



LCIE

BUREAU VERITAS

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

No. 1199, Bin'an Road, Changhe street,
Binjiang District, Hangzhou
CHINA

LCIE certifies that the Product mentioned below has been evaluated and found to be in accordance with the following requirements

ETSI EN 303 645 v2.1.1

Product: Network Camera
Model: DH-IPC-XABCNYZ-M-T-S-L
IPC-XABCNYZ-M-T-S-L
Software version: Firmware version: Security Baseline 2.1

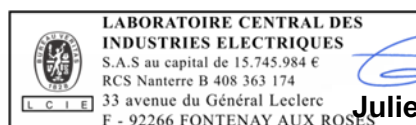
Other informations: The product has been evaluated according to the ETSI TS 103 701 v1.1.1 and found in conformity to the ETSI EN 303 645 v2.1.1 standard. This includes security controls & data processing requirement implemented in the product contributing to the General Data Protection Regulation (GDPR) compliance of the overall solution. See annex for list of models and provisions details.

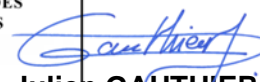
Trade Mark: 

Type certificate: LCIE N°778478

Relevant document: Test report(s) n° ESH-220208007-T02

Issue date: 03/06/2022
Fontenay-aux-Roses




Julien GAUTHIER
Certification Officer

This document shall not be reproduced, except in full, without the written approval of the LCIE.

CERT-TYPE-FORM 01 Rev. 03
Page 1 / 6



List of models	DH-IPC-XABCNYZ-M-T-S-L IPC-XABCNYZ-M-T-S-L
<p>X represent: HF / HFW / HDP / HDPW / HDW / HD / HDB / HDBW / HFS / HUM / E / EB / EW / EBW / MBW / MDW / MF / MFW / HDEW / HCBW / PFW / PDW / PDBW / PSD / PFEW / WP / WK / WB / WL / WDB / WDS / WGP / PSDW</p> <p>A represent: NA / 1 / 2 / 3 / 4 / 5 / 7 / 8</p> <p>B represent: 0 / 1 / 2 / 3 / 4 / 5 / 6 / 8 / 12 / 16 / 32 / 24 / 48 / 64</p> <p>C represent: 0 / 1 / 2 / 3 / 4 / 6 / 8</p> <p>N represent: NA / 0 / 1 / 2 / 3 / 9</p> <p>Y represent : NA / B / C / D / E / EM / F / G / H / K / M / R / R1 / S / S1 / T / T1 / TM / X / L / M / S / ML / K1 / Y / DT / DF / DS / DG / HR / DK1 / DS1 / DT1 / DE / DB / DC / DD / DEM / DH / DK / DM / DR / DR1 / DTM / DX / DL / DML / DY</p> <p>Z represent : NA / P / N</p> <p>M represent: NA / Z / Z5 / Z12 / ZH / Z5H / ZE / Z5E / Z12E / ZHE / Z5HE / W / AW / E / M / M12 / F / H / A / A2 / PT / ATC / S / ST / AS / ASE / VF / Z / IX / I1 / I2 / I3 / I4 / EX / E1 / E2 / E3 / E4 / L1 / L2 / L3 / L4 / L5 / IRA / IRE6 / B / BV / MF / A360 / A270 / A180 / B120 / B360 / STW / Z4 / Z4H / Z4HE / Z7 / Z7H / Z7HE / STW / ZVH / Z4VH / Z5VH / Z7VH / 3D / LED / NI / PV / LI / 4G / 5G / ZS / ZAS / V / SA / AS / SE / A / ASE / ZE / S / G / 32G / 64G / G4G / Z4E / ZD / ZHD / Z4D / Z4HD / SW / SAW / FR / ZFR / Z4FR / Z7FR / Z25</p> <p>T represent : NA / T47 / T87 / T44 / T84 / T20 / T40 / T80 / G / NF / D2 / I1 / I2 / D237 / D440 / D445 / D425 / E2 / IVC / D440 / D445 / D237 / L1 / L2 / L3 / L4 / L5 / ASTE / RD-ASTE / 4G / 5G / LB / 4G / SFC-I2 / PV / M / IL / IL-B / NI / LED / LED-B / E2-ASTE / E2-RD-ASTE / 5G-GD / 5G-MD / 5G-LD / T8A / GW / P / SP / HT / I2-B</p> <p>S represent : NA / S1 / S2 / S3 / S4 / S5 / S6 / S7 / S8 / S9 / S10</p> <p>L represent : NA / USA / CAN / EAU / LA</p> <p>- represent : NA / -</p> <p>IPC represent : NA / IPC</p>	

