LGAI Technological Center S.A.
Campus UAB – Ronda de la Font del Carme, s/n
08193, Bellaterra, Barcelona (Spain)
CIF: A63207492
Tel: +34 93 567 20 00
www.applus.com

Certification Report

Huawei OceanStor Hybrid Flash Storage System 6.1.8

Product name & version:	**Huawei OceanStor Hybrid Flash Storage System 6.1.8**
Developer:	Huawei Technologies Co., Ltd.
Certificate ID:	EUCC-3096-2026-003
Internal File ID:	EUCC-2025-003
Project code:	EUCHUA001
Release Date:	20/10/2026
Author:	José Carlos Andreu Galán
Approver:	Núria Carrió Misas

Version Control

Version	Date	Description
1.0	20/10/2026	First release of the Certification Report.

Report created with template TEMCER023_Certification Report Template, version 2.0.

Contents

1 Introduction 4
2 Evaluated Product Information 5
3 Executive Summary 6
4 TOE description 8
4.1 Scope and Boundaries 8
4.2 Summary of the Security Target 9
4.3 Security Policies 10
4.4 Architectural information 10
4.5 TOE components 11
4.6 Assumptions and Operational Environment 12
4.7 Lifecycle management processes and production facilities 12
4.8 Supplementary Cybersecurity information and Vulnerability management processess 12
5 Evaluation Summary 13
5.1 Assessment against each assurance requirement 14
5.2 Documentation 15
5.3 Evaluated configuration 15
5.4 Testing approach and depth 15
5.5 State of the art documents and evaluation criteria used 15
5.6 Vulnerability Analysis and Penetration Testing 15
6 Evaluation and Certification Results 17
7 Mark and Label 17
8 Comments and Recommendations from Certification Body 18
9 Annex 19
10 Bibliography 19

1 Introduction

This report documents the evaluation and certification process of: Huawei OceanStor Hybrid Flash Storage System 6.1.8 against the *Common Criteria for Information Technology Security Evaluation Version 2022, applying CC:2022 and CEM:2022 Errata v1.2.* The evaluation was conducted by Applus+ Laboratories (LGAI Technological Center S.A.) in accordance with the requirements of EUCC scheme using Common Criteria Evaluation methodology.

This document constitutes the Certification Report for the certification of the product: Huawei OceanStor Hybrid Flash Storage System 6.1.8, requested on 22/12/2025, and evaluated by Applus+ Laboratories (LGAI Technological Center S.A.), as detailed in the Evaluation Technical Report *CCEHUA001-ETR-M0* [ETR].

Developer/manufacturer:	Huawei Technologies Co., Ltd.
Name and Contact:	*Fuchu Ma; support@huawei.com*
Certification Body	LGAI Technological Center, S.A. (Applus+ Laboratories)
NCCA	Autoridad Nacional de Certificación de la Ciberseguridad en España
Evaluation Laboratory	LGAI Technological Center, S.A. (Applus+ Laboratories)
Protection Profile	N/A
Common Criteria Version	Common Criteria 2022 Revision 1 (Errata v1.2)
Evaluation end date	September 30, 2026

2 Evaluated Product Information

The next table provides information about the identification of the TOE and the certification scope:

TOE Name and Version	Huawei OceanStor Hybrid Flash Storage System 6.1.8
TOE Product's components	**Software (Product Series):** - OceanStor_6.1.8_Software.tgz - OceanStor_lite_converged_6.1.8_Software.tgz
Security Target	Huawei OceanStor Hybrid Flash Storage System 6.1.8 Security Target version 0.15
Public Security Target	**Not Applicable**
Protection profile	**Not Applicable**
Patch Management	**Not Applicable**
Supplementary Cybersecurity information	***https://e.huawei.com/en/documents/products/storage/3c531822c31f442588d3e0e77862843c***
Life-cycle	Applicable SARs: ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, and ALC_FLR.2.
Evaluation Level	EAL2 augmented with ALC_FLR.2

3 Executive Summary

This Certification Report states the outcome of the EUCC security evaluation of the Huawei OceanStor Hybrid Flash Storage System software component. The developer of the TOE is Huawei Technologies Co., Ltd. Located in P.R. of China and they also act as the sponsor of the evaluation and certification.

