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

H3C Wireless Controllers and Access Points "TOE hardware: H3C WX5800 Series, WX2800 Series, WX3800 Series Wireless Controllers and WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series Access Points TOE firmware: H3C Comware Software, Version 7.1.064, Release 5484P23; H3C Comware Software, Version 7.1.064, Release 5817P33; H3C Comware Software, Version 9.1.061, ESS1404P23; H3C Comware Software, Version 7.1.064, Release 2617P33"

Product name & version:	**H3C Wireless Controllers and Access Points** *(see version below)*
Developer:	New H3C Technologies Co., Ltd
Certificate ID:	EUCC-3096-2026-001
Project code:	EUCH3C001
Release Date:	02/07/2026
Author:	José Carlos Andreu Galán
Approver:	Núria Carrió Misas

Version Control

Version	Date	Description
1.0	30/06/2026	First release of the certification report
1.1	02/07/2026	Certification ID modification

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 10
4.3 Security Policies 10
4.4 Architectural information 10
4.5 TOE components 12
4.6 Assumptions and Operational Environment 12
4.7 Lifecycle management processes and production facilities 13
4.8 Supplementary Cybersecurity information and Vulnerability management processes 13
5 Evaluation Summary 14
5.1 Assessment against each assurance requirement 14
5.2 Documentation 16
5.3 Evaluated configuration 17
5.4 Testing approach and depth 17
5.5 State of the art documents and evaluation criteria used 17
5.6 Vulnerability Analysis and Penetration Testing 17
6 Evaluation and Certification Results 18
7 Mark and Label 18
8 Comments and Recommendations from Certification Body 19
9 Bibliography 20

1 Introduction

This report documents the evaluation and certification process of H3C Wireless Controllers and Access Points against the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5. 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 H3C Wireless Controllers and Access Points, requested on 18/12/2026, and evaluated by Applus+ Laboratories (LGAI Technological Center S.A), as detailed in the Evaluation Technical Report *CCBH3C001-ETR-M1* [ETR].

Developer/manufacturer	New H3C Technologies Co., Ltd
Name and Contact	Sun Yanan (*viola_sun@h3c.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	Network Devices Protection Profile 3.0e
Common Criteria Version	Common Criteria 3.1 release 5
Evaluation end date	June 12th, 2026

2 Evaluated Product Information

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

TOE Name	H3C Wireless Controllers and Access Points
TOE Version	TOE hardware: H3C WX5800 Series, WX2800 Series, WX3800 Series Wireless Controllers and WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series Access Points TOE firmware: H3C Comware Software, Version 7.1.064, Release 5484P23; H3C Comware Software, Version 7.1.064, Release 5817P33; H3C Comware Software, Version 9.1.061, ESS1404P23; H3C Comware Software, Version 7.1.064, Release 2617P33
Security Target	H3C WX5800 Series, WX2800 Series, WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series and WX3800 Series Wireless Controllers and Access Points Security Target v3.4
Sanitized Security Target	H3C WX5800 Series, WX2800 Series, WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series and WX3800 Series Wireless Controllers and Access Points Security Target Lite v3.4
Protection profile	Network Devices Protection Profile 3.0e with Functional Package for Secure Shell (SSH) version 1.0 and PP-Module for Wireless Local Area Network (WLAN) Access System Version: 1.0
Patch Management	**Not Applicable**
Supplementary Cybersecurity information	***https://www.h3c.com/en/Support/Online_Help/psirt/***
Life-cycle	ALC_CMS.1, ALC_CMC.1. No production sites in scope.
Evaluation Level	NDcPP evaluation level (SAR equivalent to EAL1 + ASE_SPD.1)

3 Executive Summary

This Certification Report states the outcome of the EUCC security evaluation of the H3C Wireless Controllers and Access Points Product Series. The developer of the TOEs is New H3C Technologies Co., Ltd located in P.R. China and they also act as the sponsor of the evaluation and certification.

