# IP Video Firmware Info Brief
## Information about firmware release and provisioning status

Publishing date

03 April 2024

# Table of contents

This Info Brief will continuously be updated whenever a new firmware is released, or a provisioning status changes.
It will not be versioned by number but by publishing date only.
Take care to refer always to the most recently published version.

Publishing date:                    **03 April 2024**

# 1   Introduction

This info brief aims to provide an overview of all firmware releases for the various Common Product Platforms (CPP) for Bosch IP cameras and video encoders. A Common Product Platform is defined mainly by the used system-on-chip (SoC), which provides the capabilities for certain resolution and framerate support as well as all hardware capabilities.
The info brief gives an insight to lifecycle management for firmware and related platforms. It explains the situation and status of a firmware, and when a firmware is provided for download, or revoked.

## 1.1   Where to find firmware

Released firmware is provided, together with other product information, on the respective page for a product within our product catalogue [1], or via the Bosch Download Area [2]. For detailed information of a specific product, the product catalogue is the recommended way to go. Those, who just need to update firmware and already know the platform which their product is based on, may directly go to the Download Area for a quicker and condensed overview.

## 1.2   Types of firmware releases

Firmware is software - and developed as such. It is just packaged together in a form that is not changeable by users within a fixed version. It changes and becomes feature-enriched over lifecycles. These enhancements are packaged into major and minor feature releases, reflected in the major and minor firmware version number. Due to continuous improvements, required fixes may be covered by maintenance releases. Continuous monitoring of public sources as well as internal security reviews may reveal findings that need to be tackled quickly, which may result in security releases.

A firmware version number is structured like the following:

| | |
|---|---|
| m | the major version |
| nn | the minor / maintenance version |
| bbbb | the sequential build number during development, always 4 digits with leading zeros |

The numbers are divided by dots, looking like m.nn.bbbb.
As an example, a firmware release version 7.10.0074 is defined by major version 7, minor version 1, the maintenance version 0 as for the initial feature release, and the build number 74 concluding the development.

## 1.3   Features and capabilities

The capability of a Bosch IP camera or encoder is driven by two forces: One is the hardware capability, defined by the Common Product Platform itself and the combined components of the product. The other is the firmware that drives this hardware. The firmware is developed on a common code basis and derived from there for the active platforms, making the feature sets of various platforms fairly similar within a certain firmware version.

## 2　Firmware lifecycle management

Bosch IP video firmware is constantly being developed to include new features and to support new platforms and products. In parallel, vulnerability scans, code reviews, static code analysis, and annually executed penetration tests by 3rd parties help increasing the overall security level and improve maturity.

## 2.1　Outdated firmware

The constant development and improvements come into effect with successive firmware releases. This continuity has an impact on previous firmware releases. Even without severe security issues, older firmware releases may become non-publishable due to accumulation of smaller issues.

For product compliance reasons, such outdated firmware is not allowed for free distribution anymore. Exception can only be granted for a very solid reason, for example integration with a management software that cannot be upgraded anymore but requires an exact firmware version to be functional. Such an exception requires a concession signed by the customer to acknowledge his awareness of potential security flaws that must be mitigated with respective measures.

## 2.2　Extended firmware support for EOL platforms

Support of a new platform is typically seamlessly introduced with a major or minor firmware release, then continued over a period of time as long as products based on this platform are shipped.

Before a platform is being discontinued, its feature set is typically considered quite mature. Once a platform reaches its end of life (EOL), its support by firmware also changes. Around that point, end of feature (EOF) will be declared, or has been already, meaning that no new features are to be expected for this platform. The firmware is split off from the continuous development and has its code base frozen to allow necessary fixes to be implemented on a stable firmware basis.

The firmware specific for this platform enters "maintenance mode". This phase covers the time where the last sold products of this platform are regularly maintained during their warranty period, providing bug fixes and security fixes to keep the product state-of-the-art. It applies to all products that are still within their warranty period, and firmware will only be tested for these products.

