Firmware Long-term Support Policy for Cyber Security

April. 2023

V2.2

Contents

Revision History

Ver.	Date	Details	Note
V1.0	5th June 2018	Long-term firmware support policy for cyber security established	
V1.1	11th July 2018	Modify update step	
V2.0	23 th October 2019	Modify continuous firmware improvement phase (Support for 5 to 10 years → Support for 5 years after product discontinuation)	
V2.1	22 th March 2021	Modify continuous firmware management phase (Support 5 to 10 years after product release → Support up to 5 years after product discontinuation)	
V2.2	10th April 2023	Modify templates with rebranding	

1. Introduction

Cyber security concern and awareness has been on the rise over the past several years. Hanwha Vision has established a firmware long-term support policy for cyber security in order to respond to cyber security issues quickly and so our customers can use the product with confidence.

Our cyber security firmware long-term support policy includes not only firmware improvement activities, but also response to security vulnerabilities and product security quality improvement activities to prevent security incidents. In order to strengthen cyber security and secure a competitive edge, we operate activities to develop differentiated security solutions and acquire various security certifications.

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'.

2. Cyber Security Firmware Update

Hanwha Vision offers firmware updates with enhanced cyber security through three phases:

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

Hanwha Vision continues aggressive firmware update activities to improve cyber security related to access control and image information protection (confidentiality, integrity, availability) for two years after 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 rule. Improved firmware is quickly sent to customers according to the security vulnerability disclosure policy.

- *Security Vulnerability Disclosure Policy* - Hanwha Vision HQ website

2) Product Security Improvement

Hanwha Vision is constantly conducting developer-led security check activities to investigate potential security vulnerabilities while regularly performing vulnerability checks using reverse engineering tools and penetration testing through external experts (white hackers). The results are used to develop security test cases. All products must pass the security test before they can be released.

- *Cyber Security White Paper*, *Network Hardening Guide* - Hanwha Vision HQ 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 vulnerability.

Also, in the long term, we will apply differentiated network security solutions such as user authentication, video authentication, and firmware electronic signature.

2. Cyber Security Firmware Update

4) Security Certification Acquisition

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

UL-CAP and FIPS 140-2 security certification is used worldwide and in the US, and there is TTA and IoT security certification in Korea for private/public institutions. Hanwha Vision is preparing to acquire TTA security certification first and planning to acquire FIPS 140-2 and UL-CAP certification in the future.

2.2. Proactive Firmware Improvement Phase (from the 2nd year after release until the product is discontinued)

From the second year after product launch, until the product is discontinued, proactive firmware update activities are carried out to improve cyber security 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 rule 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.

2.3. Continuous Firmware Improvement Phase (Until 5 years after product discontinuation)

Hanwha Vision provides improved firmware if a serious security vulnerability 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.

3. Conclusion

Hanwha Vision provides cyber security-enhanced firmware for up to five years after the discontinuation of products. And we will reach out to customers with safer and more reliable products.

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 of our customers.

4. Appendix. Network camera version management

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

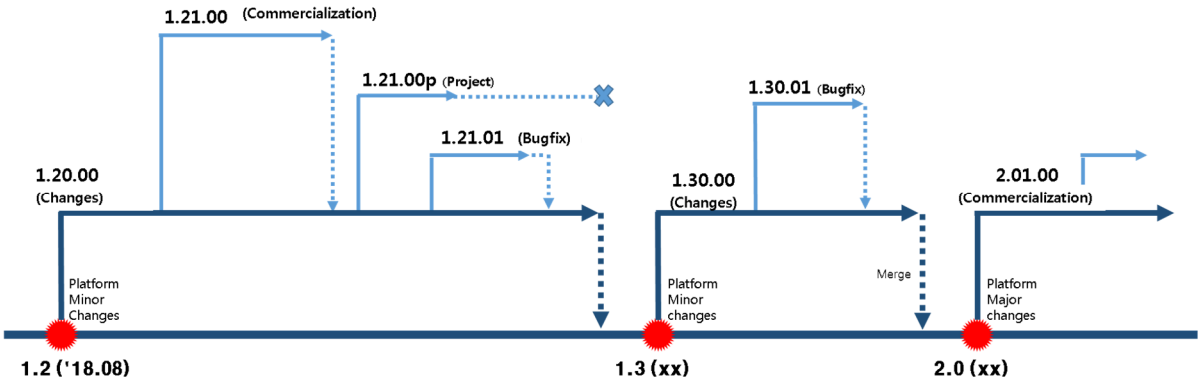
Platform change: Version update due to changes in the software platform structure and major feature changes

Product change: Version update to fix reported bugs and solve potential problems

■ Camera Version Management Procedure

The firmware of Hanwha Vision camera products are 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>

4. 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.

HEAD OFFICE

6, Pangyo-ro 319beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13488, South KOREA

TEL +82.1588.5772 www.Hanwha-Security.com