The TOE combines Wireless Access Controllers and Access Points developed by H3C to create a Wireless LAN Access System TOE. The wireless Access Controllers (ACs) are wireless switch appliances that provide a wide range of security services and features including wireless network mobility, security, centralized management, auditing, authentication, and remote access. The access point (AP) appliances service wlan clients.

The hardware of the TOE is composed of one Access Controller, a physical network device that supports modules that serve to offer a wide range of network ports varying in number, form factor (copper or fiber), and performance; and at least one Access Point, a physical network device which provides the connection point between wlan client hosts and the wired network. The software of the TOE executes entirely within the TOE hardware.

The H3C Wireless Controllers and Access Points are capable of many networking functions. However, this evaluation only addresses the functions that provided for the security of the TOE itself, excluding any traffic that may traverse it.

The different models included in the product series differ in number and type of network connections and their processing capacities. Although different firmware versions are included in the series, the provided evidence and the [ETR] confirm that their security capabilities are equivalent.

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 June 12, 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 H3C Wireless Controllers and Access Points 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 3.1 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 Organizational Security Policy defined (OSP) is that the TOE shall present an informational banner to a user accessing its management interfaces, as defined in section 3.3 of the Security Target [ST].

The results documented in the evaluation technical report [ETR] for this product series provide sufficient evidence that the TOE meets the requirements for exact conformance to the collaborative Protection Profile for Network Devices 3.0e [NDcPP3.0e] in combination with Functional Package for Secure Shell (SSH) v1.0 [FPSSH1.0] and the PP-Module for Wireless Local Area Network (WLAN) Access System Version: 1.0 [PPMWLAN1.0]. The Protection Profile [NDcPP3.0e] references specific Security Assurance Packages (SARs): ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1 and AVA_VAN.1.

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

The evaluation was conducted using the ISO/IEC 18045:2008, Common Criteria Evaluation Methodology for Information Security Evaluation (CEM) v3.1 revision 5.

Applus+ CyberCB (LGAI Technological Center, S.A.) as a Certification Body for EUCC certification activities 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 30th June, 2026, with a validity period of 5 years. The certificate unique identifier is EUCC-3096-2026-001.

4 TOE description

4.1 Scope and Boundaries

The scope of the TOE is defined by the Network Devices Protection Profile 3.0e to which the TOE is conformant to. The TOE is a product series composed of different WLAN Access Points and Access Controllers with their respective hardware and software elements identified in the following table:

Family	Type	Product Series	Models	Firmware
Comware V7	Access Controller	WX5800 Series	WX5860X	H3C Comware Software, Version 7.1.064, Release 5484P23
		WX2800 Series	WX2880X, WX2860X, WX2812X-PWR	H3C Comware Software, Version 7.1.064, Release 5817P33
	Access Point	WA6500 Series	WA6520, WA6526, WA6526E, WA6520H	H3C Comware Software, Version 7.1.064, Release 2617P33
		WA7200 Series	WA7220-HI	H3C Comware Software, Version 7.1.064, Release 2617P33
		WA7300 Series	WA7320i, WA7338-HI, WA7330X, WA7330i, WA7320XE, WA7322H-HI	H3C Comware Software, Version 7.1.064, Release 2617P33
		WA7500 Series	WA7539	H3C Comware Software, Version 7.1.064, Release 2617P33
		WA7600 Series	WA7638, WA7620CE	H3C Comware Software, Version 7.1.064, Release 2617P33
Comware V9	Access Controller	WX3800 Series	WX3840X, WX3820X	H3C Comware Software, Version 9.1.061, ESS 1404P23

The TOEs have the consideration of distributed TOEs as per the definition provided in the Protection Profile and a single TOE is the combination of at least one Access Controller Unit and one Access Point Controller with their respective evaluated H3C Comware software.

The TOEs included in the scope of evaluation claim conformance to the Network Devices Protection Profile 3.0e, PP-Module for Wireless Local Area Network (WLAN) Access System Version: 1.0 and Functional Package for Secure Shell (SSH) v1.0.

