EUCC Certification Report

Hikvision Network Camera Series iDS-2CD7x V5.9.22

Sponsor and developer:	***Hangzhou Hikvision Digital Technology Co., Ltd.*** **No. 555 Qianmo Road** **Binjian District, Hangzhou 310051** **China**
Evaluation facility:	***Bureau Veritas Cybersecurity Europe B.V.*** **Herikerbergweg 15,** **1101 CN Amsterdam** **The Netherlands**
Report number:	**EUCC-3110-2026-2500163-01 Certification Report**
Report version:	**1**
Project number:	**EUCC-2500163-01**
Author(s):	**Brian Smithson, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**15 May 2026**
Number of pages:	**16**
Number of appendices:	**0**

CONTENTS

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, 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 cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the ICT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the ICT product satisfies the security requirements stated in the security target.

International recognition of the certificate

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of published certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Hikvision Network Camera Series iDS-2CD7x V5.9.22, identified in this document as either the ICT Product or as the Target of Evaluation (TOE).

The developer of the ICT Product is Hangzhou Hikvision Digital Technology Co., Ltd. located in Hangzhou, China and they also act as the sponsor of the evaluation and certification.

This Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the ICT product for their particular requirements.

The TOE is a Network camera composed of hardware and firmware that is specific to the hardware. The TOE provides the following functionality:

- Management interface
- Video over IP
- Security audit

A certification procedure was conducted on the TOE by TrustCB B.V., in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024 and (EU) 2025/2462 of 8 December 2025.

The successful completion of the certification procedure resulted in TrustCB issuing an EUCC certificate, The certificate identifier is **EUCC-3110-2026-2500163-01**, dated 2026-05-15 and with a 5-year validity.

The evaluation of the TOE was performed by Bureau Veritas Cybersecurity Europe B.V. located in Amsterdam, The Netherlands. The evaluation was completed on 2026-05-15 with the issuance of the evaluation technical report *[ETR]*. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 *[CC]* (Parts 1, 2, 3, 4, 5).

The scope of the evaluation was defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ICT Product, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL3 augmented (EAL3+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 “Flaw Reporting Procedures”.

The AVA_VAN level applied during the evaluation was AVA_VAN.2. This assurance level is recognised by article 52 of [CSA] as ‘substantial’.

Consumers of this ICT Product are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

TrustCB B.V., as Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates.

Note that the certification results apply only to the specific version of the product as evaluated.

---

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is ICT product Hikvision Network Camera Series iDS-2CD7x V5.9.22 from Hangzhou Hikvision Digital Technology Co., Ltd. located in Hangzhou, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	IDS-2CD7*x*	Complete list of *x* models is provided in section 1.2 of the *[ST]*.
Firmware	Firmware Web Encoding	V5.9.22 5.2.46_R0101 V7.3

Additional requirements for the operational environment of the certified ICT product are described in section 4.2 of the *[ST]*.

To ensure secure usage a set of guidance documents is provided with the TOE. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information”.

2.2 Contact information related to the evaluation of the ICT Product

Holder of the EUCC Certificate

Organisation name:	Hangzhou Hikvision Digital Technology Co., Ltd.
Address:	No. 555 Qianmo Road, Binjiang District, Hangzhou 310051, China
Certified product contact details	securitylab@hikvision.com

Developer of the certified ICT Product

ICT product developer	Hangzhou Hikvision Digital Technology Co., Ltd.

Identification of CAB

The Certification Assessment Body for this ICT Product is TrustCB B.V. TrustCB is licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC certification activities up to and including EUCC High.

TrustCB point of contact: EUCC@trustcb.com

Identification of ITSEF

Evaluation and testing for this ICT Product was performed by following ITSEF:

Bureau Veritas Cybersecurity Europe B.V. in Amsterdam, The Netherlands

2.3 Security services and policies

2.3.1 Security services

The TOE provides the following security services and policies:

Security Management

The TOE maintains three different roles which are assign to each user. Allowed management functions are different for each role.