The product is designed to carry mission-critical and general-purpose services of enterprises, financial institutions, and data centers (DCs).

They fully meet current data storage requirements, innovatively converge multiple databases, compute and storage, different generations of storage systems, cloud services, and warm and hot data storage, and provide customers with an ideal choice for agile service deployment in the future.

The TOE is an internal component supporting the Huawei OceanStor Hybrid Flash Storage System, providing the following major security features:

- Identification and authentication
- Authorization
- Access control
- Auditing
- Security management

The TOE (software based) runs on top of an OS (Euler OS) (non-TOE software) and hardware (non-TOE hardware) that are developed and maintained by the developer themselves. The TOE was evaluated as a Product Series as two different sets of software are included in the scope of evaluation. These two software sets present equivalent behavior regarding security functionality in scope, whose differences are based only on adaptation to running on different hardware platforms, but not on security related functions, as per the developer's Differential Analysis Report [DAR] and Testing Reuse Rationale [TRR].

The TOE has been evaluated by Applus+ Laboratories (LGAI Technological Center, S.A.) at the facilities located in Madrid, Spain. The evaluation was completed on September 30, 2026 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the EUCC as described in Commission Implementing regulation (EU) 2024/482.

The scope of the evaluation is defined by the Security Target [ST], which identifies assumptions made during the evaluation, the intended environment in which the TOE shall be running in, the security requirements, and the level of confidence (EAL - Evaluation Assurance Level) at which the product is intended to satisfy the security requirements.

Consumers of the Huawei OceanStor Hybrid Flash Storage System 6.1.8 software are advised to verify that their own environment is consistent with the security target, and to give consideration to the comments outlined in this certification report.

There are no special configuration requirements except for those defined in the user guidance. All users shall read, apply and install the TOE in the operational environment accordingly.

The summary of the threats and security policies which the Security Target [ST] defines:

- The threats defined in section 3.2 of the Security Target [ST] are the ones addressed by the TOE in its operational environment. The assumed level of expertise of an attacker for all identified threats is Basic.
- The Security Target [ST] defines the Organizational Security Policy defined (OSP) in section 3.3.

The results documented in the Evaluation Technical Report [ETR] for this TOE provide sufficient evidence that the TOE meets the requirements for the specified set of SARs and SFRs described in the Security Target [ST].

The claimed SARs for the evaluation (given by reference to an EAL2 augmented with ALC_FLR.2) are: ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2, AVA_VAN.2, and ALC_FLR.2.

The assurance level is recognized by article 52 of [CSA] as “Substantial”.

The evaluation was conducted using the CC:2022 and CEM:2022 Release 1, applying the corrections introduced by CC:2022 and CEM:2022 Errata version 1.2.

The TOE does not claim conformance to any Protection Profile.

Applus+ CyberCB (LGAI Technological Center, S.A.) as a Certification Body for EUCC certification activities notified by the *Autoridad Nacional de Certificación de la Ciberseguridad en España,* declares that the evaluation activities meet all conditions for the issuing an EUCC certificate which will be published in the EUCC Certified Products list from ENISA. Note that the certification results apply only to the specific version of the product(s) as evaluated.

The initial date of issuance of the certificate was October 20th 2026, with a validity period of 5 years. The certificate unique identifier is EUCC-3096-2026-003.

4 TOE description

4.1 Scope and Boundaries

The scope of the TOE is defined in section 1.4 of the Security Target [ST], where the physical scope and logical scope are defined. The following figure depicts the scope of the TOE deployed within its operational environment:

