Security Systems

BOSCH

From BT-VS/MKP	Product Management		Nuremberg 12.12.2022

Release Letter

Products:	***Combined Recovery Firmware for*** ***CPP7.3 UHD/HD/MP cameras*** ***CPP7 HD/MP cameras*** ***CPP6 UHD/MP cameras*** ***CPP4 HD cameras***
Version:	***7.81****.2022 Recovery*

This letter contains latest information about the above-mentioned firmware version.

1 General

This firmware release is a combined **recovery firmware package**, applicable to H.264 and H.265 products based on one of the following platforms.
It can be used to upgrade recovery firmware on cameras of the applicable platforms running firmware version 6.51 or higher.

Every camera includes a recovery firmware with limited functionality in order to allow recovery from a fault or corruption of the normal firmware.

The recovery image can only be booted with administrative rights or with physical access to the camera and allows the upload of a new firmware in case of a damaged firmware.

From			Nuremberg
BT-VS/MKP	Product Management		12.12.2022

This firmware supports:

- CPP7.3 HD and UHD cameras
    - upgrade recovery firmware to latest FW 7.81.0060
- CPP7 HD cameras
    - upgrade recovery firmware to latest FW 7.81.0060
- CPP6 HD and UHD cameras
    - upgrade recovery firmware to latest FW 7.81.0060
- CPP4 HD and MP cameras
    - upgrade recovery firmware to latest FW 7.10.0095

Recovery firmware is not distributed as separate firmware files, only in combined form.

2 Installation Notes

- Installation of this recovery firmware does not alter or impact the operation of the normal firmware image, but a reboot of the camera is required after upload.
- As a corrupt recovery firmware will render the camera unusable if also the normal firmware gets corrupt, make sure you do not lose power during the installation of the recovery firmware. The recovery firmware is smaller due to its limited functionality and takes only a few seconds to install, reducing the potential risk of failure.

3 Important notes

3.1 End of Feature for CPP4 – Maintenance mode started

With release of FW 7.10, feature implementation for the CPP4 platform ends, and the firmware development will switch over into maintenance mode. The firmware branch for CPP4 is now treated as a **long-term supported firmware (LTSFW)**, with its code base frozen to allow bug fixing and applying security fixes where necessary.

3.2 Two-factor authenticated firmware signature

The security of the signature of the firmware file has been strengthened by using a two-factor authentication process for signing the final firmware file. This new process has been prepared for with firmware 6.50 and comes into effect with succeeding versions, from firmware 6.51 onwards.

The new signature protects from non-released versions being installed in production systems. As a result, pre-release (beta) versions, required sometimes in projects, need to have a special license installed prior to the firmware update. Requests for pre-release versions need to be handled via tech support tickets in order to allow tracking and require a concession signed by the customer.

Note:

> This combined firmware file is not applicable to devices running firmware older than FW 6.51 due to the two-factor authenticated release signature and firmware file encryption.
> For such devices apply the unsigned combined firmware file or the platform-specific firmware up to firmware 6.51 before using this combined and signed firmware.

3.3 Firmware file encryption

This combined and signed firmware includes signed and encrypted firmware files only. Thus, only platforms that support firmware file decryption are applicable to this combined and signed firmware.

3.4 Secure Element (“TPM”)

All devices incorporate a secure microcontroller, which we call our Secure Element.
“A Secure Element is a tamper-resistant platform capable of securely hosting applications and their confidential and cryptographic data (for example cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities.”[1] In this specific case the requirements are defined in the Trusted Platform Module library specification defined by the Trusted Computing Group (TCG). As the Secure Element supports the main functionalities specified by TCG, the ones needed for an IoT device, it is often referred to as a “TPM”.
Due to security reasons, the firmware or functionality of the secure crypto-microcontroller cannot be altered in the field.
Thus, not all new security features become available on devices with older secure crypto-microcontroller hardware or firmware revisions.

[1] https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf, page 1

3.5 *Open Source Software*

Bosch Security Systems is advocate of integrating open source software into its products. The use of open source software is noted in the *Service* menu on the *System Overview* page of every camera’s web interface. For general information regarding open source software in Bosch Security Systems, please visit http://www.boschsecurity.com/oss .