User Identification and Authentication

The TOE management can be done either using a computer with a web browser supporting HTTPS or by a software platform implementing the ISAPI over HTTPS. In both cases the access to the TOE is protected by a user/password authentication.

Trusted path/channel

A trusted path/channel implemented with HTTPS/TLS communication shall be established before accessing the TOE management functionality, video data and syslog transmission.

Security Audit

The TOE has the capability to generate audit records. TOE administrators have the ability to read the logs after establishing the trusted path and successfully log in. The TOE has the capability to send the audit data to a trusted network entity (e.g., a syslog server).

Protection of the TSF

The TOE has self-tests during the initial start-up. The TOE prevents reading of all TSF data.

Limited TOE Access

The TOE provides the capability to restrict the maximum number of concurrent session for a same user through the management interface. It also implements two different methods to terminate an open session: inactivity of the user or an action of the user.

Cryptographic Operation

TOE performs cryptographic operations such as encryption, decryption, hashing and digital signature.

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the Hikvision Network Camera Series iDS-2CD7x V5.9.22

Document reference: Hikvision FLR 1.0

2.3.3 Assurance Continuity policies

This is a new product certification. An assurance continuity policy was not provided.

2.3.4 Lifecycle management processes and production facilities

Not applicable to this evaluation.

2.3.5 Patch management process

Not applicable to this evaluation.

2.4 Assumptions and Clarification of Scope

2.4.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives 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 *[ST]*.

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions described in the [ST].

Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE.

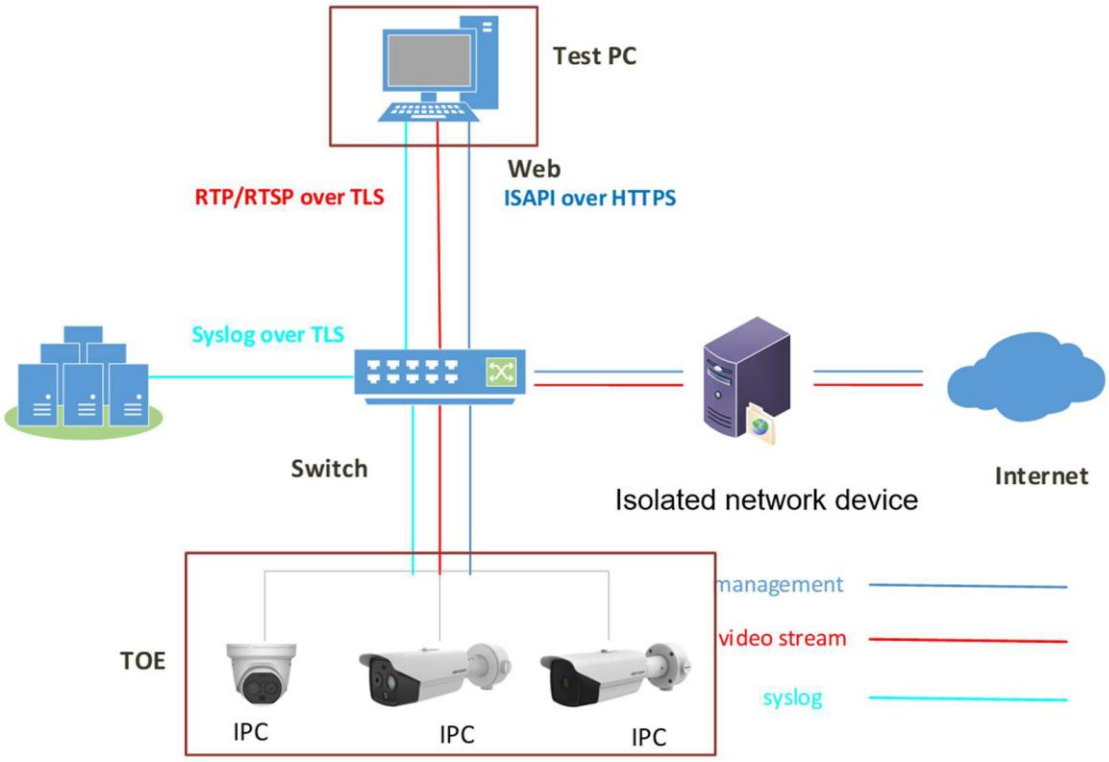
There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