After that, Bosch provides "extended support" to cover the remaining timespan while the products of this platform will be serviced by Bosch, providing security fixes.
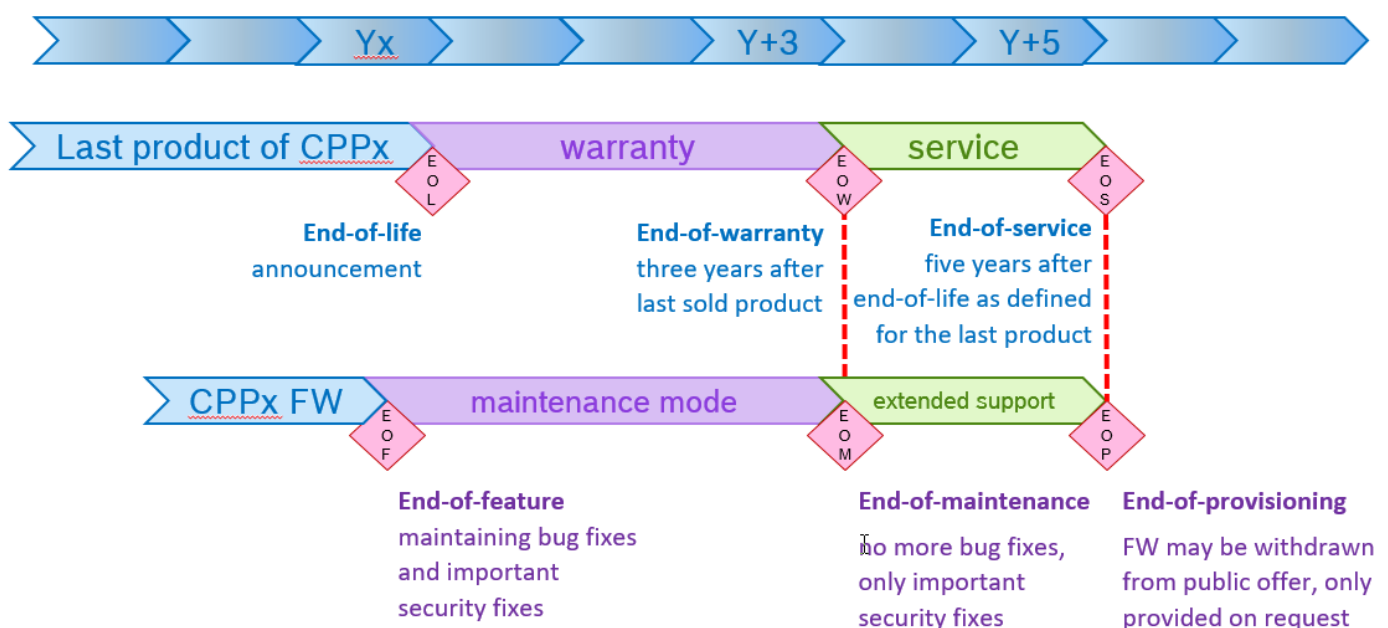


*Figure 1: Firmware maintenance lifecycle*

# 3  Firmware status and availability

## 3.1  Recent firmware for active platforms

| PLATFORM | EOF | EOM | EOS/EOP | VERSION | STATUS | AVAILABILITY | NOTES |
|---|---|---|---|---|---|---|---|
| CPP14 | | | | 9.10 | active | public | |
| CPP13, INTEOX | | | | 8.91 | active | public | |
| CPP7.3 | 05/2022 | | | 7.89 | MM | public | |
| CPP7 | 05/2022 | | | 7.89 | MM | public | |
| CPP6 | 05/2022 | | | 7.89 | MM | public | |
| AVIOTEC | 05/2022 | | | 7.82 | MM | public | |
| CPP5 | 07/2016 | 07/2019 | 10/2025 | 6.31 | ES | public | |
| CPP4 | 05/2019 | 05/2022 | 05/2024 | 7.10 | ES | public | |
| CPP3 cameras | 10/2018 | 12/2018 | 12/2023 | 5.75 | ES | public | |
| CPP3 encoders | 10/2018 | 12/2018 | 12/2023 | 5.75 | ES | public | |
| CPP-ENC | 10/2014 | 03/2018 | 03/2026 | 5.97 | ES | public | |

**Legend**
▶ Headline:
- o  EOF          End of feature development, starting maintenance mode phase.
- o  EOM          End of maintenance, starting extended support with security fixes only.
- o  EOS/EOP    End of service / end of provisioning.

▶ Status:
- o  Active        Platform is active and will potentially receive new firmware features and updates.
- o  MM           Platform firmware is in maintenance mode and will receive bug fixes and security fixes as required.
- o  ES            Platform firmware is in extended support but out of maintenance and will receive only security fixes as required.

