CSA
SINGAPORE

Cybersecurity
Certification Centre
CYBER SECURITY AGENCY OF SINGAPORE

Certificate Report

Version 1.0

14 February 2023

CSA_CC_22003

For

Hikvision Network Camera Series iDS-2CD7x
Version: 1.0

From

Hangzhou Hikvision Digital Technology Co., Ltd

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorizing Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	Feb 2023	Released

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the Hikvision Network Camera Series iDS-2CD7x Version 1.0 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Series	Models	Version of Firmware/Software	Interfaces
iDS-2CD7	iDS-2CD7046G0-AP	Firmware: v5.7.73 build 220402 Web: v4.0.1.0 build 211109 Encoding: v7.3 build 220325 Plugin: 3.0.7.45 (The 5 series) Binary file: IPCG_H8_EN_NEU_5.7.73_220402.zip	DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7086G0-AP		
	iDS-2CD7046G0/E-IHSY		
	iDS-2CD7086G0/E-IHSY		
	iDS-2CD7146G0-IZS		
	iDS-2CD7186G0-IZS		
	iDS-2CD7146G0-IZHSY		
	iDS-2CD7186G0-IZHSY		
	iDS-2CD7546G0-IZHS		
	iDS-2CD7546G0-IZHSY		
	iDS-2CD7586G0-IZHS		
	iDS-2CD7586G0-IZHSY		
	iDS-2CD7A46G0-IZHS		
	iDS-2CD7A46G0-IZHSY		
	iDS-2CD7A86G0-IZHS		
	iDS-2CD7A86G0-IZHSY		

Table 1 - TOE components identifier

The list of guidance documents to use with the product in its certified configuration is as follows.

Name	Version
Hikvision Network Camera Series Security Guidance	Version 1.0
Hikvision Network Camera User Manual	UD14456B
Hikvision Intelligent Security API (General Application) Developer guide	Version 2.7
Hikvision Intelligent Security API (Additional)	Version 2.7

Table 2 - List of guidance documents

The Target of Evaluation (TOE) is a Network Camera developed by Hikvision. The TOE provides management interface, video over IP and security audit.

The TOE environment consists of a network which is segregated from other networks (e.g. other LANs or Internet), either physically or by a Firewall/Gateway/Physical segregation device. The TOE network may contain the following components: one or multiple TOEs (IPCs), video recording devices (such as NVR) and management computers via ISAPI.

The evaluation of the TOE has been carried out by An Security Pte Ltd, an approved CC test laboratory, at the Evaluation Assurance Level (EAL2) augmented with ALC_FLR.2 and completed on 6 December 2022.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed Issue
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. The access to the management functions implements security controls to detect unsuccessful authentication attempts and insufficient password complexity and length. In case of reaching the Administrator configurable positive integer (7 by default) consecutive unsuccessful attempts, the TOE blocks the account from which the user is trying to connect.
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 provides reliable time stamps. The TOE has self-tests during the initial start-up. The TOE prevents reading of all secure 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. The session is locked after inactivity time the administrator configured and need re-authenticate.
Trusted Firmware Updates	The trusted firmware update functionality is implemented and enforced using signature verification of the signed firmware.

Table 3: TOE Security Functionalities

Please refer to the Security Target [1] for more information.

The TOE Security Problem Definition has been defined in terms of Assumptions, Threats, and Organisation Policies. These are outlined in Chapter 3 of the Security Target [1]

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Table of Contents

1 CERTIFICATION ... 9

1.1 PROCEDURE ... 9
1.2 RECOGNITION AGREEMENTS ... 9

2 VALIDITY OF THE CERTIFICATION RESULT ... 10

3 IDENTIFICATION ... 11

4 SECURITY POLICY ... 13

5 ASSUMPTIONS AND SCOPE OF EVALUATION ... 13

5.1 ASSUMPTIONS ... 13
5.2 CLARIFICATION OF SCOPE ... 14
5.3 EVALUATED CONFIGURATION ... 14
5.4 NON-EVALUATED FUNCTIONALITIES ... 14
5.5 NON-TOE COMPONENTS ... 14

6 ARCHITECTURE DESIGN INFORMATION ... 15

7 DOCUMENTATION ... 15

8 IT PRODUCT TESTING ... 15

8.1 DEVELOPER TESTING (ATE_FUN) ... 15
8.1.1 Test Approach and Depth ... 15
8.1.2 The developer performed functional testing covering all as described in the Security Target [1]. Test Configuration ... 15
8.1.3 The TOE used for testing is configured according to the TOE guidance document [9] [10].Test Results ... 15
8.2 EVALUATOR TESTING (ATE_IND) ... 15
8.2.1 Test Approach and Depth ... 15
8.2.2 Test Configuration ... 16
8.2.3 Test Results ... 16
8.3 PENETRATION TESTING (AVA_VAN) ... 16
8.3.1 Test Approach and Depth ... 16

9 RESULTS OF THE EVALUATION ... 17

10 OBLIGATIONS AND RECOMMENDATIONS FOR THE USAGE OF THE TOE ... 17

11 ACRONYMS ... 18

12 BIBLIOGRAPHY ... 19

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [2] [3] [4];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR. Hence, the certification for this TOE is fully covered by the CCRA.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **13 February 2028**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [8]. Potential users should check the SCCS website (www.csa.gov.sg/programmes/csa-cc-product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is: **Hikvision Network Camera Series iDS-2CD7x, Version 1.0**

The following table identifies the TOE deliverables.