2.4.2 Clarification of scope

Considering all Assumptions above, the evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.5 Architectural Information

TOE environment consists of a network which is isolated from other networks (e.g. other LANs or Internet) by Isolated Network Devices (e.g. it can be either Firewall/Gateway/Physical device). The TOE network may contain the following components: one or multiple TOEs (IPCs), video recording devices (such as a Network Video Recorder, NVR) and management computers (Test PC in the figure, below) via ISAPI. The figure illustrates the environment where the TOE is intended to be used:



Note that neither the management nor the video stream are accessible from the internet. The “Isolated Network Device” depicted in the figure prevents accessing the TOE from internet, while allowing the access to other non-TOE devices that might be connected to the TOE LAN.

The usage scenarios in scope of the evaluation are:

- The test PC has the web browser to access the TOE to have all management functions.
- Media interface which is used to send audio and video to the clients connected to the Test PC and internet by going throw isolated network device.
- TOE’s management interface being accessed from a browser or a client/platform software using ISAPI over HTTPS. ISAPI protocol is an HTTP-based application programming interface that enables the TOE to build communication between security devices/servers (e.g., NVR) and the client/platform programs. Client/platform programs must implement this ISAPI protocol.
- NVR is a physical device used to record and store video. The video is received via RTP/RTSP protocol over TLS. It is optional and out of the scope.
- Exporting audit logs to a trusted syslog server through syslog protocol over TLS.

2.6 Supplementary Cybersecurity Information

The following website link was provided for the Hikvision Network Camera Series iDS-2CD7x V5.9.22 for the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881: https://www.hikvision.com/en/support/cybersecurity

This link provides further details and links on:

- The period during which the Hikvision Network Camera Series iDS-2CD7x V5.9.22 security support will be offered to end users, in particular as regards the availability of cybersecurity related updates. This is stated as “until June 30, 2031”. (https://www.hikvision.com/en/support/cybersecurity/cybersecurity-white-paper/announcement-of-security-support-timeline-for-ids-2cd7x/)
- Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the Hikvision Network Camera Series iDS-2CD7x V5.9.22 (https://www.hikvision.com/en/support/cybersecurity/best-practices/ipc-security-guide/)
- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the Hikvision Network Camera Series iDS-2CD7x V5.9.22. (https://www.hikvision.com/en/support/cybersecurity/report-an-issue/, https://www.hikvision.com/en/support/cybersecurity/security-advisory/)
- The online repository listing publicly disclosed vulnerabilities related to the Hikvision Network Camera Series iDS-2CD7x V5.9.22 and to any relevant cybersecurity advisories. (https://www.hikvision.com/en/support/cybersecurity/cybersecurity-white-paper/announcement-of-security-support-timeline-for-ids-2cd7x/

Note: The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the Hikvision Network Camera Series iDS-2CD7x V5.9.22:

Identifier	**Version**
Hikvision Security Guidance	V1.2
UD38502B_Network Camera User Manual_H11	V5.9.14

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were:

- **EAL 3 augmented with ALC_FLR.2**

as defined by, and detailed in, *[CC]* and *[CEM]*.

3.2 EUCC State of the Art documents and Protection Profiles

Not applicable to this evaluation.

3.3 ICT Product testing

The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

3.3.1 Testing approach and depth

Developer ATE tests conducted from 2026-09-06 to 2025-09-12 were reviewed, and seven (7) such tests were chosen by the ITSEF to be repeated, based on:

- Criticality of tests, and
- Depth of provided test evidence

Additionally, nine (9) Independent ATE tests were proposed and performed by the ITSEF.

3.3.2 Independent penetration testing

A Public vulnerability search was performed to check for disclosed vulnerabilities, exploits, or attack techniques applicable to the TOE. Hikvision shared the different versions of firmware for three different version of hardware including the TOE version. Public vulnerability search was performed on these versions.