▶ Availability:
- o  public        Firmware is publicly provided for download. Public firmware is recommended by Bosch as the most stable and secure version.
- o  revoked      Firmware is no more publicly available for download due to accumulation of various issues or vulnerabilities, requires a concession.
- o  terminated   Firmware is no more provided at all, typically if older than 5 years back, when service period expired.

## 3.2    Combined firmware files

Besides the firmware files for each platform, Bosch provides files that combine multiple firmware files for certain maintained platforms to simplify the firmware update process in case of installations with a mix of platforms. These combined firmware files also include all firmware versions that are required to be sequentially installed, so-called intermediate versions, if coming from an older installed firmware. Intermediate firmware versions introduce architectural changes and take care for compatibility when crossing over, thus are mandatory steps for upgrades and downgrades.

Instead of collecting all separate intermediate firmware files prior to starting the upgrade process and uploading them in the right order, a combined firmware file allows installing the same firmware file repeatedly until the target firmware version is reached. The camera will automatically choose the next appropriate firmware version.

There are two types of combined firmware file:
▶ one that holds firmware for certain maintained platforms including EOL platforms still in service, filename starting with "CPP_", and
▶ one that only holds firmware for certain platforms capable of working with encrypted and signed firmware, filename starting with "CPPS_".

They are named for the most-recent firmware version included, and only the latest combined firmware is provided.
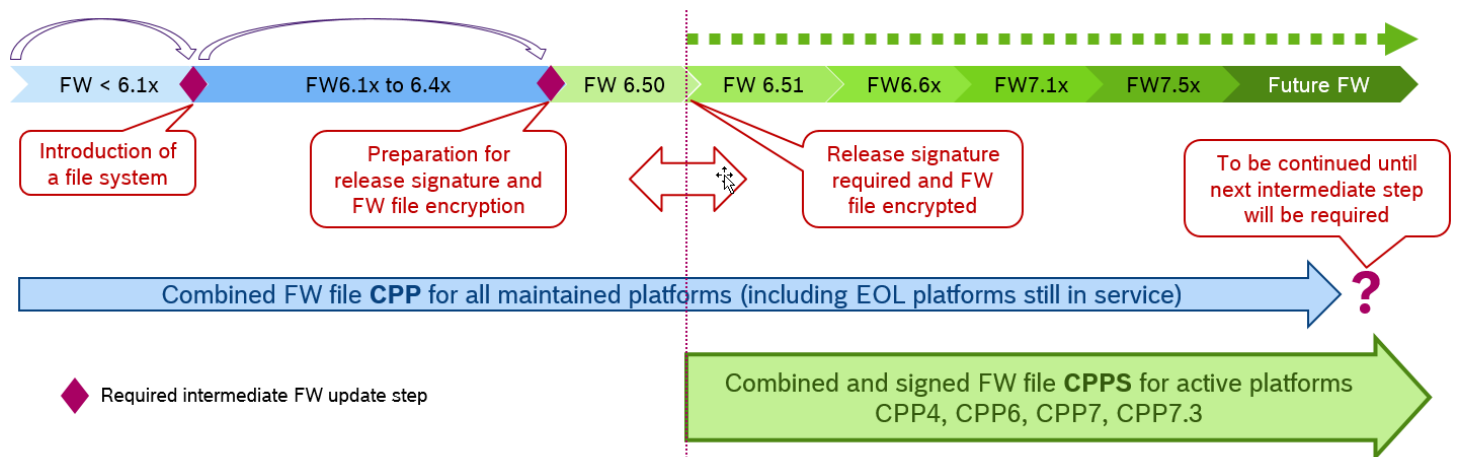


*Figure 2: Combined firmware files, timeline and availability*

The comparison table below provides hints when a certain combined firmware file is applicable.

| CPP | CPPS |
|---|---|
| Supports platforms still active or within service period: CPP-ENC, CPP3, CPP4, CPP5, CPP6, CPP7 and CPP7.3 | Supports only active platforms: CPP4, CPP6, CPP7 and CPP7.3 |
| Mix of unencrypted and encrypted files | Encrypted firmware files only |
| Not release-signed (not supported by old products and firmware) | Container and single files are all release-signed |
| Not usable with FW 6.51 and higher | Usable only with FW 6.51 and higher |
| Will be continued until new intermediate firmware upload step is required | May also include intermediate firmware upload steps in future |

Note:    Newer platforms, like CPP13 and CPP14, are not covered by these combined firmware files.

