Reference: 2022-49-INF-4218- v1
Target: Pública
Date: 12.11.2024

Created by: I003
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2022-49**
TOE	**H3C Switch Series version 1.0**
Applicant	**91330100754408889H - New H3C Technologies Co., Ltd.**

References

[EXT-8176] Certification Request

[EXT-8732] Evaluation Technical Report

Certification report of the product H3C Switch Series version 1.0, as requested in [EXT-8176] dated 21/11/2022, and evaluated by SGS Brightsight Barcelona, S.L. (Unipersonal), as detailed in the Evaluation Technical Report [EXT-8732] received on 22/09/2023.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product H3C Switch Series version 1.0.

The TOE is a network device series that is connected to the network and has an infrastructure role within the network, it is composed of hardware and firmware that implements network layers 2 and 3 switching.

Developer/manufacturer: New H3C Technologies Co., Ltd..

Sponsor: New H3C Technologies Co., Ltd..

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

ITSEF: SGS Brightsight Barcelona, S.L. (Unipersonal).

Protection Profile: collaborative Protection Profile for Network Devices v2.2e, 23-03-2020.

Evaluation Level: Common Criteria v3.1 R5 (assurance package according to the [cPP_ND_22e]).

Evaluation end date: 26/08/2024

Expiration Date[1]: 08/11/2029

All the assurance components required by the evaluation level of the [cPP_ND_22e] have been assigned a "PASS" verdict. Consequently, the laboratory SGS Brightsight Barcelona, S.L. (Unipersonal) assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the [cPP_ND_22e] assurance level package, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product H3C Switch Series version 1.0, a positive resolution is proposed.

TOE SUMMARY

Each TOE appliance runs Comware software and has physical network connections to its environment to facilitate the switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

[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.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote (SSH) or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external audit server in the network environment, it can also be configured to work with a Network Time Server (NTP Server) and supports authentication against an external server. These three communication channels are protected with IPsec.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the assurance package defined in the [cPP_ND_22e], according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.1
	ASE_REQ.1
	ASE_SPD.1
	ASE_TSS.1
ADV	ADV_FSP.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.1
	ALC_CMS.1
ATE	ATE_IND.1
AVA	AVA_VAN.1

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

SECURITY FUNCTIONAL REQUIREMENTS
FAU_GEN.1
FAU_GEN.2
FAU_STG_EXT.1
FCS_CKM.1
FCS_CKM.2
FCS_CKM.4
FCS_COP.1/DataEncryption
FCS_COP.1/SigGen
FCS_COP.1/Hash
FCS_COP.1/KeyedHash
FCS_RBG_EXT.1
FCS_IPSEC_EXT.1
FCS_NTP_EXT.1
FCS_SSHS_EXT.1
FIA_AFL.1
FIA_PMG_EXT.1
FIA_UIA_EXT.1
FIA_UAU_EXT.2
FIA_UAU.7
FIA_X509_EXT.1/Rev
FIA_X509_EXT.2
FIA_X509_EXT.3
FMT_MOF.1/ManualUpdate
FMT_MTD.1/CoreData
FMT_MTD.1/CryptoKeys
FMT_SMF.1
FMT_SMR.2
FPT_SKP_EXT.1
FPT_APW_EXT.1
FPT_TST_EXT.1
FPT_TUD_EXT.1
FPT_STM_EXT.1
FTA_SSL_EXT.1
FTA_SSL.3
FTA_SSL.4
FTA_TAB.1
FTP_ITC.1
FTP_TRP.1/Admin

IDENTIFICATION

Product: H3C Switch Series version 1.0

Security Target: H3C S10500 Series, S7500 Series, S6500 Series, S5100 Series, S5500 Series, S12500 Series, S9800 Series and S6800 Series Switches Security Target (version 2.0).

Protection Profile: collaborative Protection Profile for Network Devices v2.2e, 23-03-2020.

Evaluation Level: Common Criteria v3.1 R5 (assurance package according to the [cPP_ND_22e]).

SECURITY POLICIES

The use of the product H3C Switch Series version 1.0 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 3 ("*Security problem Definition*"), that redirects to the section 4.3 ("*Organizational Security Policy*") of the [cPP_ND_22e].

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 3 ("*Security problem Definition*"), that redirects to the section 4.2 ("*Assumptions*") of the [cPP_ND_22e].