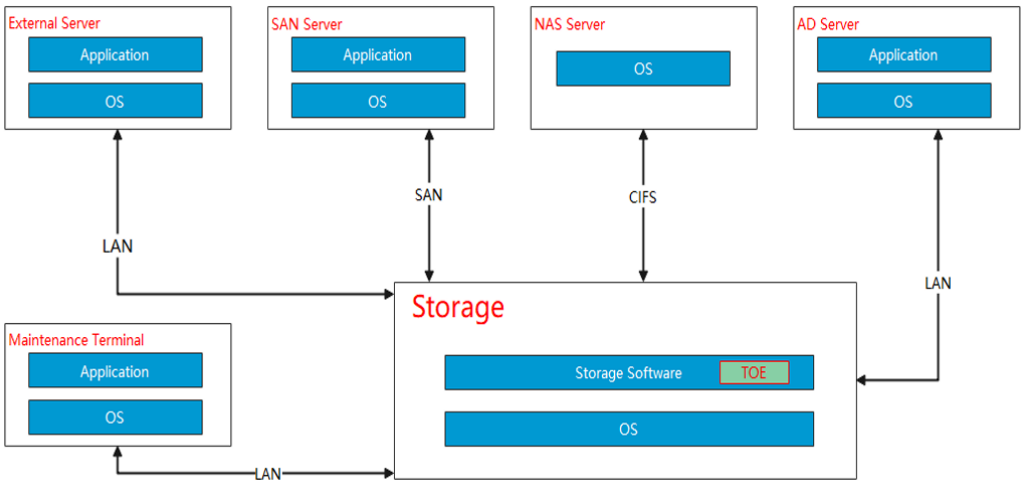


FIGURE 1 TOE BOUNDARIES

The TOE boundary from a logical point of view is represented by the elements that are displayed with a red dotted box within the rectangle in the figure. The TOE consists of I/O Service, OMM, SYS CTRL subsystems. The following figure provides greater detail on the logical scope:

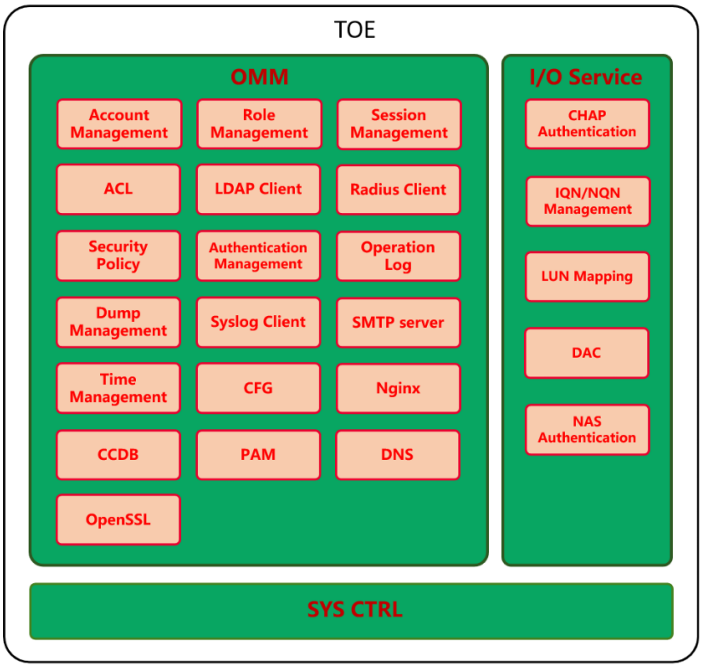


FIGURE 2 LOGICAL SCOPE OF THE TOE

From a logical perspective, as described in section 1.4.2 of [ST], the scope boundaries of the software are defined by the security functions that it implements. The functions can be grouped as the major security features of the TOE:

• Identification and Authentication: For user access, the TOE has two authentication modes, TOE provides identification and authentication support in case of local authentication. In remote authentication mode, the TOE does not support authentication and only obtains authentication results from the domain server.

For data access, the TOE provides SAN service and NAS service. In data access for SAN service, the available LUN is limited by the initiator. CHAP authentication is supported. for NAS service, the TOE maintains NTFS-Style files and provides CIFS protocol for access.

• Authorization: Authorization indicates that devices assign operation authorities to accounts according to their validity. The TOE implements authorization by a Role Based Access Control (RBAC) model.

• Access Control: The TOE supports filtering of incoming access to management interfaces. IP whitelist to limit access from IP addresses out of the list or limit an account's interface access methods.

• Auditing: The TOE generates audit records for security-relevant management actions and stores the audit records in the TOE.

• Security Management: Security functionality management includes authentication, access level, and management of security related data, including configuration profile and runtime parameters.