The public vulnerability analysis was focused on:

- Specific firmware uploaded into the Hikvision device.
- Online search based on the product name.
- Search based on evaluation evidence

Based on firmware and evaluation evidence search, and on the presentation of results of independent AVA tests conducted from 2025-09-06 to 2025-09-12, three (3) public AVA tests were proposed and performed.

3.3.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]* and as shown in the figure in section 2.5 of this report. The Test PC used tools for network and traffic analysis, cryptographic testing, fuzzing, etc.

The particular sample TOE used for testing is identified below:

- Model: iDS-2CD7A46G2-IZHSY(1T)
- Firmware version: V5.9.22 build 250513
- Encoding version: V7.3 build 250513
- Web version: V5.2.46_R0101 build 250506
- Firmware version property: B-R-H11-0

One of three device settings were employed during testing, depending on the test:

1. Initial TOE configuration (ENV_TOE_RAW)

- Switch on the TOE and connect the equipment to switch through net cable.
- PC connect to switch and configure two different IP addresses 192.168.1.100 and 10.65.151.127
- Switch on Google Chrome, input http://192.168.1.64
- Configure password, click “Activation”, Configure Account Security Settings and activate the TOE
- Click “Configuration-Network-TCP/IP”, modify equipment IPv4 Address 10.65.151.118, IPv4 Subnet Mask 255.255.255.0, IPv4 Default Gateway 10.65.151.254, choose “Save” and restart the equipment
- Go to browser page, click “Download Plug-In”, download web plug-ins, install and run it.
- Enter “Maintenance and Security -Security-Advanced Security”, choose “Enable Security Reinforce”, save and restart TOE

2. TOE configure user（ENV_TOE_USER）

- TOE input ENV_TOE_RAW status and environment.
- Open a web browser and type the following URL: https://10.65.151.118
- Login with administrator
- Go to the Configuration-System-User Management-User Management， Add click add， create one new Operator user and one User

3. TOE for syslog (ENV_TOE_SYSLOG)

- TOE input ENV_TOE_RAW status and environment.
- Open a web browser and type the following URL: https://10.65.151.118
- Login with administrator
- Enter Maintenance and Security- Maintenance- Security Audit Log
- Click Advanced Configuration, Activate Enable Log Upload Server, configure Log Server Address and Log Server Port
- In the "Maintenance and Security- Security- Certificate Management" interface, create a client certificate request and import the certificate
- In the "Maintenance and Security- Security- Certificate Management" interface, import the CA certificate.
- Select the corresponding client certificate and CA certificate in the security audit log interface

3.3.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised 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 *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

3.4 ICT Product evaluation

3.4.1 Reused evaluation results

There is no reuse of evaluation results in this certification.

3.4.2 Evaluated configuration

The TOE is defined uniquely by its name and version number Hikvision Network Camera Series iDS-2CD7x V5.9.22.

3.4.3 Assessment against each assurance requirement

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.2
TOE summary specification	ASE.TSS.1

Based on the results of evaluation for ASE assurance class it can be concluded that ST is sound and internally consistent and is suitable for use as the basis for a TOE evaluation. The ST meets the requirements presented within all work units of ASE class.

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.3
TOE design	ADV_TDS.2

As the result of evaluation activities for ADV class, Bureau Veritas Cybersecurity concludes that it has a sufficient level of understanding of the TOE's functioning (including information on subsystems, modules and available interfaces) to be used as the basis for conducting vulnerability analysis and testing upon the TOE. The provided description for the TOE meets the requirements presented within all work units of ADV class.

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

The guidance documentation provided by the developer include the guidance for all user roles. It includes both operational user guidance and preparative procedures. The documentation describes all relevant aspects for the secure handling of the TOE. The guidance documentation meets the requirements presented within all work units of AGD class.

ALC

ALC	
CM capabilities	ALC_CMC.3
CM Scope	ALC_CMS.3
Delivery	ALC_DEL.1
Development security	ALC_DVS.1
Life cycle definition	ALC_LCD.1
Flaw remediation	ALC_FLR.2

The lifecycle support of the TOE allows for establishing control over the processes of refinement of the TOE during its development and maintenance. The lifecycle implemented by the developer allows for high assurance that the TOE security requirements correspond to the TOE due to the fact that the lifecycle process is implemented as an integral part of the development and maintenance activities. The provided documentation and evidence meet the requirements presented in all work units of ALC class.