Provisions number and title	
Reference	VERDICT
5.1 No universal default passwords	
Provision 5.1-1 M C (1)	PASS
Provision 5.1-2 M C (2)	PASS
Provision 5.1-3 M C (8)	PASS
Provision 5.1-4 M C (8)	PASS
Provision 5.1-5 M C (5)	PASS
5.2 Implement a means to manage reports of vulnerabilities	
Provision 5.2-1 M	PASS
Provision 5.2-2 R	
Provision 5.2-3 R	
5.3 Keep software updated	
Provision 5.3-1 R	
Provision 5.3-2 M C (5)	PASS
Provision 5.3-3 M C (12)	PASS
Provision 5.3-4 R C (12)	
Provision 5.3-5 R C (12)	
Provision 5.3-6 R C (9, 12)	
Provision 5.3-7 M C (12)	PASS
Provision 5.3-8 M C (12)	PASS
Provision 5.3-9 R C (12)	
Provision 5.3-10 M C (11,12)	PASS
Provision 5.3-11 R C (12)	
Provision 5.3-12 R C (12)	
Provision 5.3-13 M	PASS
Provision 5.3-14 R C (3,4)	
Provision 5.3-15 R C (3,4)	
Provision 5.3-16 M	PASS
5.4 Securely store sensitive security parameters	
Provision 5.4-1 M C (14)	PASS
Provision 5.4-2 M C (10)	PASS
Provision 5.4-3 M	PASS
Provision 5.4-4 M C (15)	PASS
5.5 Communicate securely	

Provisions number and title	
Reference	VERDICT
Provision 5.5-1 M	PASS
Provision 5.5-2 R	
Provision 5.5-3 R	
Provision 5.5-4 R C (16)	
Provision 5.5-5 M C (17)	PASS
Provision 5.5-6 R C (18)	
Provision 5.5-7 M C (19)	PASS
Provision 5.5-8 M C (20)	PASS
5.6 Minimize exposed attack surfaces	
Provision 5.6-1 M	PASS
Provision 5.6-2 M	PASS
Provision 5.6-3 R	
Provision 5.6-4 M C (13)	PASS
Provision 5.6-5 R	
Provision 5.6-6 R	
Provision 5.6-7 R	
Provision 5.6-8 R	
Provision 5.6-9 R	
5.7 Ensure software integrity	
Provision 5.7-1 R	
Provision 5.7-2 R	
5.8 Ensure that personal data is secure	
Provision 5.8-1 R C (21)	
Provision 5.8-2 M C (22)	PASS
Provision 5.8-3 M C (23)	PASS
5.9 Make systems resilient to outages	
Provision 5.9-1 R	
Provision 5.9-2 R	
Provision 5.9-3 R	
5.10 Examine system telemetry data	
Provision 5.10-1 R C (6)	
5.11 Make it easy for users to delete user data	
Provision 5.11-1 M C (24)	PASS

Provisions number and title	
Reference	VERDICT
Provision 5.11-2 R C (25)	
Provision 5.11-3 R C (26)	
Provision 5.11-4 R C (26)	
5.12 Make installation and maintenance of devices easy	
Provision 5.12-1 R	
Provision 5.12-2 R	
Provision 5.12-3 R	
5.13 Validate input data	
Provision 5.13-1 M C (27)	PASS
6 Data protection provisions for consumer IoT	
Provision 6-1 M C (28)	PASS
Provision 6-2 M C (7)	PASS
Provision 6-3 M C (7)	PASS
Provision 6-4 R C (6)	
Provision 6-5 M C (6)	PASS
<p><i>Notes:</i></p> <ul style="list-style-type: none"> ▪ <i>M: the provision is a mandatory requirement</i> ▪ <i>R: the provision is a recommendation</i> ▪ <i>MC: the provision is a mandatory requirement and conditional</i> ▪ <i>RC: the provision is a recommendation and conditional</i> 	

Conditions

- 1) passwords are used
- 2) pre-installed unique per device passwords are used
- 3) software components are not updateable
- 4) the device is constrained
- 5) the device is not constrained
- 6) telemetry data being collected
- 7) personal data is processed on the basis of consumers' consent
- 8) the device allowing user authentication
- 9) the device supports automatic updates and/or update notifications
- 10) a hard-coded unique per device identity is used for security purposes
- 11) updates are delivered over a network interface
- 12) an update mechanism is implemented
- 13) a debug interface is physically accessible
- 14) sensitive security parameters are stored persistently
- 15) critical security parameters used for integrity and authenticity checks of software updates in device software or for protection of communication with associated services in device software exist
- 16) access to device functionality via a network interface in the initialized state is possible
- 17) device functionality that allows security-relevant changes in configuration via a network interface exists
- 18) critical security parameters are transmitted
- 19) critical security parameters are transmitted via remotely accessible network interfaces
- 20) critical security parameters relating to the device exist
- 21) personal data is transmitted between a device and a service
- 22) sensitive personal data is transmitted between a device and a service
- 23) external sensing capabilities exist
- 24) user data is stored on the device
- 25) personal data is stored on associated services
- 26) personal data is stored
- 27) data input via user interfaces or transferred via APIs or between networks in services and devices is supported
- 28) personal data is processed.