## 3.3    Firmware history of IP camera platforms

| VERSION | PLATFORMS | RELEASE DATE | STATUS | AVAILABILITY | NOTES |
|---|---|---|---|---|---|
| 9.10.0192 | CPP14 | 04/2024 | active | public | |
| 9.00.0210 | CPP14 | 11/2023 | active | replaced | Replaced by 9.10.0192 |
| 8.91.0028 | CPP13, INTEOX | 11/2023 | active | public | |
| 8.90.0037 | CPP13, INTEOX | 09/23 | active | replaced | Replaced by 8.91.0028 |
| 8.90.0036 | CPP13, INTEOX | 07/2023 | outdated | revoked | Replaced by 8.90.0037 |
| 8.80.0090 | CPP14 | 06/2023 | active | replaced | Replaced by 9.00.0210 |
| 8.71.0069 | CPP14.2 | 04/2023 | active | replaced | Replaced by 8.80.0090 |
| 8.71.0066 | CPP14 | 02/2023 | active | replaced | Replaced by 8.80.0090 |
| 8.71.0066 | CPP14.1 | 02/2023 | active | replaced | Replaced by 8.80.0090 |
| 8.71.0066 | CPP14.2 | 01/2023 | active | replaced | Replaced by 8.71.0069 |
| 8.70.0067 | CPP14.2 | 11/2022 | active | replaced | Replaced by 8.71.0066 |
| 8.51.0009 | CPP14.2 | 07/2022 | active | revoked | Replaced by 8.70.0067 |
| 8.50.0138 | CPP14.2 | 05/2022 | active | revoked | Replaced by 8.51.0009 |
| 8.48.0017 | CPP13, INTEOX | 05/2023 | active | replaced | Replaced by 8.90.0036 |
| 8.47.0026 | CPP13, INTEOX | 01/2023 | defective | revoked | Replaced by 8.48.0017 |
| 8.46.0030 | CPP13, INTEOX | 11/2022 | active | replaced | Replaced by 8.47.0026 |
| 8.45.0032 | CPP13, INTEOX | 07/2022 | active | replaced | Replaced by 8.46.0030 |
| 8.41.0029 | CPP13, INTEOX | 04/2022 | active | replaced | Replaced by 8.45.0032 |
| 8.40.0029 | CPP13, INTEOX | 01/2022 | active | replaced | Replaced by 8.41.0029 |
| 8.30.0082 | CPP14.1 | 12/2021 | active | revoked | |
| 8.20.0143 | CPP14.2 | 12/2021 | active | revoked | Replaced by 8.50.0138 |
| 8.12.0005 | CPP13, INTEOX | 09/2021 | outdated | replaced | Replaced by 8.40.0029 |
| 8.10.0075 | CPP13, INTEOX | 09/2021 | outdated | replaced | Replaced by 8.12.0005 |
| 8.00.0155 | CPP14.1 | 07/2021 | active | revoked | Replaced by 8.20.0143 |
| 8.00.0153 | CPP14.1 | 06/2021 | outdated | revoked | Initial CPP14 platform release |
| 7.89.0030 | CPP7.3, CPP7, CPP6 | 12/2023 | active | public | |
| 7.87.0029 | CPP7.3, CPP7, CPP6 | 05/2023 | active | replaced | Replaced by 7.89.0030 |
| 7.86.0019 | CPP7.3, CPP7, CPP6 | 12/2022 | active | replaced | Replaced by 7.87.0029 |
| 7.85.0016 | CPP7.3, CPP7, CPP6 | 08/2022 | active | replaced | Replaced by 7.86.0019 |