The TOE's functionalities include: remote secure management over SSH, management over a local interface (serial), secure external logging support (syslog over IPSec), secure time synchronization (NTP over IPSec), Wireless connectivity and management, delegated external authentication over an IPSec channel.

The major security features are the following:

- Security audit

- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels.
- Communication

The scope of evaluation excludes explicitly any traffic that may traverse the TOE or any function not explicitly stated as included in scope of evaluation. Moreover, the following protocols are not part of the evaluated configuration:

- FTP
- HTTP(S)
- SNMP
- TACACS
- Telnet
- Bash shell
- TFTP
- BGP
- RIP/RIPng
- OSPF
- STP

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 must be installed and operated in a secure location.
- The TOE does not protect against non-management network traffic. Additionally, attacks as Denial of Service are not in scope of evaluation.
- Administrators are diligent, trained, keep credentials secure and are not hostile to the TOE.

4.2 Summary of the Security Target

The evaluated Security Target is titled H3C WX5800 Series, WX2800 Series, WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series and WX3800 Series Wireless Controllers and Access Points Security target v3.4. This document will be publicly available at the EUCC Certification page. The certifier validated that the published document [ST_Lite] has been sanitized before being published in accordance with point V.2 of Annex V of Regulation (EU) 2019/881.

The Security Target claims exact conformance to the Collaborative Protection Profile for Network Devices 3.0e [NDcPP3.0e] in combination with Functional Package for Secure Shell (SSH) v1.0 [FPSSH1.0] and the PP-Module for Wireless Local Area Network (WLAN) Access System Version: 1.0 [PPMWLAN1.0].

The claimed SARs for [NDcPP3.0e] are: ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1 and AVA_VAN.1.

4.3 Security Policies

The Organizational Security Policy defined (OSP) is that the TOE shall present an informational banner to a user accessing its management interfaces, as defined in section 3.3 of the Security Target [ST].

4.4 Architectural information

4.4.1 Logical architecture

Security audit

The TOE generates an audit record for each auditable event. Each security relevant event has an associated timestamp, description, outcome and associated identity (if applicable to the event). The administrator can configure the auditable events and audit data storage. The TOE overwrites oldest logs when audit storage is full and has the capability of sending the audit trail to a remote server over a trusted channel protected with IPSec.

Cryptographic support

The TOE provides cryptographic services in support of the remote interfaces. Remote management can be performed via SSHv2. IPSec is used to provide security to NTP, to external authentication services and syslog. TLS 1.2 and DTLS 1.2 for the internal communication channels between the Access Controllers and Access Points.

Identification and authentication

The TOE provides authentication services for administrative users willing to connect to the TOE's CLI interface. Identification and authentication are mandatory before a user can interact with the TSF. The TOE is configured to require a minimum of 15 characters that prevents the use of weak passwords. The TOE is able to lock temporally a user based on failed authentication attempts. Password-based authentication can be used both on local console and remote console over SSHv2. Remote console also accepts authentication based on public-key cryptography.

Security management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection.

Protection of the TSF

The TOE protects against interference and tampering by untrusted entities by implementing identification, authentication, and access controls to limit configuration to authorized administrators. The TOE prevents the reading of cryptographic keys and passwords. The software does not allow for general purpose computing, only for the intended network management functionalities.

The TOE provides secure update functionality, requiring each update to be authenticated prior its installation.

The TOE performs self-tests at boot time to confirm its correct operation.

TOE access

The TOE can terminate inactive sessions after an authorized administrator configurable time period. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session. The administrators can also terminate their own sessions by exiting the CLI.

The TOE can display an authorized administrator specified content on a banner in the CLI management interface before the user is identified and authenticated.

Trusted path/channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 for remote CLI access. The TOEs allow to connect to NTP, syslog and authentication services over IPSec connections.