4 Applicable products

CPP7.3

- AUTODOME IP 4000i
- AUTODOME IP 5000i
- AUTODOME IP starlight 5000i (IR)
- AUTODOME IP starlight 5100i (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 indoor 8000i (– X series)
- FLEXIDOME IP starlight 5000i (IR)
- FLEXIDOME IP starlight 8000i
- FLEXIDOME IP starlight 8000i (– X series)
- 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

- DINION IP starlight 8000 12MP
- DINION IP ultra 8000 12MP
- DINION IP ultra 8000 12MP with C/CS mount telephoto lens
- FLEXIDOME IP panoramic 6000 12MP 180
- FLEXIDOME IP panoramic 6000 12MP 360
- FLEXIDOME IP panoramic 6000 12MP 180 IVA
- FLEXIDOME IP panoramic 6000 12MP 360 IVA
- FLEXIDOME IP panoramic 7000 12MP 180
- FLEXIDOME IP panoramic 7000 12MP 360
- FLEXIDOME IP panoramic 7000 12MP 180 IVA
- FLEXIDOME IP panoramic 7000 12MP 360 IVA

CPP4

- AUTODOME IP 4000 HD
- AUTODOME IP 5000 HD
- AUTODOME IP 5000 IR
- AUTODOME 7000 series
- DINION HD 1080p
- DINION HD 1080p HDR
- DINION HD 720p
- DINION imager 9000 HD
- DINION IP bullet 4000
- DINION IP bullet 5000
- DINION IP 4000 HD
- DINION IP 5000 HD
- DINION IP 5000 MP
- DINION IP starlight 7000 HD
- ~~EXTEGRA IP dynamic 9000~~
- ~~EXTEGRA IP starlight 9000~~
- FLEXIDOME corner 9000 MP
- FLEXIDOME HD 1080p
- FLEXIDOME HD 1080p HDR
- FLEXIDOME HD 720p
- Vandal-proof FLEXIDOME HD 1080p
- Vandal-proof FLEXIDOME HD 1080p HDR
- Vandal-proof FLEXIDOME HD 720p
- FLEXIDOME IP micro 2000 HD
- FLEXIDOME IP micro 2000 IP
- FLEXIDOME IP indoor 4000 HD
- FLEXIDOME IP indoor 4000 IR
- FLEXIDOME IP outdoor 4000 HD
- FLEXIDOME IP outdoor 4000 IR
- FLEXIDOME IP indoor 5000 HD
- FLEXIDOME IP indoor 5000 MP
- FLEXIDOME IP micro 5000 HD
- FLEXIDOME IP micro 5000 MP
- FLEXIDOME IP outdoor 5000 HD
- FLEXIDOME IP outdoor 5000 MP
- FLEXIDOME IP panoramic 5000
- IP bullet 4000 HD
- IP bullet 5000 HD
- IP micro 2000
- IP micro 2000 HD
- MIC IP dynamic 7000
- MIC IP starlight 7000
- TINYON IP 2000 family

5 Changes

In case the recovery image is booted:

- An issue is fixed where a specially crafted TCP/IP packet may cause a camera recovery image telnet interface to crash. It may also cause a buffer overflow which could enable remote code execution (CVE-2021-23850).
- An issue is fixed where a specially crafted TCP/IP packet may cause a camera recovery image web interface to crash. It may also cause a buffer overflow which could enable remote code execution (CVE-2021-23851).

For more details refer to our Security Advisory BOSCH-SA-446276-BT, published at our Security Advisory web page
https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html
or visit our PSIRT website at https://psirt.bosch.com.

Changes in updated version 7.81.2022:

- Recovery image for CPP6E included.

6 Restrictions; Known Issues

- This combined firmware file is not applicable to devices running firmware older than FW 6.51 due to the two-factor authenticated release signature and firmware file encryption.

7 System Requirements

Possible clients for configuration purposes:

- Configuration Manager 7.50 or newer
- Web Browsers:
  - Google Chrome
  - Microsoft Internet Explorer 11 or higher
  - Microsoft Edge (Chromium based)
  - Mozilla Firefox

Possible clients for operation purposes:

- Bosch Video Security App 1.2 or higher
- Bosch Video Security Client 2.0 or higher
- Web Browsers:
  - Google Chrome
  - Microsoft Internet Explorer 11 or higher
  - Microsoft Edge (Chromium based)
  - Mozilla Firefox

- DirectX 11
- MPEG-ActiveX 6.34 or newer (for IE only)