| Version | Platforms | Release date | Status | Availability | Notes |
|---------|-----------|--------------|--------|--------------|-------|
| 7.84.0023 | CPP7.3, CPP7, CPP6 | 05/2022 | active | replaced | Replaced by 7.85.0016 |
| 7.83.0027 | CPP7.3 | 02/2022 | active | replaced | Replaced by 7.84.0023 |
| 7.83.0027 | CPP7, CPP6 | 02/2022 | active | replaced | Replaced by 7.84.0023 |
| 7.82.0028 | FLEXIDOME IP 5000i (CPP7.3) | 12/2021 | active | replaced | Replaced by 7.83.0027 |
| 7.82.0025 | AVIOTEC | 12/2021 | active | public | |
| 7.82.0025 | CPP7.3 | 10/2021 | active | replaced | Replaced by 7.83.0027 |
| 7.82.0025 | CPP7, CPP6 | 10/2021 | active | replaced | Replaced by 7.83.0027 |
| 7.81.0060 | AVIOTEC | 07/2021 | outdated | replaced | Replaced by 7.82.0025 |
| 7.81.0060 | CPP7.3 | 07/2021 | outdated | replaced | Replaced by 7.82.0025 |
| 7.81.0060 | CPP7, CPP6 | 07/2021 | outdated | replaced | Replaced by 7.82.0025 |
| 7.80.0129 | CPP7.3, CPP7, CPP6 | 06/2021 | vulnerable | revoked | Replaced by 7.81.0060 |
| 7.80.0128 | CPP7.3, CPP7, CPP6 | 04/2021 | vulnerable | revoked | Replaced by 7.80.0129 |
| 7.80.0127 | CPP7.3, CPP7, CPP6 | 03/2021 | vulnerable | revoked | Replaced by 7.80.0128 |
| 7.75.0008 | CPP13, INTEOX | 06/2021 | outdated | replaced | Replaced by 8.10.0075 |
| 7.75.0006 | CPP13, INTEOX | 12/2020 | vulnerable | revoked | |
| 7.72.0013 | AVIOTEC | 06/2021 | vulnerable | revoked | Replaced by 7.81.0060 |
| 7.72.0008 | AVIOTEC | 11/2020 | vulnerable | revoked | |
| 7.72.0008 | CPP7.3, CPP7 | 11/2020 | vulnerable | revoked | Replaced by 7.80.0128 |
| 7.70.0098 | CPP13, INTEOX | 12/2020 | vulnerable | revoked | Initial INTEOX platform release, replaced by 7.75.006 |
| 7.70.0126 | CPP7.3, CPP7, AVIOTEC | 08/2020 | vulnerable | revoked | Replaced by 7.80.0128 |
| 7.70.0126 | CPP6 | 08/2020 | vulnerable | revoked | Replaced by 7.80.0128 |
| 7.62.0005 | CPP7.3, CPP7, CPP6 | 06/2021 | vulnerable | revoked | Replaced by 7.81.0060 |
| 7.62.0003 | CPP7.3 | 07/2020 | vulnerable | revoked | |
| 7.61.0026 | CPP7.3 | 05/2020 | vulnerable | revoked | Replaced by 7.62.0003 |
| 7.61.0023 | CPP7.3 | 04/2020 | vulnerable | revoked | |
| 7.61.0023 | CPP7, CPP6, AVIOTEC | 04/2020 | vulnerable | revoked | |
| 7.61.0019 | AVIOTEC | 03/2020 | vulnerable | revoked | Replaced by 7.61.0023 |
| 7.60.0118 | CPP7.3, CPP7, CPP6 | 02/2020 | vulnerable | revoked | |
| 7.60.0116 | CPP7.3, CPP7, CPP6 | 01/2020 | vulnerable | revoked | |
| 7.50.0079 | CPP7.3, CPP7, CPP6, AVIOTEC | 08/2019 | vulnerable | revoked | |

| VERSION | PLATFORMS | RELEASE DATE | STATUS | AVAILABILITY | NOTES |
|---------|-----------|--------------|--------|--------------|-------|
| 7.10.0096 | CPP4 | 06/2021 | active | public | |
| 7.10.0095 | CPP4 | 06/2021 | outdated | replaced | Replaced by 7.10.0096 |
| 7.10.0076 | CPP4 | 07/2019 | vulnerable | revoked | |
| 7.10.0074 | CPP7.3, CPP7, CPP6 | 05/2019 | vulnerable | revoked | |
| 7.10.0074 | CPP4 | 05/2019 | vulnerable | revoked | |
| 6.61.0025 | CPP7.3, CPP7, CPP6, CPP4, AVIOTEC | 03/2019 | vulnerable | revoked | |
| 6.60.0065 | CPP7.3, CPP7, CPP6, CPP4 | 01/2019 | vulnerable | revoked | Replaced by 6.61.0025 |
| 6.51.0028 | CPP7.3, CPP7, CPP6, CPP4 | 01/2019 | vulnerable | revoked | Replaced by 6.60.0065 |
| 6.51.0026 | CPP7.3, CPP7, CPP6, CPP4 | 09/2018 | vulnerable | revoked | |
| 6.50.0133 | CPP7.3, CPP7, CPP6, CPP4 | 01/2019 | vulnerable | public | In combined file for upgrading only, Intermediate version * |
| 6.50.0128 | CPP7.3, CPP7, CPP6, CPP4 | 06/2018 | vulnerable | revoked | |
| 6.11.0030 | CPP6, CPP4 | 12/2019 | vulnerable | public | In combined file only, Intermediate version * |
| 5.75.0011 | CPP3 | 08/2019 | ES | public | |

