IP video firmware info brief

Information about firmware release and provisioning status

Publishing date

09 April 2020

Table of contents

1 Introduction 3

1.1 Where to find firmware 3

1.2 Types of firmware releases 3

1.3 Features and capabilities 3

2 Firmware lifecycle management 4

2.1 Outdated firmware 4

2.2 Extended firmware support for EOL platforms 4

3 Firmware status and availability 5

3.1 Recent firmware for active platforms 5

3.2 Combined firmware files 6

3.3 Firmware history of IP camera platforms 7

3.4 Firmware history of IP encoders / decoders / transcoders 10

4 References 11

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: **09 April 2020**

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 improvement comes 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 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.

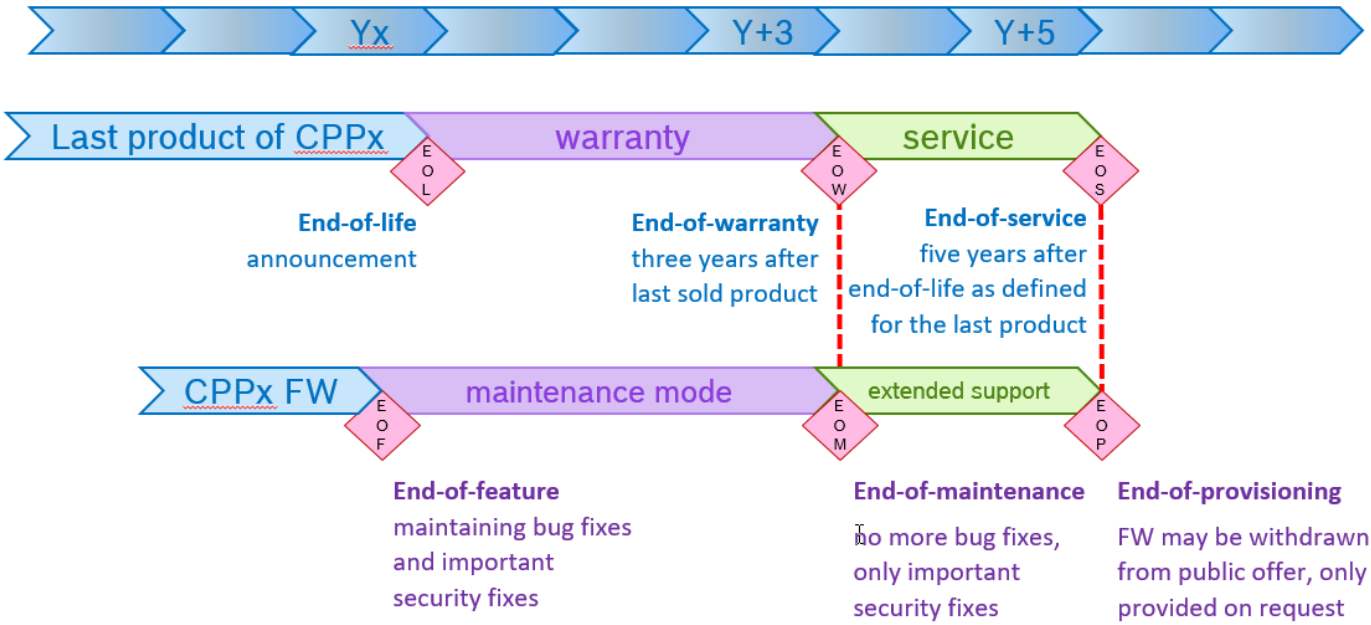

Figure 1: Firmware maintenance lifecycle

3 Firmware status and availability

3.1 Recent firmware for active platforms

Platform	EOF	EOM	EOS/EOP	Version	Status	Availability	Notes
CPP7.3				7.61	active	public	
CPP7				7.61	active	public	
AVIOTEC				7.61	active	public	
CPP6				7.61	active	public	
CPP5	07/2016			6.31	ES	public	
CPP4	05/2019			7.10	MM	public	
CPP4	12/2018	12/2019	12/2021	6.32	ES	public	EXTEGRA only
CPP3 cameras	10/2018	12/2018	12/2023	5.75	ES	public	
CPP3 encoders	10/2018	12/2021	12/2023	5.75	MM	public	
CPP-ENC	10/2014			5.97	MM	public	
CPP-ENC	07/2012	12/2019	12/2021	5.54	MM	public	VIP-X1600 only

