilities of users to establish sessions with the TOE and maintains a separate execution context for every operation. Also the Memory Management functionality belongs to the area of Session Handling and ensures that any previous information in memory is made unavailable before the memory is used either by overwriting the memory explicitly with a certain pattern or by overwriting the memory completely with new information.

PHYSICAL ARCHITECTURE

This TOE is a software-only TOE and physically consists of GaussDB 200 packages and related guidance documents. These software packages and guidance documents are provided in the DVD-ROM.

The TOE Binary is a database server program named *gaussdb* in *GaussDB_200_6.5.1_SLES.tar.gz* package and its patch *GaussDB_200_6.5.1_SUSE-64bit.tar.gz* provided in the DVD-ROM.

File Name	SHA256 Value
GaussDB_200_6.5.1_SLES.tar.gz	f3790bf3d37521f2aaa13f05bfb2ee52717bf057b7a8382f2dc3a2d729391f0a
GaussDB-200-6.5.1-SUSE-64bit.tar.gz	88a06b27aa5b8e77ed2013dec8cce91bcc70aec17a70c780d1156dc8cf92f13e
GaussDB_200_6.5.1_SLES.tar.gz.asc	-

In addition, the DVD-ROM includes a set of packages necessary to install the TOE:

File Name	SHA256 Value
FusionInsight_BASE_6.5.1_SLES.tar.gz	6b4b69b2588994f616e15c31c61241f8e738b8a66860b27f429df6a8a625f9c7
FusionInsight_Manager_6.5.1_SLES.tar.gz	96f6f55f087aa446aaa21ab00f6eb1aeddcaee2055ee1855bc0173a3b4a1257a
FusionInsight_SetupTool_6.5.1_SLES.tar.gz	e6a5936c4bdfedb523a422633ff806d760b9f7acbe1f505e3ff019419a3fd4da

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version. The documents are available to download from the DVD-ROM.

File Name	Version	SHA256 Value
GaussDB 200 6.5.1 Product Documentation 09.pdf	V09	ffa61309d2580c184867fb1265700aa344d42779a3ce07cdd0b2485b812ce93b
GaussDB 200 6.5.1 Administrator Guide 02.pdf	V02	e32d5b4009b31bfe3fff343b17313a1c7873f4832fb62ab7154224f28533f2af
GaussDB 200 6.5.1 Capacity Adjustment Guide 05.docx	V05	a767e08cbd71c603b20103eb04d092b0f55ce0e18daacdbbaf52cae989071ef4
GaussDB 200 6.5.1 Communication Matrix 02.xlsx	V02	ebf6c07685a2c5fdd8eee423675c70880e41b9217c7f3ea69dfb1cb82c72fcd6
GaussDB 200 6.5.1 Developer Guide 08.pdf	V08	fad4167fc2e38f3d177006c632131926988c7612b5ff23c7d9c8742d1f7a7624
GaussDB 200 6.5.1 Health Check Guide 01.pdf	V01	ac39348a3aa5e8ac01159d2cb460131f3b261ffe7343ea9414bba5193725cf7e
GaussDB 200 6.5.1 Security Hardening Guide 01.pdf	V01	88857ed642b4f5a3e8de303a3578706e9b7383d4a327839bcc4a6c6045bcb282
GaussDB 200 6.5.1 Security Maintenance Guide 01.pdf	V01	5c085317e28a4ed8646756eadeff78d154b223cb63447c39ea5ab5f0a3877faf
GaussDB 200 6.5.1 Software Installation 03.pdf	V03	ea1ca758a453d584c1f841c71645a18964da26f92884d9333c0a4f00d8d2cd5e
HUAWEI GaussDB 200 6.5.1 AGD_OPE V0.6.pdf	V06	3673113836f215f39252dab3bc6acbf4393099942eb113f2da977a685ba35ae3
HUAWEI GaussDB 200 6.5.1 AGD_PRE V0.7.pdf	V07	8f086c3933cc5c26f43a53db246a0bd3db08f449453a723b6610d1abcdfd0d45

PRODUCT TESTING

The TOE has two main subsystems, the Cluster Management Subsystem and the Kernel Subsystem. The strategy has been to test both of them (not covering each subsystem separately) by testing their functionalities through SFR testing.