Series	Models	Version of Firmware/Software	Interfaces
iDS-2CD7	iDS-2CD7046G0-AP	Firmware: v5.7.73 build 220402 Web: v4.0.1.0 build 211109 Encoding: v7.3 build 220325 Plugin: 3.0.7.45 (The 5 series) Binary file: IPCG_H8_EN_NEU_5.7.73_220402.zip	DC12V, SD, RJ45, audio 1in 1out, alarm 1in 1out
	iDS-2CD7086G0-AP		
	iDS-2CD7046G0/E-IHSY		
	iDS-2CD7086G0/E-IHSY		
	iDS-2CD7146G0-IZS		
	iDS-2CD7186G0-IZS		
	iDS-2CD7146G0-IZHSY		
	iDS-2CD7186G0-IZHSY		
	iDS-2CD7546G0-IZHS		
	iDS-2CD7546G0-IZHSY		
	iDS-2CD7586G0-IZHS		
	iDS-2CD7586G0-IZHSY		
	iDS-2CD7A46G0-IZHS		
	iDS-2CD7A46G0-IZHSY		
	iDS-2CD7A86G0-IZHS		
	iDS-2CD7A86G0-IZHSY		

Table 4 - TOE Deliverables

The guide for receipt and acceptance of the above-mentioned TOE are described in the set of guidance documents.

Name	Version
Hikvision Network Camera Series Security Guidance	Version 1.0
Hikvision Network Camera User Manual	UD14456B
Hikvision Intelligent Security API (General Application) Developer guide	Version 2.7
Hikvision Intelligent Security API (Additional)	Version 2.7

Table 5 - Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

TOE	Hikvision Network Camera Series iDS-2CD7x version 1.0
Security Target	Hikvision Network Camera Series iDS-2CD7x Security Target, version 2.1
Developer	Hangzhou Hikvision Digital Technology Co Ltd
Sponsor	Hangzhou Hikvision Digital Technology Co Ltd
Evaluation Facility	An Security Pte Ltd
Completion Date of Evaluation	06 December 2022
Certification Body	Cyber Security Agency of Singapore (CSA)
Certificate ID	CSA_CC_22003
Certificate Validity	5 years from date of issuance

Table 6: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to the following security functional classes:

- Cryptographic Support
- Identification and Authentication
- Trusted Path/Channel
- Protection of the TSF
- Security Management
- Security Audit
- TOE Access

Specific details concerning the abovementioned security policy can be found in Chapter 6 of the Security Target [1].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [1] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Usage Assumptions	Description
OE.TRUSTED_USERS	It is assumed that the administrator of the TOE will correctly configure and install the TOE in its operational environment by following the guidance documentation. It is assumed that the users of the TOE will not carry out any malicious action trying to compromise the availability of the TOE.

Table 7: Usage Assumptions

Environmental Assumptions	Description
OE.TRUSTED_NETWORK_SYSTEMS	It is assumed that attackers have no chance to connect any malicious devices into the local network of the TOE.
OE.NO_PHYSICAL_ACCESS	It is assumed that the TOE will not be physically accessible.

Table 8: Environmental Assumptions

Details can be found in section 4.2 of the Security Target [1].

5.2 Clarification of Scope

The scope of evaluation is limited to the claims made in the Security Target [1].

5.3 Evaluated Configuration

The evaluated configuration in the Security Target [1] is as shown in Figure 1, where the TOE takes one of the three possible IPC form factors.

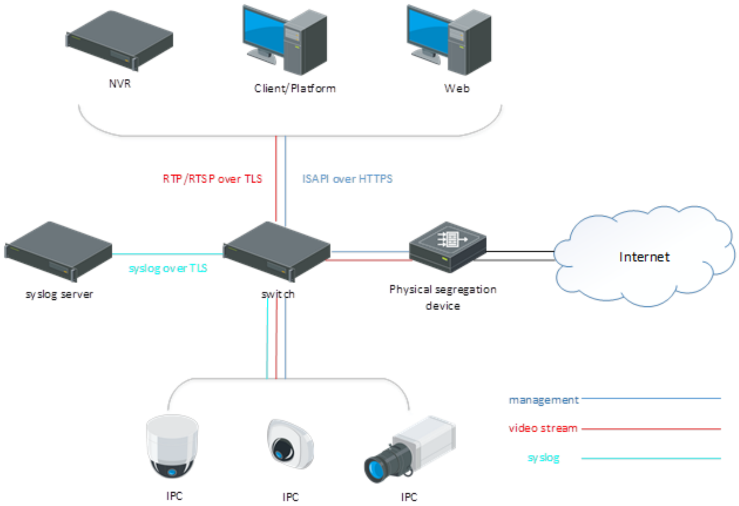

Figure 1 - Hikvision Network Camera Series DS-2CD7x

5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities within the scope as clarified in section 5.2.

