Long-Term Firmware Support Policy

July 2024

V3.0

Copyright ⓒ 2024 Hanwha Vision Co., Ltd. All rights reserved.

Contents

Revision History

Version	Date	Details
V1.0	June 5, 2018	Established long-term firmware support policy for cybersecurity
V1.1	July 11, 2018	Modified update step
V2.0	October 23, 2019	Modified continuous firmware improvement phase (Support for 5 to 10 years → Support for 5 years after product discontinuation)
V2.1	March 22, 2021	Modified continuous firmware management phase (Support 5 to 10 years after product release → Support up to 5 years after product discontinuation)
V2.2	April 10, 2023	Modified templates with rebranding
V3.0	July 12, 2024	Added Firmware enhancements and fixes and clarifying some of the terms being used

1. Introduction

This document explains the Long-Term Firmware Support for all Hanwha Vision's IP cameras. This policy covers cybersecurity, new features, performance enhancements, and bug fixes. It spans from before the launch of the product, through its lifecycle, and after its end-of-life.

Hanwha Vision has established this policy to ensure quick and efficient responses to cybersecurity vulnerabilities, new features requests, improvements, OS updates, performance enhancements, and bug fixes.

The firmware long-term support policy applies as follows:

■ Network Camera

Firmware version 1.30 or higher

[Network camera version structure]

MODEL NAME_#.##.##_YYMMDD

Example: XND-8080R_1.31.00_20190905

- Policies do not apply if the network camera version is below 1.30 or if the version structure is "0.00.YYMMDD".

■ Recorder

Firmware version 3.00 or higher

[Recorder version structure]

MODEL NAME_#.##.##_YYMMDD

Example: HRX-1621_3.01.00_20190905171108

- Policies do not apply if the recorder version is below 3.00 or if the version structure is "0.00.YYMMDD".

2. Cybersecurity Firmware Update

Hanwha Vision offers firmware updates with enhanced cybersecurity through four phases:

2.1. Before Product Launch Phase

Hanwha Vision ensures that all the Open-Source Software (OSS) is secure and up to date. Additionally, an external company is hired to conduct aggressive penetration testing and a comprehensive evaluation of our firmware to maximize security at the time of launch.

2.2. Aggressive Firmware Improvement Phase (up to 2 years after product release)

Hanwha Vision continues aggressive firmware update activities to improve cybersecurity related to access control and image information protection (confidentiality, integrity, availability) for two years after the product launch.

Through regular self-penetration testing, security checking, and reported or known vulnerabilities, we take actions to address and prevent the exploitation of unknown security threats or potential risks. The following are specific examples of aggressive firmware improvement activities.

1) Security Vulnerability Response

Security incidents (security vulnerabilities) reported from external sources are quickly responded to and followed up by Hanwha Vision's security response rules. Improved firmware is quickly sent to customers according to the security vulnerability disclosure policy.

- Refer to *Security Vulnerability Disclosure Policy* on the Hanwha Vision website

2) Product Security Improvement

Hanwha Vision constantly conducts developer-led security check activities to investigate potential security vulnerabilities. We regularly perform vulnerability assessments using reverse engineering tools and penetration testing by external experts (white hackers). The results inform the development of security test cases, ensuring all products undergo rigorous security testing before release.

- Refer to *Cybersecurity White Paper* and *Network Hardening Guide* on the Hanwha Vision website

3) Differentiated Security Solution Development

In order to prevent security vulnerabilities caused by open-source software such as OpenSSL, Hanwha Vision applies device certification and a private key to each network device for fundamental improvement of communication security. Our long-term strategies include implementing differentiated network security solutions such as user authentication and video authentication.

2. Cybersecurity Firmware Update

4) Security Certification Acquisition

There is a growing interest in security certification as the importance of cybersecurity grows worldwide. In response to these changes, Hanwha Vision is working to mitigate security threats and improve product competitiveness through the acquisition of security certifications.

Hanwha Vision holds UL-CAP and applies FIPS standard security certifications, which are recognized worldwide and in the US. We utilize FIPS standard-certified TPMs and secure elements to protect our products from cybersecurity risks. Given the evolving nature of cyber threats, we continually pursue stable cybersecurity certifications on a global scale.

2.3. Proactive Firmware Improvement Phase (from the 2nd year after release until product discontinuation)

From the second year after product launch, until the product is discontinued, proactive firmware update activities are carried out to improve cybersecurity vulnerabilities related to access control and video information protection.

During this period, firmware updates are provided to reflect improvements to security vulnerabilities reported by external organizations or issues known to be potentially attackable.

Hanwha Vision immediately convenes a security countermeasures council in accordance with security response rules and analyzes the content and impact of the vulnerability when a security vulnerability is reported by external organizations. In addition, according to the security vulnerability disclosure policy, the improved firmware is distributed as soon as possible.