.**ATE**

ATE	
Coverage	ATE_COV.2
Depth	ATE_DPT.1
Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2

The ATE evaluation activities allowed for conclusion that the TOE operates according to its design descriptions. The tests performed by the developer proofed to be complete and accurate. Additional independent tests were performed by Bureau Veritas Cybersecurity by repeating a sample of test performed by the developer based on the criticality of the tests and the depth of provided evidence.

AVA

AVA	
Vulnerability analysis	AVA_VAN.2

Vulnerability analysis of the TOE demonstrated that no potential vulnerabilities were identified (during the evaluation of the development and anticipated operation of the TOE) that could allow attackers to violate the SFRs.

3.5 Results of the evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report, other evaluator documents and developer documentation *[DEV_DOCS]*.

The verdict of each claimed assurance requirement is "**Pass**".

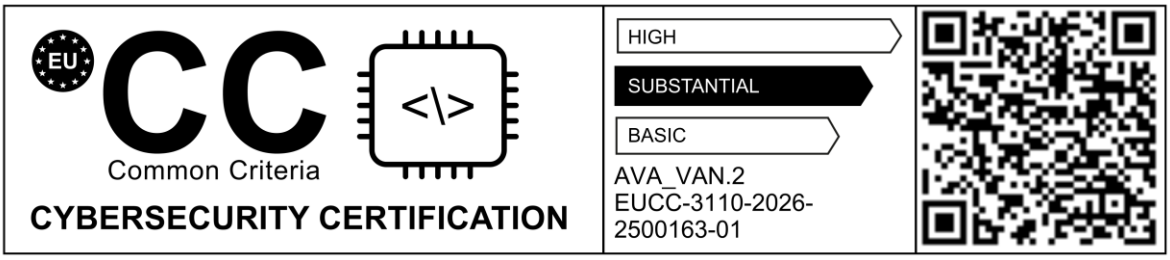
Based on the evaluation results the evaluation lab concluded the Hikvision Network Camera Series iDS-2CD7x V5.9.22, to be **CC:2022 R1 1 Part 2 extended, CC:2022 R1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as '**Substantial**' with **AVA_VAN 2** and to meet the requirements of **EAL 3 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

3.6 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-3110-2026-2500163-01

Date of issuance: 15-May-2026 and with a validity period of **5 years**.



3.7 Comments and Recommendations

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part 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.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <none>, which are out of scope as there are no security claims relating to these.

4 Security Target

The certification references the following security target:

Hikvision Network Camera Series iDS-2CD7x V5.9.22 Security Target, v1.7, 16 April 2026 *[ST]*.

5 Glossary

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information and communication technologies product as defined by [EUCC]
ITSEF	IT Security Evaluation Facility
EUCC	European Cybersecurity Certification Scheme [EU-EUCC], created under the Cybersecurity Act [EU-CSA] and detailed in Commission Implementing Regulation (EU) 2024/482
PP	Protection Profile
SotA	EUCC State-of-the-Art document
TOE	Target of Evaluation; the object of the certification activity described by this report

6 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, CC:2022 Parts 1, 2, 3, 4 and 5, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 R1, November 2022
[CCMB-2024-002]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2
[DEV_DOCS]	UD38502B_Network Camera User Manual_H11, v5.9.14, 09 October 2025
	Hikvision Network Camera Series Security Guidance, v1.2, 30 July 2025
[ETR]	EVALUATION TECHNICAL REPORT Hikvision Network Camera Series iDS-2CD7x V5.9.22, v2.0, 17 April 2026
[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 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 cybersecurity certification scheme (EUCC)
[EU-EUCC-amdt.1]	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EU-EUCC-amdt.2]	Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art documents
[ST]	Hikvision Network Camera Series iDS-2CD7x V5.9.22 Security Target, v1.7, 16 April 2026

(This is the end of this report.)