WISENET

Hanwha Techwin

Cyber Security
Long-term Firmware Support Policy

July 11, 2018

Hanwha Techwin

Contents

Revision History

Ver.	Date	Details	Note
v1.0	June 5, 2018	Long-term firmware support policy for cyber security established	
v1.1	July, 11 2018	Period of firmware improvement phase revised	

1. Introduction

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

Our cyber security related, long-term firmware support policy includes various firmware improvement activities, countermeasures against security vulnerabilities and product security quality improvement activities. In addition, the development of differentiated security solutions and the acquisition of various security certifications strengthen 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 5 years after discontinuation.

Hanwha Techwin offers firmware updates with enhanced cyber security in 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 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 Techwin's security response rule. Improved firmware is quickly sent 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 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 Techwin HQ website*

3) Differentiated Security Solution Development

In order to prevent security vulnerabilities caused by open source software such as OpenSSL, Hanwha Techwin 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.

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.

2.2. Proactive Firmware Improvement Phase (2 years - Discontinuation)

From the third year to discontinuation, Hanwha Techwin performs active firmware update activities to improve cyber security related to access control and image information protection. During 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 organizations. In addition, according to the security vulnerability disclosure policy, the improved firmware is distributed as soon as possible.

2.3. Consistent Firmware Improvement Phase (5 years after discontinuation)

Hanwha Techwin provides improved firmware to maintain the security of the product if a serious vulnerability is reported during 5 years after 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 Techwin will provide firmware updates up to 5 years after product discontinuation for cyber security of Wisenet X series network cameras.

The X series network cameras will be more secure, 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