5.5 Non-TOE Components

The TOE requires at least one additional non-TOE component (i.e. hardware/software/firmware) for its operation. These include:

Component	Required	Description
Management computer with a web browser	Mandatory	General purpose computer, based on Windows and/or macOS platforms, that is used to manage the TOE using a web interface implementing ISAPI protocol over HTTPS and to receive video data through the RTP/RTSP protocol over TLS.
Network Video Recorder (NVR)	Optional	Physical device used to record and store video. The video is received via RTP/RTSP protocol over TLS
Client/Platform	Optional	General purpose computer which implements a software solution to record and store video from the TOE using RTP/RTSP protocol over TLS and/or manage the same TOE through ISAPI protocol over HTTPS.
Syslog Server	Optional	General purpose computer running syslog service and receive audit log via syslog protocol over TLS.

Table 9: Non-TOE Hardware/Software/Firmware

6 Architecture Design Information

The major components of the TOE are Access subsystem, Management subsystem, Hardware subsystem, Boot/OS subsystem, the Media subsystem.

The Access subsystem implements the ISAPI interface, manages user authentication and authorisation, provides cryptographic services, manages access to the video stream, and is responsible for the establishment of the trusted path.

The Management subsystem manages users, access control, certificates, time settings etc.

The Hardware subsystem is the enforcing subsystem for the whole TOE, providing Secure Boot and reliable timestamps.

The Boot/OS subsystem is responsible for the camera's hardware drivers, file systems for data storage, secure boot-up etc.

The Media subsystem provides video streams and functional features for the video.

7 Documentation

The evaluated documentation as listed in Table 5 - Guidance Document (part of TOE deliverables) is being provided with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the Security Target.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

8.1.2 The developer performed functional testing covering all as described in the Security Target [1]. Test Configuration

8.1.3 The TOE used for testing is configured according to the TOE guidance document [9] [10].Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

The evaluator sampled and repeated developer's test cases that are related to the TSFs claimed by the TOE. The results of the repeated developer's test cases yield the same result as those stated in the developer's test plan. The results of the evaluators tests are recorded in the evaluator's test plan.

In addition to the developer's tests, the evaluators devised a set of independent tests that has not been tested by the developer to gain assurance of the security of the TOE.

8.2.2 Test Configuration

A detailed test description was provided in the ATE document. The evaluator conducted all the developer's functional tests found in the developer test plan and procedures in the premises of the evaluation lab.

8.2.3 Test Results

No deviations were found between the expected and the actual results of the developer's tests repeated and for the independent tests.

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN) treating the resistance of the TOE to an attack with the Basic attack potential i.e. amongst other that the evaluator used sources of information publicly available to identify potential vulnerabilities in the TOE. The evaluator analysed which potential vulnerabilities are not applicable to the TOE in its operational environment.

- VA1: Buffer overflow
- VA2: Strip and exploit SSL/TLS
- VA3: Attempting to inject malicious commands in TOE by replicating CVE-2021-36260
- VA4: Attempting to authentication bypass the TOE by replicating CVE-2021-36320
- VA5: Attempting to brute force the password and to conduct buffer overflow to the password or username field.
- VA6: Attempting to capture, replay with the parameters of the ISAPI TSFI so that an attacker can bypass identification and authentication of the TOE
- VA7: Using the script provided by VA3 and VA4, at attacker can customized the script to bypass the controls that has been fixed for the previous CVEs.

For the potential vulnerabilities being applicable to the TOE in its operational environment and, hence, which were candidates for testing applicable to the TOE in its operational environment, the evaluator devised the attack scenarios where these potential vulnerabilities could be exploited. For each such attack scenario he firstly performed a theoretical analysis on the related attack potential. Where the attack potential was Basic or near to Basic, the evaluator conducted penetration tests for such attack scenarios. He analysed then the results of these tests with the aim to determine, whether at least one of the attack scenarios with the attack potential Basic was successful.

The tests are performed on the TOE as stated in the Security Target [1]. This evaluated configuration is reflected in the preparative procedures of the user guidance [10].

The evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration. No residual risks were identified.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 augmented by ALC_FLR.2 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

10 Obligations and recommendations for the usage of the TOE

The documents as outlined in Table 2 - List of guidance documents contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

No additional recommendation was provided by the evaluators.

11 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

[1] Hikvision, “Hikvision Network Camera Series iDS-2CD7x Security Target, Version 2.1,” 23 November 2022.

[2] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5,” 2017.

[3] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5,” 2017.

[4] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5,” 2017.

[5] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5,” 2017.

[6] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0,” 2018.

[7] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0,” 2018.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0,” 2018.

[9] Hikvision, “Hikvision Network Camera User Manual, UD14456B,” 2022.

--End of Report ---------------------------------------