WISENET

Hanwha Techwin

Long-term Firmware Support Policy for Cyber Security

13th June 2018

Hanwha Techwin

Contents

Revision History

Ver.	Date	Details	Note
v1.0	5th June 2018	Long-term firmware support policy for cyber security established	

1. Introduction

As the awareness of cyber security has increased recently, Hanwha Techwin has established a long-term firmware support policy for cyber security so that it can respond to cyber security issues quickly and customers can use the product at ease.

Our cyber security-related long-term firmware support policy includes not only various firmware improvement activities, but also countermeasures against security vulnerabilities that occur and product security quality improvement activities to prevent security incidents. In addition, development of differentiated security solutions and acquisition of various security certifications correspond to the long-term support policy.

Long-term firmware support policy is applied to Wisenet X series network cameras and will provide firmware updates with improved security for up to 10 years.

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

2.1. Aggressive Firmware Improvement Phase (Product launch - 2 years)

Hanwha Techwin 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 test and security checking activities as well as reported or known vulnerabilities, we also take actions to 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 the outside are quickly responded to and followed up by Hanwha Techwin's security response rule. Improved firmware is quickly delivered to customers according to the security vulnerability disclosure policy.

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

2) Product Security Improvement

Hanwha Techwin is constantly conducting developer-led security check activities to investigate potential security vulnerabilities and regularly performing vulnerability check using reverse engineering tools and penetration testing through external experts (white hackers). The results lead to the development of security test cases and all products must pass the security test before they can be released.

- *Cyber Security White Paper, Network Hardening Guide - Hanwha Techwin HQ website*

3) Differentiated Security Solution Development

In order to prevent security vulnerabilities caused by open source software such as OpenSSL, Hanwha Techwin is applying device certification and 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.

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 Techwin 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 Techwin is preparing to acquire TTA security certification first and planning to acquire FIPS 140-2 and UL-CAP certification in the future.

2.2. Active Firmware Improvement Phase (2 - 5 years)

During the 2 to 5 years after product launch, Hanwha Techwin performs active firmware update activities to improve cyber security related to access control and image information protection. In this period, firmware updates include improvements for known or potential security vulnerabilities.

Hanwha Techwin 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 agencies. In addition, according to the security vulnerability disclosure policy, the improved firmware is distributed as soon as possible.

2.3. Constant Firmware Improvement Phase (5 - 10 years)

Hanwha Techwin provides improved firmware to maintain the security of the product if a serious vulnerability is reported during 5 to 10 years after the product is released.

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 Techwin will provide firmware updates up to 10 years for cyber security of Wisenet X series network camera.

The X series network cameras with Hanwha Techwin's Wisenet 5 soc, provide the world's best 150dB WDR and low-light noise reduction technology, DIS with gyro sensor, and WiseStream II video compression technology. It also has the non plug-in webviewer, USB dongle for easy installation and setup, dual SD memory slot, etc. The X series network cameras will be more reliable and valuable with the long-term firmware support policy for cyber security.

In addition, Hanwha Techwin will endeavor to provide security firmware updates through appropriate procedures for products other than X Series network cameras, if they are exposed to serious security vulnerabilities.

WISENET

Hanwha Techwin Co.,Ltd.

13488 Hanwha Techwin R&D Center,
6 Pangyoro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do
TEL (82) 70.7147.8771-8
FAX (82) 31.8018.3715
http://www.hanwha-security.com

Hanwha
Techwin