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

The Security Target states that:

- The TOE and its operational environment must be installed and operated in a physically secure location.
- The TOE administrators are non-hostile, are properly trained in the TOE usage and follow guidance.
- The TOE's operational environment provides a secure network to protect the data exchanged to and from the TOE.
- Assumes the hardware and the operating system function properly and that there are no vulnerabilities in the hardware platform.
- Assumes that the external servers, such as the NTP server, syslog server, AD server, RADIUS server, DNS server, and SMTP server, will provide correctly their related functions to the TOE.

4.2 Summary of the Security Target

The evaluated Security Target is titled Huawei OceanStor Hybrid Flash Storage System 6.1.8 Security Target Issue 0.15, dated 7th September 2026. This document will be publicly available at the EUCC Certification page. No sanitization of the ST has been performed.

The security target [ST] does not claim conformance to any Protection Profile. The claimed assurance level is EAL2 augmented with ALC_FLR.2.

4.3 Security Policies

The Security Target defines two Organizational Security Policies (OSP):

- P.DataCorruption: TOE users should avoid incorrect system accesses to avoid data corruption, and non-TOE users / applications should avoid unauthorized data modifications. Inadequate configurations through LAN should be avoided.
- P.UnauthorizedSubject: Applications or servers with no access rights should not be able to read/write data through SAN/NAS to prevent unintended user data access.

4.4 Architectural information

4.4.1 Logical architecture

Security audit

The TOE generates audit records for security-relevant management actions and stores the audit records in the TOE.

By default, all commands for configuring along with a timestamp when they are executed are logged

The TOE allows the review of logs.

The TOE has means to export to external entities (SFTP) the logs.

Identification and Authentication

For user access, the TOE has two authentication modes, TOE provides identification and authentication support in case of local authentication. In remote authentication mode, the TOE does not support authentication and only obtains authentication results from the domain server. The remote authentication endpoints can be an Active Directory server or a Radius server.

In local authentication mode, the TOE performs user identification and authentication using locally stored credentials. The supported authentication mechanisms are password-only authentication, SSH key-pair authentication, and password combined with a one-time password (OTP) sent by email.

For data access, the TOE provides SAN service and NAS service. In data access for SAN service, the available LUN is limited by the initiator. CHAP authentication is supported. for NAS service, the TOE maintains NTFS-Style files and provides CIFS protocol for access.

Authorization

The TOE controls access by the RBAC (Role Based Access Control) model. The TOE provides 9 default roles with pre-existing permission definitions. These pre-defined roles cannot be modified or deleted. However, authorized administrators can create and customize new roles based on their needs.

Access Control

- The TOE support filtering to management interfaces. The filtering can be based on the IP address of the incoming connection or based on the user's account configured access methods (e.g. not all users of the TOE are allowed to use the same interfaces). DAC policies are used to control the file access when using the CIFS protocol.

Security management

The following management can be performed on the TOE:

- Authentication, access level, and management of security related data, including configuration profile and runtime parameters.
- Management of users and user attributes, including user credentials.
- Management of the user policy, including user name length, password complexity, failure policy, and lockout policy.
- Management of IP whitelist and login method.
- Management of the TOE's time.