Legend

- Headline:
  - EOF — End of feature development, starting maintenance mode phase
  - EOM — End of maintenance, starting extended support with security fixes only
  - EOS/EOP — End of service / end of provisioning
- Status:
  - Active — Platform is active and will potentially receive new firmware features and updates
  - MM — Platform firmware is in maintenance mode and will receive bug fixes and security fixes as required
  - ES — Platform firmware is in extended support but out of maintenance and will receive only security fixes as required

3.2 Combined firmware files

Besides the firmware files for each platform, Bosch provides files that combine multiple firmware files for all 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 all maintained platforms including EOL platforms still in service, filename starting with “CPP_”
- and one that only holds firmware for the platforms capable of working with encrypted and signed firmware, filename starting with “CPPS_”.

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

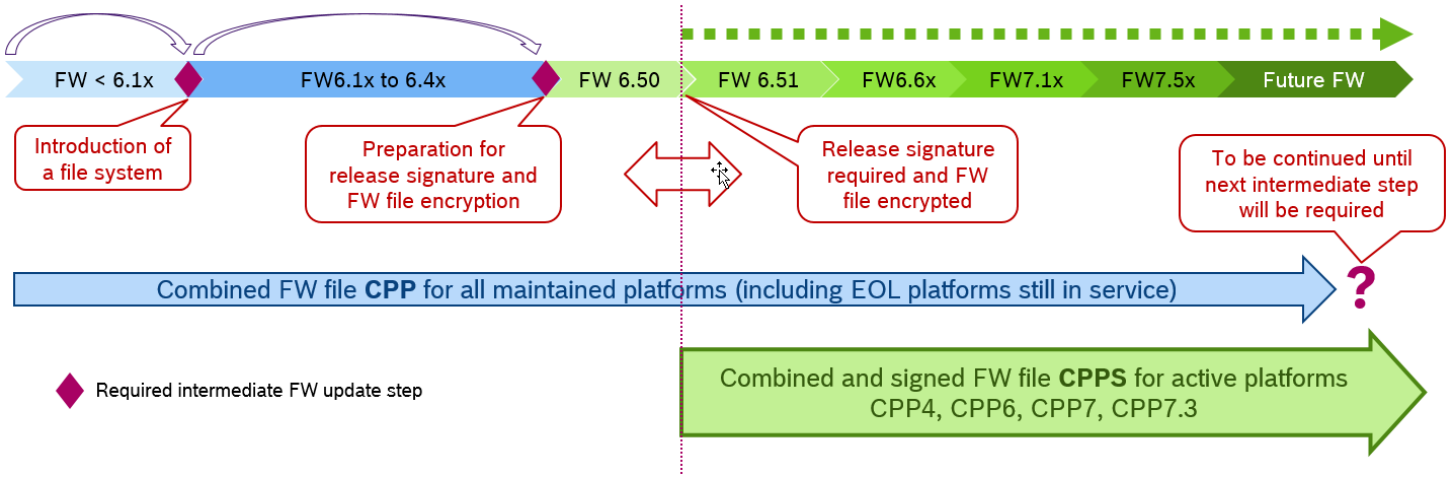

Figure 2: Combined firmware files, timeline and availability

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

CPP	CPPS
Supports all 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

3.3 Firmware history of IP camera platforms

Version	Platforms	Release date	Status	Availability	Notes
7.61.0023	CPP7.3, CPP7, CPP6, AVIOTEC	04/2020	active	public	
7.61.0019	AVIOTEC	03/2020	active	replaced	Replaced by 7.61.0023
7.60.0118	CPP7.3, CPP7, CPP6	02/2020	active	replaced	Replaced by 7.61.0023
7.60.0116	CPP7.3, CPP7, CPP6	01/2020	outdated	replaced	Replaced by 7.60.0118
7.50.0079	CPP7.3, CPP7, CPP6, AVIOTEC	08/2019	active	replaced	Replaced by 7.60.0116
7.10.0074	CPP7.3, CPP7, CPP6	05/2019	active	replaced	Replaced by 7.50.0079
7.10.0076	CPP4	07/2019	MM	public	
7.10.0074	CPP4	05/2019	outdated	replaced	Replaced by 7.10.0076
6.61.0025	CPP7.3, CPP7, CPP6, CPP4, AVIOTEC	03/2019	active	replaced	Replaced by 7.10.0074, except AVIOTEC
6.60.0065	CPP7.3, CPP7, CPP6, CPP4	01/2019	outdated	replaced	Replaced by 6.61
6.51.0028	CPP7.3, CPP7, CPP6, CPP4	01/2019	outdated	replaced	Replaced by 6.60