In the case of the TSFIs, there are four interfaces: *gsql* Interface, *JDBC* Interface, *ODBC* Interface, Cluster Management Interface. The evaluation of these interfaces has been covered by testing the 100% of the Security Functional Requirements (SFR) specified in the [ST].

With this test strategy in conjunction with the vendors test suite, the evaluator has assured that all the TSFIs and Subsystems have been tested correctly and completely.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment, the evaluation team has devised attack scenarios for penetration tests. Within these activities, all aspects of the security architecture, which were not covered by functional testing, have been considered.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential *Basic* has been successful in the TOE's operational environment as defined in the security target when all security measures required by the developer in the security guidance defined in *DOCUMENTS* section are applied.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below.

Three servers (nodes) have been used in the evaluation with the following characteristics:

Type	Requirement
TOE	"GaussDB_200_6.5.1_SLES.tar.gz". The TOE Binary is a database server program named gaussdb in the package labelled as "GaussDB_200_6.5.1_SLES.tar.gz" "GaussDB-200-6.5.1-SUSE-64bit.tar.gz" The TOE patch
Server Nodes	2 Control Management nodes 1 Data node
TOE operation mode	OPEN mode (see section 3 Operation Mode of Huawei GaussDB 200 6.5.1 AGD_OPE v0.6)
CPU	x86_64 Dual socket 24 cores Intel processor 2.6 GHz
Memory	256 GB
Hard disk	1.2 TB disk space
OS type and version	SUSE Linux Enterprise Server 12 (SUSE 12) SP3, x86_64
Software	Python v2.7.5
Clients	gsql 6.5.1, JDBC, ODBC
Server Tools	All tools listed in section 7.3 of GaussDB 200 6.5.1 Product Documentation 09.pdf)
Firewall	Protection of the TOE interfaces (see section 6.7 Configuring Firewalls of Huawei GaussDB 200 6.5.1 AGD_PRE v0.7)

EVALUATION RESULTS

The product Huawei GaussDB 200 version 6.5.1 build e3690037 has been evaluated against the Security Target: Huawei GaussDB 200 6.5.1 Security Target (version: 0.7, date: 2021-07-02).

All the assurance components required by the evaluation level EAL2 + ALC_FLR.2 have been assigned a "PASS" verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2 + ALC_FLR.2, as defined by Common Criteria for Information Technology Security Evaluation Version 3.1 R5 and the Common Methodology for Information Technology Security Evaluation Version 3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- The fulfillment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.
- The application of all firewall rules according to the preparative procedures are extremely important to maintain the security in the TOE environment denying all external access to the TOE.
- The application of the TLS encryption after the installation procedures is critical to maintain the communication secure and safeguard the TOE assets.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product DEKRA Testing and Certification S.A.U., a positive resolution is proposed.

During the evaluation, the ITSEF noticed that **the TOE provides, at least, 21 non-declared interfaces** (TSFI), that is, services listening on several ports. As these accesses are not declared in the TOE documentation and **they could provide information related to the TOE**, the vendor fixed this providing **firewall rules in order to mitigate these vulnerabilities.** These firewall rules are indicated in *6.7 Configuring Firewalls* in document *Huawei GaussDB 200 6.5.1 AGD_PRE* (version 0.6, 18-03-2021).

Additionally, although GaussDB 200 supports TLSv1.1 and TLSv1.2, **only TLSv1.2 with some specific ciphersuites** are included in the scope of this certification. Therefore, the user should follow the steps in section *6.8 Configuring TLS protocol* in order to configure TLS accordingly.

In general,

- for a secure installation of the TOE, the user should follow the TOE guidelines (see the Security Target, section *2.4.2.2 TOE Guide*). Special attention have to be paid to the section "*6 TOE Secure Installation*" in the guide "*HUAWEI GaussDB 200 6.5.1 AGD_PRE V0.7.pdf*", and
- for a secure operation of the TOE, the user should also follow the TOE guidelines (see the Security Target, section *2.4.2.2 TOE Guide*). Special attention have to be paid to the section "*7. Security requirements*" in the guide "*HUAWEI GaussDB 200 6.5.1 AGD_OPE.pdf*".

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: Huawei GaussDB 200 6.5.1 Security Target (version: 0.7, date: 2021-07-02).

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components selected.