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product H3C Switch Series version 1.0, although the agents implementing attacks have the attack potential according to the Basic of [CPP_ND_22e] 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 Security Target, section 3 ("*Security problem Definition*"), that redirects to the section 4.1 ("*Threats*") of the [cPP_ND_22e].

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 4.2 ("*Security Objectives for the Operational Environment*"), that redirects to the section 5.1 ("*Security Objectives for the Operational Environment*") of the [cPP_ND_22e].

ARCHITECTURE

LOGICAL ARCHITECTURE

The main security functionalities provided by the TOE are the following:

- Security audit. The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and to send the logs to a designated external SYSLOG server to mitigate the possibility of losing audit records when available space becomes exhausted on the TOE. Locally stored audit records can be reviewed and managed by an administrator.
- Cryptographic support. The TOE includes a cryptographic module that provides key management and encryption/decryption features in support of higher level cryptographic protocols to provide a trusted path (e.g. for remote administration).
- Identification and authentication. The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console as well as network accessible interfaces (SSH) for interactive administrator sessions. The TOE supports the local definition of users with usernames and roles that can be authenticated with passwords or Public-Key. The TOE has policies to force the passwords to meet security requirements and can prevent brute-forcing it. The TOE supports roles to control permissions for administrators. Additionally, TOE can configure IPSEC connected RADIUS servers for authentication services to support e.g. centralized user management.
- Security management. The TOE provides Command Line (CLI) commands to access the wide range of security management functions. Security management commands are limited to administrators only after they have provided acceptable user identification and authentication data to the TOE.
- Protection of the TSF. The TOE protects the pre-shared keys, symmetric keys, and private keys from reading them by an unauthorized entity. The TOE stores the users or administrator passwords in non-plaintext form preventing them from reading. The TOE

performs self-tests on its power on to ensure its correct behaviour. The TOE verifies the packet before their installation and uses the digital signature.

- TOE access. The TOE can be configured to display advisory banners when user's login and will enforce an administrator defined inactivity timeout value after which an inactive session will be terminated, also allowing the capability of self-terminate its session for the administrator.
- Trusted path/channels. The TOE protects communication with an associated Audit server using IPSEC primarily to protect exported audit records. The TOE uses IPSEC to protect communications with the associated AAA server, primarily for authentication of accessing users. The TOE also provides the capability of remote administration via SSH.

PHYSICAL ARCHITECTURE

The physical scope of the TOE is detailed in the table below.

PRODUCT SERIES	MODELS	FIRMWARE
S10500 Series	S10506X, S10508X, S10510X	H3C Comware Software, Version 7.1.070, Release 7640P01
	S10506X-G, S10508X-G, S10512X-G	H3C Comware Software, Version 7.1.070, Release 7760P01
S7500 Series	S7503X, S7503E-M, S7506X-POE, S7506X-S, S7510X-POE	H3C Comware Software, Version 7.1.070, Release 7640P01
	S7503X-M-G, S7503X-G, S7506X-G-POE, S7510X-G-POE	H3C Comware Software, Version 7.1.070, Release 7760P01
S6500 Series	S6520X-18C-SI, S6520X-26C-SI, S6520X-26MC-UPWR-SI,S6520X-26MC-SI,S6520X-16ST-SI,S6520X-24ST-SI, S6520X-10XT-SI, S6520X-16XT-SI, S6520X-26XC-UPWR-SI, S6520X-54XC-UPWR-SI,S6520X-30HC-EI, S6520X-30QC-EI, S6520X-54HC-EI, S6520X-54QC-EI,S6520X-54HC-HI, S6520X-54QC-HI, S6520X-30HC-HI,S6520X-30QC-HI,S6520X-54HF-EI,S6520X-54HF-HI,S6520X-30HF-EI,S6520X-30HF-HI	H3C Comware Software, Version 7.1.070, Release 6628P92
S5100 Series	S5130S-28S-HI,S5130S-52S-HI,S5130S-28S-PWR-HI,S5130S-52S-PWR-HI,S5130S-28C-HI,S5130S-52C-HI,S5130S-28C-PWR-HI,S5130S-52C-PWR-HI	H3C Comware Software, Version 7.1.070, Release 6348P21