6.51.0026	CPP7.3, CPP7, CPP6, CPP4	09/2018	vulnerable	revoked	Replaced by 6.51.0028
6.50.0133	CPP7.3, CPP7, CPP6, CPP4	01/2019	outdated	public	In combined file only, Intermediate version *
6.50.0128	CPP7.3, CPP7, CPP6, CPP4	06/2018	vulnerable	revoked	
6.44.0027	CPP7.3, CPP7, CPP6, CPP4	01/2019	outdated	revoked	
6.44.0020	CPP7.3, CPP7, CPP6, CPP4	05/2018	vulnerable	revoked	
6.43.0027	CPP7.3, CPP7, CPP6, CPP4	01/2018	vulnerable	revoked	
6.42.0021	CPP7.3, CPP7, CPP6, CPP4	11/2017	vulnerable	revoked	
6.41.0037	CPP7.3, CPP7, CPP6, CPP4	09/2017	vulnerable	revoked	
6.40.0240	CPP7.3, CPP7, CPP6, CPP4	07/2017	vulnerable	revoked	
6.40.0232	CPP7, CPP6, CPP4	07/2017	vulnerable	revoked	
6.32.0124	CPP4 (EXTEGRA)	12/2018	outdated	public	EXTEGRA only
6.32.0123	CPP7, CPP6, CPP4	09/2018	vulnerable	revoked	
6.32.0111	CPP7, CPP6, CPP4	04/2017	vulnerable	revoked	
6.32.0109	CPP7, CPP6, CPP4	12/2016	vulnerable	revoked	
6.32.0099	CPP7, CPP6, CPP4	09/2016	vulnerable	revoked	
6.30.0140	CPP7, CPP6, CPP4	08/2016	vulnerable	revoked	
6.30.0136	CPP7, CPP6, CPP4	07/2016	vulnerable	revoked	
6.22.0007	CPP6, CPP4	04/2016	vulnerable	revoked	

6.21.0008	CPP6, CPP4	03/2016	vulnerable	revoked	
6.20.0089	CPP6, CPP4	12/2015	vulnerable	revoked	
6.11.0030	CPP6, CPP4	12/2019	outdated	public	In combined file only, Intermediate version *
6.11.0026	CPP6, CPP4	11/2018	vulnerable	revoked	
6.11.0021	CPP6, CPP4	08/2015	vulnerable	revoked	
6.11.0019	CPP6, CPP4	07/2015	vulnerable	revoked	
6.11.0006	CPP6	06/2015	vulnerable	revoked	
6.10.0129	CPP6, CPP4	06/2015	vulnerable	revoked	
6.10.0128	CPP4	05/2015	vulnerable	revoked	
6.10.0127	CPP6	05/2015	vulnerable	revoked	
6.10.0126	CPP4	05/2015	vulnerable	revoked	
5.93.0025	CPP4	10/2014	vulnerable	revoked	
5.92.0090	CPP4	07/2014	vulnerable	revoked	
5.90.0126	CPP4	05/2014	vulnerable	revoked	
5.90.0112	CPP4	02/2014	vulnerable	revoked	
5.90.0098	CPP4	01/2014	vulnerable	revoked	
5.85.0016	CPP4	09/2013	vulnerable	revoked	
5.80.0073	CPP4	06/2013	vulnerable	revoked	
5.75.0011	CPP3	08/2019	ES	public	
5.75.0004	CPP3	09/2018	outdated	revoked	
5.75.0002	CPP3	08/2018	outdated	revoked	
5.74.0010	CPP3	04/2018	outdated	revoked	
5.74.0004	CPP3	07/2017	outdated	revoked	
5.74.0001	CPP3	03/2017	vulnerable	revoked	

