kaspersky

Security Maturity Certificate

Certificate holder

Bosch Security Systems B.V.

P.O. Box 80002, 5600 JB Eindhoven, The Netherlands

Date of issue	**Date of expiration**
27 Sept 2021	27 Sept 2023

Certified product

BOSCH IP video surveillance camera platforms

Applicable product line

CPP14, CPP13, CPP7.3, CPP7, CPP6

Firmware version(s)

Starting with
FW 8.20.0126 (CPP14)
FW 8.10.0075 (CPP13)
FW 7.81 (CPP7.3, CPP7, CPP6)

Security Maturity Target ID

2021-0009-BOSCH-IPC

Security Maturity Target and Assessment Report

https://kas.pr/9xin

Applicable models

CPP14: FLEXIDOME multi 7000i, FLEXIDOME panoramic 5100i

CPP13: AUTODOME inteox 7000i, MIC inteox 7100i

CPP7.3: AUTODOME IP 4000i, AUTODOME IP 5000i, AUTODOME IP starlight 5000i (IR), AUTODOME IP starlight 7000i, DINION IP 3000i, DINION IP bullet 4000i, DINION IP bullet 5000, DINION IP bullet 5000i, DINION IP bullet 6000i, FLEXIDOME IP 3000i, FLEXIDOME IP 4000i, FLEXIDOME IP 5000i, FLEXIDOME IP starlight 5000i (IR), FLEXIDOME IP starlight 8000i, MIC IP starlight 7000i, MIC IP starlight 7100i, MIC IP ultra 7100i, MIC IP fusion 9000i

CPP7: DINION IP starlight 6000, DINION IP starlight 7000, DINION IP thermal 8000, FLEXIDOME IP starlight 6000, FLEXIDOME IP starlight 7000, DINION IP thermal 9000 RM

CPP6: AVIOTEC IP starlight 8000, DINION IP starlight 8000 12MP, DINION IP ultra 8000 12MP

Vulnerability Research Report number

2021-0009-0002-VR

Terms and conditions of the certificate

1. This Certificate provides the following guarantees:
   a. that the current practices adopted to support product security are in line with the Security Maturity Target indicated on this Certificate.
   b. that the product vendor has implemented the infrastructure, organizational measures, processes, procedures, policies, tools and methods required to maintain the comprehensiveness level of all security practices defined in the Security Maturity Target and address the specific issues identified at the industry and system scope levels in the Security Maturity Target definition.

   This Certificate is issued based on the results of certification tests, including technical and vulnerability assessments.
2. All terms used in this Certificate should be construed to have meanings defined in the IIC Security Maturity Model (https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf);
3. This Certificate is valid until the Date of Expiration indicated on it, provided that the conditions of validity are not breached before that date.
4. Factors limiting the validity of this Certificate may include clear signs of failure to follow the security practices that we re described as implemented when demonstrating conformance with the Security Maturity Target. Such signs may include:
   a. software vulnerabilities that were not properly addressed in accordance with the procedure and within the time frame meeting the requirements defined in the Security Maturity Target*;
   b. incidents that were not handled in accordance with the procedure and policies defined in the Security Maturity Target;
   c. demonstrated attitude towards cybersecurity risk that is significantly different from that specified in the Security Maturity Target;
   d. unavailability of important information, including information on practices implemented in accordance with the guidelines and recommendations contained in the Security Maturity Target, as well as information on the appropriate comprehensiveness level and target scope;
   e. other clear signs that the security practices described as implemented when demonstrating conformance with the Security Maturity Target were in fact not followed.
5. The Certificate can be revoked in the event of the existence of factors described in paragraph 4 above.

* Although the certification body has used its best effort and expertise to perform a comprehensive security analysis of the certified product, the certificate does not guarantee that all security vulnerabilities or weaknesses have been identified in the process of certification or that the product is not vulnerable or susceptible to exploitation and will not eventually be breached. This means that, if a new vulnerability is identified, the certificate will remain valid, provided that the vendor fully addresses the vulnerability in accordance with the procedure and within the time frame meeting the requirements defined in the Security Maturity Target.

Visit webpage to get full information