	S5130S-10P-EI, S5130S-12TP-EI,S5130S-20P-EI,S5130S-28P-EI,S5130S-52P-EI,S5130S-10P-HPWR-EI,S5130S-12TP-HPWR-EI,S5130S-20P-PWR-EI,S5130S-28P-PWR-EI,S5130S-28P-HPWR-EI,S5130S-52P-PWR-EI,S5130S-28S-EI,S5130S-52S-EI,S5130S-28F-EI,S5130S-52F-EI,S5130S-28TP-EI,S5130S-52TP-EI,S5130S-28S-PWR-EI,5130S-28S-HPWR-EI,S5130S-52S-PWR-EI	H3C Comware Software, Version 7.1.070, Release 6348P21
	S5170-28S-EI,S5170-54S-EI,S5170-54S-PWR-EI,S5170-28S-HPWR-EI	H3C Comware Software, Version 7.1.070, Release R1122P30
S5500 Series	S5570S-28S-EI, S5570S-54S-EI, S5570S-54F-EI, S5570S-36F-EI, S5570S-54S-PWR-EI-A, S5570S-28S-HPWR-EI-A	H3C Comware Software, Version 7.1.070, Release R1122P30
	S5560X-30C-EI, S5560X-54C-EI, S5560X-30C-PWR-EI, S5560X-54C-PWR-EI, S5560X-30F-EI, S5560X-54F-EI, 5560X-34S-EI, S5560X-54S-EI,S5560X-30F-EIF	H3C Comware Software, Version 7.1.070, Release 6628P92
	S5590-28T8XC-EI, S5590-48T4XC-EI, S5590-28S8XC-EI, S5590-48S4XC-EI, S5590-28P8XC-EI, S5590-48P6XC-EI	H3C Comware Software, Version 7.1.070, Release 8108P60
S12500 Series	S12504X-AF, S12508X-AF,S12516X-AF	H3C Comware Software, Version 7.1.070, Release 2830
	S12504G-AF, S12508G-AF,S12516G-AF	H3C Comware Software, Version 7.1.070, Release 7640P01
S9800 Series	S9820-8C, S9820-8C-SAN	H3C Comware Software, Version 7.1.070, Release 6715P01
	S9850-32H, S9850-4C, S9850-32H-H1, S9850-4C-H1	H3C Comware Software, Version 7.1.070, Release 6715P01
	S9820-64H, S9820-64H-H1	H3C Comware Software, Version 7.1.070, Release 6715P01
S6800 Series	S6890-54HF, S6890-30HF	H3C Comware Software, Version 7.1.070, Release 2830
	S6825-54HF	H3C Comware Software, Version 7.1.070, Release 6715P01
	S6800-54HT, S6800-54HF, S6800-32Q-H1, S6800-2C-H1, S6800-4C-H1, S6800-54QF-H3, S6800-54QT-H3, S6800-	H3C Comware Software, Version 7.1.070, Release

	54QF-H5	6715P01
	S6812-24X6C, S6812-48X6C	H3C Comware Software, Version 7.1.070, Release 6628P92
	S6813-24X6C, S6813-48X6C	H3C Comware Software, Version 7.1.070, Release 6628P92
	S6805-54HF, S6805-54HT, S6805-54HF-H1, S6805-54HT-H1	H3C Comware Software, Version 7.1.070, Release 6715P01
	S6850-56HF, S6850-2C, S6850-56HF-H1, S6850-56HF-SAN,	H3C Comware Software, Version 7.1.070, Release 6715P01

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

PRODUCT SERIES	MODEL SERIES	DOCUMENT NAME	VERSION
All	All	Preparative and Operative Procedures for CC NDPP Switch Series	2.0
S10500 Series	S10500X	H3C S10500X Switch Series Command References	6W100
		H3C S10500X Switch Series Configuration Guides	6W100
	S10500X-G	H3C S10500X-G Switch Series Command References	6W100
		H3C S10500X-G Switch Series Configuration Guides	6W100
S7500 Series	S7500X	H3C S7500X Switch Series Command References	6W100
		H3C S7500X Switch Series Configuration Guides	6W100
	S7500X-G	H3C S7500X-G Switch Series Command References	6W100
		H3C S7500X-G Switch Series Configuration Guides	6W100
S6500 Series	S6520X	H3C S6520X-EI & S6520X-HI & S6520X-SI Switch Series Command References	6W100
		H3C S6520X-EI & S6520X-HI & S6520X-SI Switch Series Configuration Guides	6W100
S5100 Series	S5130S	H3C S5130S-EI & S5130S-HI Switch Series Command References	6W100