2.4. Continuous Firmware Improvement Phase (until 5 years after product discontinuation)

Hanwha Vision provides improved firmware if a serious security vulnerability[1] is reported in the product until 5 years after product discontinuation.

The identified issues will be resolved in a quick and thorough analysis of the security vulnerabilities in accordance with the security incident response rules.

[1] Serious Security Vulnerability: a hacker can access or disable the system without needing admin credentials

3. Firmware Enhancements and Fixes

Hanwha Vision will continue to support regular updates on our IP cameras throughout the product's lifecycle with a frequency of at least once per year.

These updates will include cybersecurity updates, performance enhancements, bug fixes and new features.

After the product is discontinued, Hanwha Vision will continue to provide updates and bug fixes according to the table below in the '4. Conclusion' section.

4. Conclusion

Hanwha Vision provides cybersecurity vulnerability fixes via firmware updates for up to five years after the discontinuation of IP cameras.

In addition, if there is a possibility that products other than network cameras and recorders are exposed to security threats due to security vulnerabilities, we will provide formal security updates for those products through official procedures.

We will endeavor to reduce the security risks for our customers.

Type	Description	Support after EOL
Cybersecurity	Serious vulnerability	5 years
Critical Bug	No workaround available	3 years
Light Bug	Workaround available	1 year
OS Updates	Operating system updates	1 year * Only when provided by SoC vendor
Feature Request	Customer feature request	1 year

5. Appendix: Network Camera Version Management

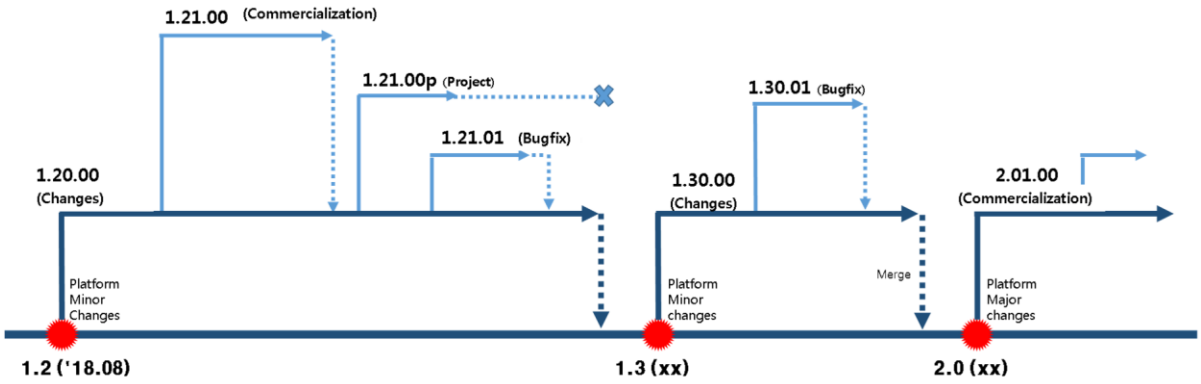
This describes the Hanwha Vision network camera version rules. A camera version is updated when new features are added or bugs are fixed, and there are the following two categories:

- Platform change: Version update due to changes in the software platform structure and major feature changes
- Product change: Version update to fix reported bugs and solve potential problems

Camera Version Management Procedure

The firmware of Hanwha Vision camera products is being developed based on the common platform, and this is developed across all camera product development.

Any features developed for a product firmware will be consolidated into the common platform and applied to new camera products accordingly.



Camera Version Rules

The camera version is structured as below and it is generated using the following rules.

<PlatformMajor>.<PlatformMinor><ProductMajor>.<ProductMinor>

5. Appendix: Network Camera Version Management

Platform: Specifies the release version of the common platform

- Major: Reflects any changes in platform structure and major feature changes.
- Minor: Reflects upgrade with new features and consolidated changes that apply to all models.

Product: Specifies the product release version

- Major: Reflects the addition of major product features and changes.
- Minor: Reflects firmware changes for minor fixes that solve reported bugs and potential problems

Each firmware release is displayed using a unique number given to each release type and is a combination of a platform version and a product version. The following examples explain the version rules.

Version 1.20.00 indicates the combination of platform version 1.2 and product version 0.00. It represents the first product that is applied with the common platform version 1.2.

Version 1.22.10 indicates the combination of platform version 1.2 and product version 2.10. It represents a product that is applied with the common platform version 1.2 and updated twice.

Hanwha Vision Co., Ltd.
13488 Hanwha Vision R&D Center,
6 Pangyo-ro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do
TEL 070.7147.8771-8
FAX 031.8018.3715
www.HanwhaVision.com

Copyright ⓒ 2024 Hanwha Vision Co., Ltd. All rights reserved.