Long-Term Firmware Support Policy

Sept. 2024

V3.1

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
V3.1	Sept. 10, 2024	Appendix: Corrected version rules, Corrected terms (Camera → Device)

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 more

[Network camera version structure]

MODEL NAME_##.##.##_YYMMDD

ex) XND-8080R_1.31.00_20190905

- If the network camera version is under 1.30 or Exclude policy if version structure is '0.00.YYMMDD'.

■ Recorder

☞ Firmware version 3.00 or more

[Recorder version structure]

MODEL NAME_##.##.##_YYMMDD

ex) HRX-1621_3.01.00_20190905171108

- If the recorder version is under 3.00 or Exclude policy if version structure is 0.00.YYMMDD'.

※ For details, refer to '5. Appendix'.

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 Device Version Management

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

- Platform change: Specifies the platform release version of the Hanwha Vision network device.

  The Major version of a platform is represented by a single or two-digit number, with the leading digit omitted when representing a single digit number.

  - 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 change: Specifies the release version for each model of Hanwha Vision network device.
  - Major: Reflects major feature additions and changes by model.
  - Minor: Reflects firmware changes for minor fixes that solve reported bugs and potential problems by model.

<Example of version notation>

Version 23.01.00 means that the platform version is 23.0 and the product version is 1.00, indicating that version 23.0 of the platform was first reflected in the product.

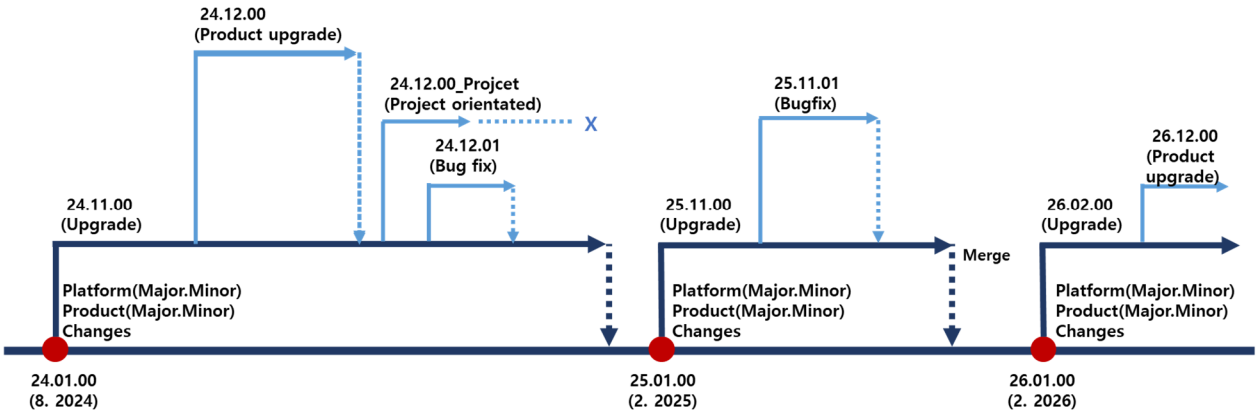
The 23.02.01 version means that there are two feature additions and one issue fix based on version 23.0 of the platform.

5. Appendix: Network Camera Version Management

If the platform version is represented by a single digit, as shown below, omit the leading digit.

Network device Version Management Procedure

The firmware of Hanwha Vision network device is being developed based on the platform. Any features developed for a product firmware will be consolidated into the platform and applied to new products accordingly.



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