4.4.2 Physical architecture

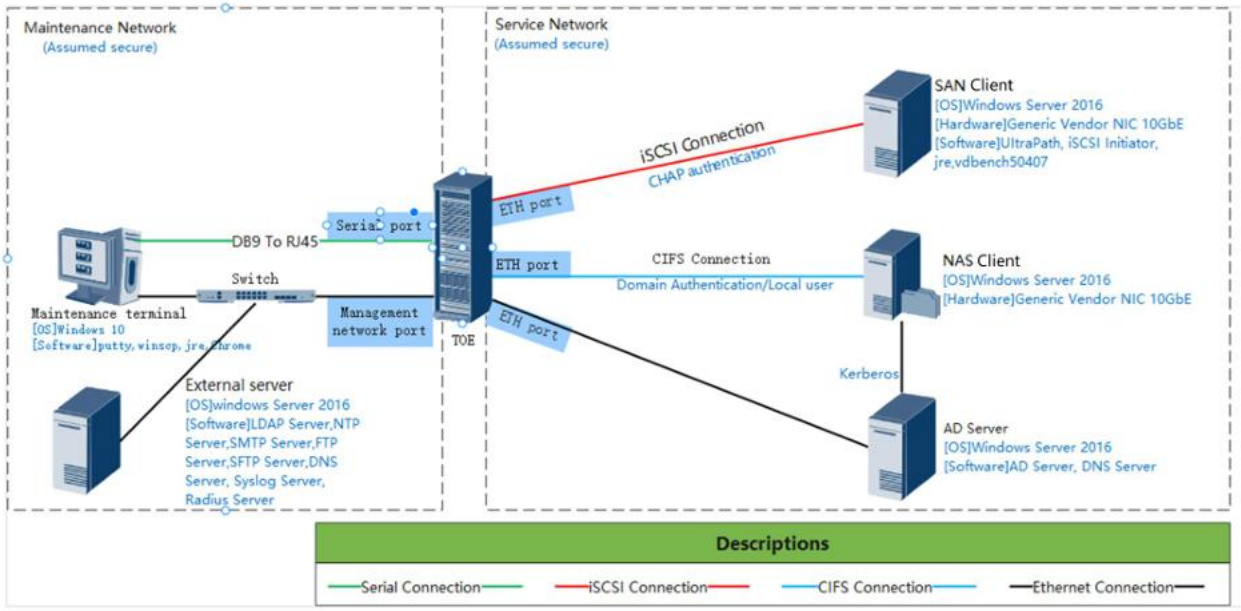


FIGURE 3 PHYSICAL ARCHITECTURE OF THE TOE

The TOE (software) is expected to be installed on dedicated hardware and connected to its environment in a similar scheme to the one depicted in the figure above.

4.5 TOE components

The TOE components as defined in section 1.4.1 of the Security Target:

Type	Item	Version

Software	OceanStor_6.1.8_Software.tgz	6.1.8
	OceanStor_lite_converged_6.1.8_Software.tgz	6.1.8
Digital Signature	OceanStor_6.1.8_Software.tgz.asc	6.1.8
	OceanStor_lite_converged_6.1.8_Software.tgz.asc	6.1.8
Product guidance	OceanStor 6.1.8 Error Code	01
	OceanStor 6.1.8 Command Reference Manual	01
	OceanStor 6.1.8 Event	01
	OceanStor 6.1.8 REST Interface Reference	03
	OceanStor 6.1.x & V700R001 Administrator Guide	14
	OceanStor 6.1.x & V700R001 Initialization Guide	14
	OceanStor 6.1.x & V700R001 Security Configuration Guide	15
	Huawei OceanStor Hybrid Flash Storage System 6.1.8 AGD_PRE_User	0.4
	Huawei OceanStor Hybrid Flash Storage System 6.1.8 AGD_OPE	0.7

4.6 Assumptions and Operational Environment

The assumptions defined by the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives that are to be fulfilled by the TOE environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the Security Target [ST].

The product guidance, as provided in section 4.5 contains necessary information about the usage of the TOE and the configuration of its environment to fulfill all the Assumptions as described in the Security Target [ST].

4.7 Lifecycle management processes and production facilities

Not applicable for this evaluation. See ALC in section 5.1.

4.8 Supplementary Cybersecurity information and Vulnerability management processess

The following link was provided to fulfill with the required supplementary cybersecurity information as referred to in Article 55 of Regulation (EU) 2019/881:

https://e.huawei.com/en/documents/products/storage/3c531822c31f442588d3e0e77862843c

Subsequent links provide more information about compliance with:

- a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services.

  https://support.huawei.com/hedex/hdx.do?docid=EDOC1100233756&id=oceanstor_18x10_001

  https://support.huawei.com/hedex/hdx.do?docid=EDOC1100233761&id=oceanstor_5x10_031

- b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates:

  https://www.huawei.com/en/declarations/lifecycle-management-letter

- c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers:

  https://www.huawei.com/en/psirt/report-vulnerabilities

- d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories:

  https://securitybulletin.huawei.com/carrier/en/security-advisory

Note: From principal link it is possible to access the rest of supplementary information.