The TOE allows non-administrative connections to other networks via a Wireless LAN interface (Wi-Fi) provided by the Access Points. The identification and authentication of WLAN client credentials is supported by implementing IEEE 802.1X. The wireless communication between the Access Point and the WLAN client can be secured using WPA3-Enterprise, WPA2 Enterprise, WPA3-SAE or WPA2-PSK.

Communication

The TOE is a distributed product, being Access Controllers and Access Points two elements of the same TOE. However, placed in different nodes of the network and thus, subject to interference, tampering or eavesdropping of its communications. The different distributed parts of the TOE use TLS and DTLS protocols to protect their internal communications.

The figure in next section depicts the distributed architecture of the TOE. Mainly the Access Controller and the Access Points, showing example flows of data containing Management plane, control plane and data plane flows.

4.4.2 Physical Architecture

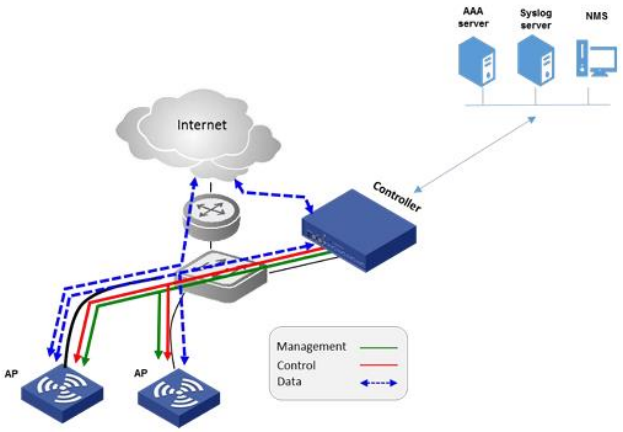


FIGURE 1 DISTRIBUTED ARCHITECTURE OF THE TOE

The next figure shows the TOE considering its operational environment and the potential users of it:

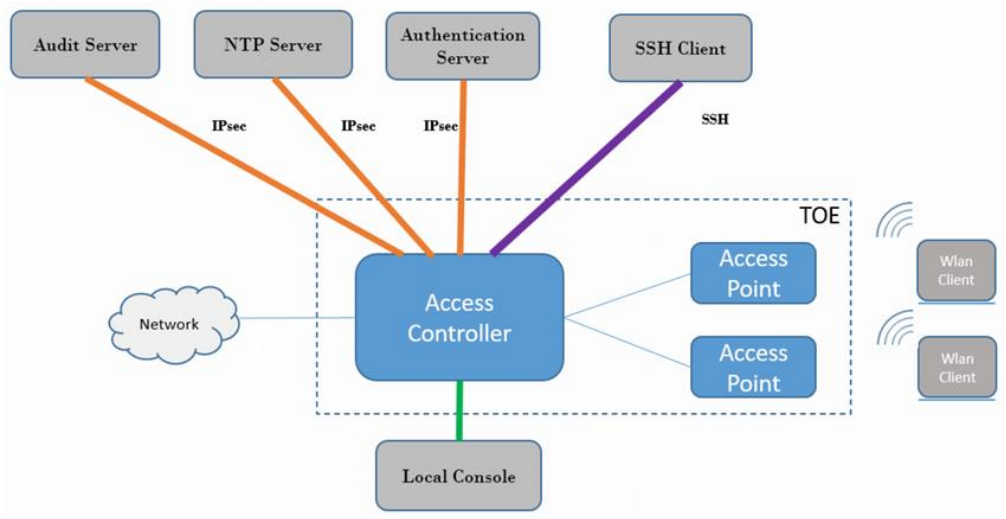


FIGURE 2 TOE AND OPERATIONAL ENVIRONMENT

4.5 TOE components

The physical scope of the TOE is composed of the hardware and its related software as provided in the table in section 4.1.

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 user guidance, as provided in section 4.8 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]. Certain aspects of the TOE's security functionality, in particular countermeasures against attacks, depend on accurate conformance to the user guidance of both software and hardware parts of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

4.7 Lifecycle management processes and production facilities

For the assurance level selected for the product certification (equivalent to EAL1 + ASE_SPD.1), no additional requirements are imposed beyond ensuring that the TOE has a unique identifier. This identifier ensures that there is no ambiguity regarding the specific instance of the TOE being evaluated.