Legend

- Status:
  - Active — Platform is active and will potentially receive new firmware features and updates
  - MM — Firmware is in maintenance mode and will receive bug fixes and security fixes as required
  - ES — Firmware is in extended support and will receive only security fixes as required
  - Outdated — Firmware is outdated, may have had findings, and is replaced by a newer version
  - Vulnerable — Firmware has known vulnerabilities and is replaced by a newer version

  Note:
  Outdated or vulnerable firmware versions are not available for free distribution. If required for good reason, a concession must be signed by the customer to acknowledge the risk of known issues.
- Availability:
  - public — Firmware is publicly provided for download
  - replaced — Firmware is replaced by a newer version but can still be requested without concession
  - revoked — Firmware is no more publicly available for download due to accumulation of various issues or vulnerabilities, requires concession
- 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.

3.4 Firmware history of IP encoders / decoders / transcoders

Version	Platforms	Release date	Status	Availability	Notes
6.31.0010	CPP5	07/2019	ES	public	
6.31.0007	CPP5	01/2019	outdated	revoked	
6.31.0003	CPP5	08/2019	outdated	revoked	
6.30.0059	CPP5	04/2018	outdated	revoked	
6.30.0047	CPP5	07/2016	outdated	revoked	
5.97.0013	CPP-ENC	12/2018	ES	public	
5.93.0026	CPP-ENC	06/2016	vulnerable	revoked	
5.92.0027	CPP-ENC	08/2014	vulnerable	revoked	
5.92.0029	CPP5	11/2015	vulnerable	revoked	
5.92.0026	CPP5	09/2015	vulnerable	revoked	
5.92.0023	CPP5	12/2014	vulnerable	revoked	
5.92.0006	CPP5	08/2014	vulnerable	revoked	
5.90.0070	CPP5	04/2014	vulnerable	revoked	
5.90.0064	CPP5	02/2014	vulnerable	revoked	
5.85.0040	CPP-ENC	11/2013	vulnerable	revoked	
5.75.0011	CPP3	08/2019	MM	public	
5.75.0004	CPP3	09/2018	outdated	revoked	
5.75.0002	CPP3	08/2018	outdated	revoked	
5.74.0010	CPP3	04/2018	outdated	revoked	
5.74.0004	CPP3	07/2017	outdated	revoked	
5.74.0001	CPP3	03/2017	vulnerable	revoked	
5.70.0028	CPP5	06/2013	vulnerable	revoked	
5.70.0023	CPP5	03/2013	vulnerable	revoked	
5.70.0020	CPP5	01/2013	vulnerable	revoked	
5.60.0061	CPP-ENC	06/2013	vulnerable	revoked	
5.54.0012	CPP-ENC	12/2018	ES	public	VIP-X1600 only
5.54.0004	CPP-ENC	08/2018	outdated	revoked	
5.53.0004	CPP-ENC	07/2017	outdated	revoked	
5.52.0031	CPP-ENC	10/2016	vulnerable	revoked	
5.52.0015	CPP-ENC	11/2012	vulnerable	revoked	

4 References

Reference	Target	Link
1	Bosch Security Systems Product Catalogue	Via https://www.boschsecurity.com/
2	Bosch Security Systems Download Area	https://downloadstore.boschsecurity.com/

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com