**Legend**

▶ Status:
- o  Active       Platform is active and will potentially receive new firmware features and updates
- o  Defective    Firmware has critical known issues and is revoked and replaced by a newer version
- o  ES           Firmware is in extended support and will receive only security fixes as required
- o  Outdated     Firmware is outdated, may have had findings, and is replaced by a newer version
- o  Vulnerable   Firmware has known vulnerabilities and is replaced by a newer version

▶ Availability:
- o  public       Firmware is publicly provided for download. Public firmware is recommended by Bosch as the most stable and secure version.
- o  replaced     Firmware is replaced by a newer version but is still publicly provided and can be downloaded. Replaced firmware is still secure but maybe missing features.
- o  revoked      Firmware is no more publicly available for download due to accumulation of various issues or security vulnerabilities, requires concession.
- o  terminated   Firmware is no more provided at all, typically if older than 5 years back, when service period expired.

▶ Notes:
   * Intermediate versions are required steps in an upgrade path to higher firmware versions.
     They are not recommended as final version if newer versions are available.

   Any older version, not mentioned in the above or below list, is considered terminated.

## 3.4   Firmware history of IP encoders / decoders / transcoders

| VERSION | PLATFORMS | RELEASE DATE | STATUS | AVAILABILITY | NOTES |
|---------|-----------|--------------|--------|--------------|-------|
| 6.31.0019 | CPP5 | 01/2023 | ES | public | |
| 6.31.0010 | CPP5 | 07/2019 | vulnerable | terminated | |
| 6.31.0007 | CPP5 | 01/2019 | vulnerable | terminated | |
| 6.31.0003 | CPP5 | 08/2019 | vulnerable | terminated | |
| 6.30.0059 | CPP5 | 04/2018 | vulnerable | terminated | |
| 6.30.0047 | CPP5 | 07/2016 | vulnerable | terminated | |
| 5.97.0013 | CPP-ENC | 12/2018 | ES | public | |
| 5.93.0026 | CPP-ENC | 06/2016 | vulnerable | terminated | |
| 5.92.0027 | CPP-ENC | 08/2014 | vulnerable | terminated | |
| 5.92.0029 | CPP5 | 11/2015 | vulnerable | terminated | |
| 5.92.0026 | CPP5 | 09/2015 | vulnerable | terminated | |
| 5.92.0023 | CPP5 | 12/2014 | vulnerable | terminated | |
| 5.92.0006 | CPP5 | 08/2014 | vulnerable | terminated | |
| 5.90.0070 | CPP5 | 04/2014 | vulnerable | terminated | |
| 5.90.0064 | CPP5 | 02/2014 | vulnerable | terminated | |
| 5.85.0040 | CPP-ENC | 11/2013 | vulnerable | terminated | |
| 5.75.0011 | CPP3 | 08/2019 | ES | public | |
| 5.75.0004 | CPP3 | 09/2018 | outdated | terminated | |
| 5.75.0002 | CPP3 | 08/2018 | outdated | terminated | |
| 5.74.0010 | CPP3 | 04/2018 | outdated | terminated | |
| 5.74.0004 | CPP3 | 07/2017 | outdated | terminated | |
| 5.74.0001 | CPP3 | 03/2017 | vulnerable | terminated | |
| 5.70.0028 | CPP5 | 06/2013 | vulnerable | terminated | |
| 5.70.0023 | CPP5 | 03/2013 | vulnerable | terminated | |
| 5.70.0020 | CPP5 | 01/2013 | vulnerable | terminated | |
| 5.60.0061 | CPP-ENC | 06/2013 | vulnerable | terminated | |
| 5.54.0012 | CPP-ENC | 12/2018 | ES | terminated | VIP-X1600 only |
| 5.54.0004 | CPP-ENC | 08/2018 | outdated | terminated | |
| 5.53.0004 | CPP-ENC | 07/2017 | outdated | terminated | |
| 5.52.0031 | CPP-ENC | 10/2016 | vulnerable | terminated | |

## 4   References

| REFERENCE | TARGET | LINK |
| --- | --- | --- |
| 1 | Bosch Security Systems Product Catalogue | Via https://www.boschsecurity.com/xc/en/product-catalog/ |
| 2 | Bosch Security Systems Download Area | https://downloadstore.boschsecurity.com/ |