The TOEs in the scope are identified by the combination of the hardware model and the version of the software.

4.8 Supplementary Cybersecurity information and Vulnerability management processes

The contact information for the H3C Wireless Controllers and Access Points was provided as: psirt@h3c.com

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

- 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://www.h3c.com/en/Support/Resource_Center/Technical_Documents/

- 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.h3c.com/en/Support/Policy_Dynamics/Management_Strategy/

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

  https://www.h3c.com/en/d_202305/1846951_294551_0.htm

- 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://www.h3c.com/en/Support/Online_Help/psirt/

Note: from link https://www.h3c.com/en/Support/Online_Help/psirt/ it is possible to access to the rest of the supplementary cybersecurity information.

5 Evaluation Summary

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

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	ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1 and AVA_VAN.1.
Protection Profile used	***PP Author:*** *Network Device international Technical Community (NDiTC);* ***PP Name:*** *Collaborative Protection Profile for Network Devices 3.0e (6 December 2023);* ***PP Identifier:*** *CCEVS-VR-PP-0099;* ***Certification Body and ITSEF of the certified PP****: NIAP (CB) and Leidos Common Criteria Testing Laboratory (ITSEF)* ***PP Assurance packages:*** *exact conformance to the previously mentioned SARs.*
Common Criteria Version used	3.1 revision 5
Evaluation end date	June 8, 2026

5.1 Assessment against each assurance requirement

ASE

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

The Security Target [ST] of the TOE claims exact conformance to the Collaborative Network Devices Protection Profile 3.0e. The scope of the TOE, Objectives for the Environment, Assumptions, Organizational Security Policies, Security Problem Definition, Security Assurance Requirements and Security Functional Requirements are based on the Protection Profile and are appropriately addressed.

The findings for the ASE related activities are well-documented and internally consistent. The laboratory applied the specific refinements and additional activities that the Supporting Document of the Protection Profile [SDNDcPP30e] mandates. No issues or deviations were identified.

ADV

The specific assurance requirements evaluated for the ADV class are: ADV_FSP.1

The ADV class related activities are limited to the Functional Specification (ADV_FSP.1). The assessment ensures that the TSF is described in terms of its externally visible interfaces, including purpose, usage, parameters and behavior, providing sufficient understanding of how a user is expected to exercise and operate the TOE interfaces. No issues or deviations were identified.

AGD

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

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure acceptance, installation, configuration, and operation of the TOE within its intended environment by its user roles. The guidance effectively helps preventing common misconfigurations and promotes correct and secure usage. The AGD related activities fulfill the assurance requirements by AGD_OPE.1 and AGD_PRE.1 with the additional application of refinements and activities set in the Supporting Document of the Network Devices Protection Profile [SDNcPP30e]. No issues or deviations were found.

ALC

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

The life-cycle support requirements for these assurance components ensure that the TOE is uniquely identified and that its configuration is defined in a consistent and unambiguous manner. The evaluation confirmed that the TOE identification is correct and unambiguous and that the list of configuration items list is complete, with each item clearly identified. The findings demonstrate that the ALC related activities satisfy the assurance requirements in accordance to the Protection Profile [NDcPP30e], with no issues or deviations identified.

ATE

The specific assurance requirements evaluated for the ATE class are: ATE_FUN.1

For the evaluator's independent testing, the approach described in the Supporting Document of the Protection Profile [SDNcPP30e] was followed. Functional testing was performed on a sample of the TOEs in the scope. The sample was selected in accordance to developer's DAR/TRR documentation and applying ENISA's Product Series evaluation methodology [ENISAPS]. All the executed tests in the test plan passed, therefore, confirming that the TOE satisfies the assurance requirements regarding the ATE class. No issues or deviations were identified.