		H3C S5130S-EI & S5130S-HI Switch Series Configuration Guides	6W100
	S5170-EI	H3C S5170-EI Switch Series Command References	6W100
		H3C S5170-EI Switch Series Configuration Guides	6W100
S5500 Series	S5570S-EI	H3C S5570S-EI&S5500V3-SI Switch Series Command References	6W100
		H3C S5570S-EI&S5500V3-SI Switch Series Configuration Guides	6W100
	S5560X	H3C S5560X-EI Switch Series Command References	6W100
		H3C S5560X-EI Switch Series Configuration Guides	6W100
	S5590-EI	H3C S5590-HI&S5590-EI&S5500V3-HI Switch Series Command References	6W100
		H3C S5590-HI&S5590-EI&S5500V3-HI Switch Series Configuration Guides	6W100
S12500 Series	S12500X-AF	H3C S12500X-AF Switch Series Command References	6W100
		H3C S12500X-AF Switch Series Configuration Guides	6W100
	S12500G-AF	H3C S12500G-AF Switch Series Command References	6W100
		H3C S12500G-AF Switch Series Configuration Guides	6W100
S9800 Series	S9820-8C	H3C S9820-8C Switch Command References	6W100
		H3C S9820-8C Switch Configuration Guides	6W100
	S9850	H3C S6805[S6825] [S6850] [S9850] Command References	6W100
		H3C S6805[S6825] [S6850] [S9850] Configuration Guides	6W100
	S9820-64H	H3C S9820-64H Switch Command References	6W100
		H3C S9820-64H Switch Configuration Guides	6W100
S6800 Series	S6890	H3C S6890 Switch Series Command References	6W100
		H3C S6890 Switch Series Configuration Guides	6W100
	S6825 S6850 S6805	H3C S6805[S6825] [S6850] [S9850] Command References	6W100
		H3C S6805[S6825] [S6850] [S9850] Configuration Guides	6W100
	S6800	H3C S6800[S6860] [S6861] & S6820 Switch Series Command References	6W100

		H3C S6800[S6860] [S6861] & S6820 Switch Series Configuration Guides	6W100
	S6812 S6813	H3C S6812 & S6813 Switch Series Command References	6W100
		H3C S6812 & S6813 Switch Series Configuration Guides	6W100

PRODUCT TESTING

The developer has executed tests for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers has been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results. The approach resulted on the 100% of the TSFI and the SFRs tested.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product H3C Switch Series version 1.0 it is necessary the disposition of the following software components:

FIRMWARE/SOFTWARE	REFERENCE TOE
Version: H3C Comware Software, Version 7.1.070, Release 6628P92	S5560X-30F-EI (S5500 Series)
Version: H3C Comware Software, Version 7.1.070, Release 6715P01	S6805-54HT (S6800 Series)

EVALUATION RESULTS

The product H3C Switch Series version 1.0 has been evaluated against the Security Target H3C S10500 Series, S7500 Series, S6500 Series, S5100 Series, S5500 Series, S12500 Series, S9800 Series and S6800 Series Switches Security Target (version 2.0).

All the assurance components required by the evaluation level of the [cPP_ND_22e] have been assigned a "PASS" verdict. Consequently, the laboratory SGS Brightsight Barcelona, S.L. (Unipersonal) assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the [cPP_ND_22e] assurance level package, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 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.

- To strictly follow the secure configuration guidance provided by the manufacturer.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product H3C Switch Series version 1.0, a positive resolution is proposed.

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.

[cPP_ND_22e] collaborative Protection Profile for Network Devices v2.2e, 23-03-2020.

[cPP_ND_SD_22] Evaluation Activities for Network Device cPP, December-2019, Version 2.2

[ST] H3C S10500 Series, S7500 Series, S6500 Series, S5100 Series, S5500 Series, S12500 Series, S9800 Series and S6800 Series Switches Security Target (version 2.0).

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- H3C S10500 Series, S7500 Series, S6500 Series, S5100 Series, S5500 Series, S12500 Series, S9800 Series and S6800 Series Switches Security Target (version 2.0).

RECOGNITION AGREEMENTS

In order to avoid multiple certifications 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.eu.

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.