5 Evaluation Summary

LGAI Technological Center, S.A. is acting as both the ITSEF (Evaluation Laboratory) and CB (Certification Body) in the current certification process, under the notification of *Autoridad Nacional de Certificación de la Ciberseguridad en España.*

The CAB point of contact is: cybercert@applus.com

Evaluation Laboratory:	LGAI Technological Center, S.A. (Applus+ Laboratories)
Conformity Assessment Body	LGAI Technological Center, S.A. (Applus+ Laboratories)
National Cybersecurity Certification Authority	Autoridad Nacional de Certificación de la Ciberseguridad en España
Assurance components:	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2, AVA_VAN.2, and ALC_FLR.2
Protection Profile used	Not applicable
Common Criteria Version used	CC:2022 Release 1

Evaluation end date	September 30th, 2026

5.1 Assessment against each assurance requirement

ASE

The specific assurance requirements evaluated for the ASE class are**:** ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, and ASE_TSS.1

The [ST] contains all relevant information to comply with all the families according to EAL2 augmented with ALC_FLR.2.

ADV

The specific assurance requirements evaluated for the ADV class are**:** ADV_ARC.1, ADV_FSP.2, ADV_TDS.1

The developer demonstrated compliance by providing evidence regarding the Security Architecture of the TOE, its interfaces with complete summary through the functional specification and the TOE design decomposed in subsystems.

AGD

The specific assurance requirements evaluated for the AGD class are: AGD_OPE.1 and AGD_PRE.1

The evaluation of the user guidance (AGD) showed that the provided user guidance gives clear instructions on how to perform the acceptance procedures, installation and operation of the TOE such that its security claims are maintained. The evaluator concludes that the requirements of the assurance class AGD are met by the TOE.

ALC

The specific assurance requirements evaluated for the ALC class are: ALC_CMC.2, ALC_CMS.2, ALC_DEL.1 and ALC_FLR.2

The evaluation of the lifecycle related aspects (ALC) successfully verified the use of the CM system, parts of the TOE CM coverage and delivery procedures. The evaluator concluded that all the requirements for the ALC class are met.

ATE

The specific assurance requirements evaluated for the ATE class are: ATE_COV.1, ATE_FUN.1, ATE_IND.2

The evaluation of the functional testing campaign consisted in the repetition of all the test plan provided by the developer and a set of independent tests to provide greater assurance of correct operation of the security functions. The repetition of developer's test plan and the execution of the independent tests was performed remotely by the evaluator.

The evaluator concludes that all requirements of the assurance ATE class are met.

AVA

The specific assurance requirements evaluated for the AVA class are AVA_VAN.2.

The evaluator performed a public search of vulnerabilities for the TOE, its related third-party components and for vulnerabilities in components of its operational environment which could have an impact on the TOE's scope. The vulnerability analysis resulted in the developer devising a series of penetration tests. The tests were focused on exploiting logical flaws through the network interfaces of the TOE. The AVA related activities were conducted in full compliance with the assurance requirements set for AVA_VAN.2. As such, the evaluator demonstrates that the TOE is resistant to an attacker possessing basic attack potential.

5.2 Documentation

See section 4.5, product guidance row in the table.

5.3 Evaluated configuration

The evaluated configuration is based on the [AGD_PRE] guidance and all the accompanying product guidance in scope. The evaluator tested the TOE with its configuration in accordance to the descriptions provided in the Security Target [ST].

5.4 Testing approach and depth

The evaluator performed the installation and configuration in its operational environment according to the steps provided in the installation and operation manuals. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to the Security Target [ST].

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarized in the [ETR], with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its Security Target [ST] and in the functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

5.5 State of the art documents and evaluation criteria used

No EUCC State of the art documents were used for this evaluation.

However, the following EUCC guideline documents were applied:

- ENISA, Agreed Cryptographic Mechanisms version 2 (May 2025) [ACM]
- ENISA, Evaluation methodology for Product Series, version 1, July 2025 [PS]

5.6 Vulnerability Analysis and Penetration Testing

The evaluator performed the Vulnerability Analysis and the Penetration Testing following AVA_VAN.2 SAR and its associated methodology defined in [CEM].

The evaluator did not find deviations from the expected results during the penetration testing campaign.

The evaluator conducted a public domain vulnerability search up until 15/09/2026 to check whether any new vulnerabilities may affect the TOE.