AVA

The specific assurance requirements evaluated for the AVA class are: AVA_VAN.1

The evaluator performed a public vulnerability search. Additionally, the evaluator executed a number of verification and penetration tests using tools to verify if new potential vulnerabilities could impact any of the services running on the TOE in its evaluated configuration, as well as fuzzing tests on its network interfaces. The AVA related activities were performed in full compliance with the assurance requirements set for AVA_VAN.1 and with the Supporting Document of the Protection Profile [SDNDcPP30e]. As such, the it has been demonstrated that the TOE is resistant to an attacker with basic attack potential.

5.2 Documentation

Models	Item	Name	Version
WX5860X	Installation Guides	H3C WX5860X Access Controllers Installation Guide	6W105
	Command References	H3C WX5800X Series Access Controllers Command References	6W101
	Configuration Guides	H3C WX5800X Series Access Controllers Configuration Guides	6W101
WX2880X, WX2860X, WX2812X-PWR	Installation Guides	H3C WX2880X Access Controllers Installation Guide H3C WX2860X Access Controllers Installation Guide H3C WX2812X-PWR Access Controllers Installation Guide	6W101 6W101 5W103
	Command References	H3C WX2800X&WSG1800X Command References	6W101
	Configuration Guides	H3C WX2800X&WSG1800X Configuration Guides	6W101
WA6520	Installation Guides	H3C WA6520 Access Point Installation Guide	5W101
WA6526, WA6526E	Installation Guides	H3C Wi-Fi6 Indoor Access Points Installation Guide	6W104
WA6520H	Installation Guides	H3C WA6520H Access Point Installation Guide	5W100
WA7322H-HI	Installation Guides	H3C WA7322H-HI Access Point Installation Guide	AW100
WA7220-HI, WA7330i, WA7338-HI, WA7320i, WA7539, WA7638	Installation Guides	H3C Wi-Fi7 Indoor Access Points Installation Guide	5W109
WA7320XE	Installation Guides	H3C WA7320XE Access Point Installation Guide	5W100
WA7330X	Installation Guides	H3C WA7330X Access Point Installation Guide	5W101
WA7620CE	Installation Guides	H3C WA7620CE Access Point Installation Guide	6W105
WX3840X, WX3820X	Installation Guides	H3C WX3840X Access Controllers Installation Guide H3C WX3820X Access Controllers Installation Guide	6W105 6W105
	Command References	H3C WX3800X Series Access Controllers Command References	6W101
	Configuration Guides	H3C WX3800X Series Access Controllers Configuration Guides	6W101
[AGD_PREOPE]	Guidance Document	H3C Wlan Series Preparative and Operative Procedures	2.7

5.3 Evaluated configuration

The acceptance and installation procedures are given in section 5 of H3C Wlan Series Preparative and Operative Procedures [AGD_PREOPE].

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 product series testing has followed the ENISA Evaluation methodology for Product Series version 1. The ITSEF analyzed the DAR (Differential Analysis Report) and TRR (Testing Reuse Rationale) provided by H3C to prepare the independent testing strategy.

The evaluator has executed the set of tests defined in the Supporting Document of the Collaborative Protection Profile for Network Devices [SDNDcPP3.0e], as required by the Protection Profile [NDcPP3.0e] to which the Security Target [ST] claims conformance to. The evaluator found deviations from the expected results during the independent testing campaign which resulted in the developer applying changes to the software implementation.

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) [ENISAPS]

5.6 Vulnerability Analysis and Penetration Testing

The evaluator performed the Vulnerability Analysis and the Penetration Testing following AVA_VAN.1 SAR and its associated methodology defined in [CEM] with the additional activities and refinements set out in the Supporting Document of the Collaborative Protection Profile for Network Devices [SDNDcPP3.0e].

The evaluator found deviations from the expected results during the penetration testing campaign which resulted in the developer applying changes to the software implementation.

The evaluator conducted a public domain vulnerability search up until 12/03/2026 to check whether any new vulnerabilities may affect the TOE.

The total test effort expended by the evaluators was 2.5 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.1.