The total test effort expended by the evaluators was approximately 2 weeks. During that test campaign, 100% of the time was spent on logical tests.

These activities were conducted successfully, demonstrating that the TOE is resistant to an attacker possessing Basic attack potential as defined for AVA_VAN.2.

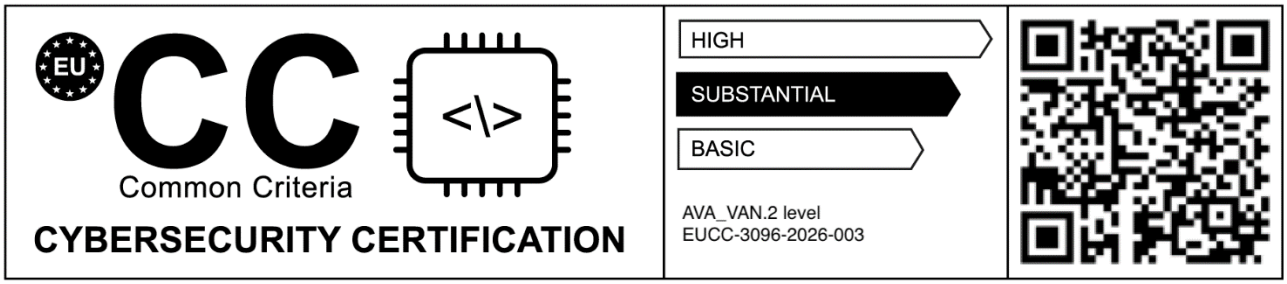
6 Evaluation and Certification Results

The ETR [ETR] did not reuse any previous results for the evaluation, as this was a first-time evaluation for this Product Series evaluation.

The Security Target does not claim conformance to a Protection Profile, referencing specific assurance requirements ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2, AVA_VAN.2, and ALC_FLR.2.

Based on the above evaluation results presented in the ETR [ETR], the evaluation laboratory concluded the Huawei OceanStor Hybrid Flash Storage System 6.1.8 to be CC Part 2 Conformant, CC Part 3 conformant. The obtained results imply that the product satisfies the security requirements set in the Security Target [ST]. The assurance level defined in [ST] is recognized by article 52 of [CSA] as “Substantial”.

7 Mark and Label



8 Comments and Recommendations from Certification Body

Considering the obtained evidences, the [ETR] from the laboratory and the own conclusions from the Certification Body, a positive resolution is proposed.

The certifier recommends TOE consumers to analyze the Security Target [ST] to verify that the security problem definition and the security functional requirements meet potential consumer security needs and recommends to strictly follow the guidance referenced in the Security Target [ST].

9 Annex

Not applicable.

10 Bibliography

[ACM] ENISA, «Agreed Cryptographic Mechanisms version 2,» May 2025.

[PS] ENISA, «Evaluation methodology for Product Series, version 1» July 2025.

[EUCC] European Parliament and of the Council, «Regulation (EU) 2024/482 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based sybersecurity scheme (EUCC),» 31 January 2024.

[CSA] European Parliament and of the council, «Regulation 2019/881 on ENISA and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act),» 17 April 2019.

[ETR] Applus+ Laboratories, «Evaluation Technical Report (Huawei OceanStor Hybrid Flash Storage System 6.1.8) version M0».

[ST] Huawei Technologies Co., Ltd., «Huawei OceanStor Hybrid Flash Storage System 6.1.8 Security Target version 0.15».

[CEM] «Common Methodology for Information Technology Security Evaluation, version 2022 revision 1,» November 2022.

[AGD_PRE] Huawei Technologies Co., Ltd., « Huawei OceanStor Hybrid Flash Storage System Software 6.1.8 AGD_PRE_User version 0.4».

[DAR] Huawei Technologies Co., Ltd., «Huawei OceanStor Hybrid Flash Storage System 6.1.8 DIFFERENTIAL ANALYSIS REPORT (DAR) version 0.5».

[TRR] Huawei Technologies Co., Ltd., «Huawei OceanStor Hybrid Flash Storage System 6.1.8 TESTING REUSE RATIONALE (TRR) version 0.4».