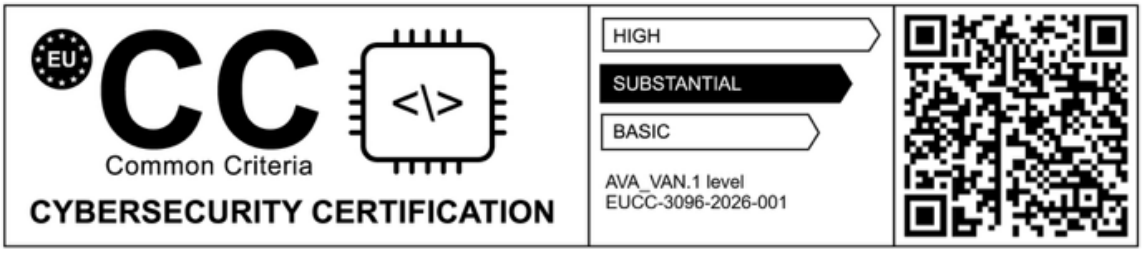
6 Evaluation and Certification Results

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 claims exact conformance to the Collaborative Protection Profile for Network Devices 3.0e [NDcPP3.0e] with the Functional Package for Secure Shell (SSH) v1.0 [FPSSH1.0] and the PP-Module for Wireless Local Area Network (WLAN) Access System Version: 1.0 [PPMWLAN1.0], referencing specific assurance requirements: ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1 and AVA_VAN.1.

Based on the above evaluation results presented in the ETR [ETR], the evaluation laboratory concluded that the H3C Wireless Controllers and Access Points with TOE hardware: H3C WX5800 Series, WX2800 Series, WX3800 Series Wireless Controllers and WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series Access Points TOE firmware: H3C Comware Software, Version 7.1.064, Release 5484P23; H3C Comware Software, Version 7.1.064, Release 5817P33; H3C Comware Software, Version 9.1.061, ESS 1404P23; H3C Comware Software, Version 7.1.064, Release 2617P33 to be CC Part 2 Extended, 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 by the Protection Profile [NDcPP3.0e] is recognised 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 Bibliography

[CC] «Common Criteria for Information Technology Security Evaluation, Parts 1, 2, and 3, version 3.1 revision 5,» April 2017.

[CEM] «Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5,» April 2017.

[NDcPP30e] «collaborative Protection Profile for Network Devices 3.0e,» December 2023.

[SDNDcPP30e] «Supporting Document for collaborative Protection Profile for Network Devices 3.0e,» December 2023.

[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.

[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.

[EUCCAMD1] European Parliament and of the Council, «Commission Implementing Regulation (EU) 2024/3144 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation,» 18 December 2024.

[EUCCAMD2] European Parliament and of the Council, «Commission Implementing Regulation (EU) 2025/2462 amending Implementing Regulation (EU) 2024/482 as regards defintions, ICT Product series certification, assurance continuity and state-of-the-art documents» 8 December 2025.

[ST] New H3C Technologies Co., Ltd, «H3C WX5800 Series, WX2800 Series, WA6500 Series, WA7200 Series version 3.4».

[ST_Lite] H3C WX5800 Series, WX2800 Series, WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series and WX3800 Series Wireless Controllers and Access Points Security Target Lite v3.4

[AGD_PREOPE] Preparative and Operative Procedures for CC NDPP Evaluated H3C Enterprise WX5800 Series, WX2800 Series, WA6500 Series, WA7200 Series, WA7300 Series, WA7500 Series, WA7600 Series and WX3800 Series version 2.7

[FPSSH10] NIAP, «Functional Package for Secure Shell (SSH) v1.0,» 13 May 2021.

[PPMWLAN10] NIAP, «PP-Module for Wireless Local Area Network (WLAN) Access System Version 1.0,» 31 March 2022.

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

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

[ETR] Applus+ Laboratories, Evaluation Technical Report (H3C Wireless Controllers and Access Points) version M1

EU