WISENET

Hanwha Techwin

Cyber Security Enhancement Activities

August 8, 2018

Hanwha Techwin

Contents

1. Introduction

Hanwha Techwin operates a security vulnerability response team (S-CERT) to prevent illegal and unauthorized security breaches from external sources, and to prevent internal security flaws.

In order to improve the quality of product security, S-CERT pre-checks product security at product the development stage and conducts penetration testing periodically by specialized agencies. If a security issue arises, a countermeasure council is organized around S-CERT to respond promptly.

Furthermore, S-CERT is committed to developing a differentiated security solution to lead the field of video surveillance, and is also endeavoring to acquire various security certifications to be recognized externally for the quality of the improved product.

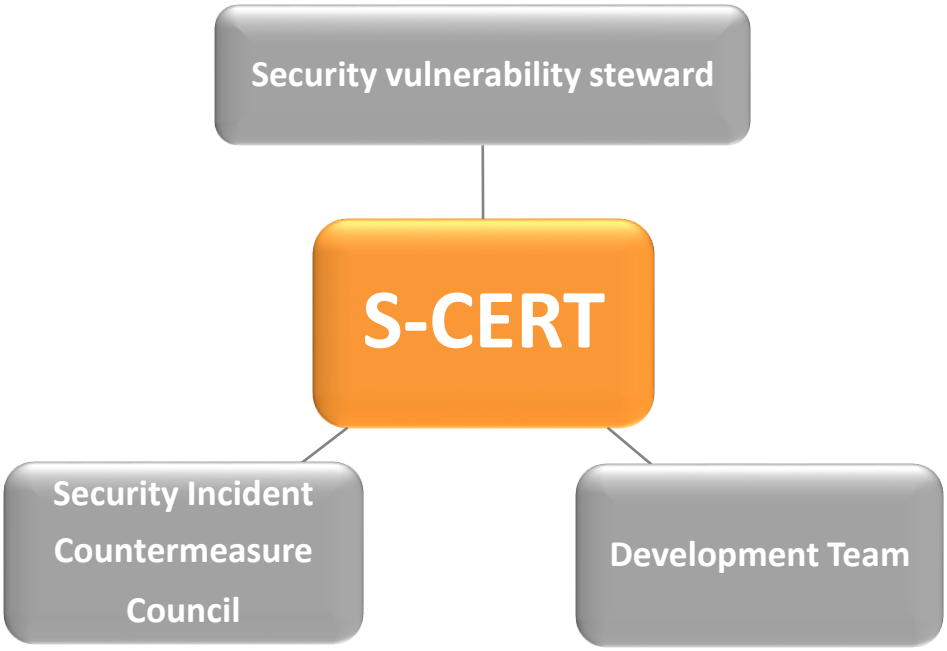
In the next section, we will look at four major activities: security vulnerability response, product security quality improvement, security solution development, and security certification acquisition.

2. Cyber Security Enhancement Activities

2.1 Security vulnerability response activity

<table>
<tr><th>Item</th><th>Contents</th></tr>
<tr><td>Overview</td><td>
■ <u>External security vulnerability monitoring</u>
- Monitoring through CVE*, ICS-CERT, KISA* and cyber security news

■ <u>Response and management according to security response rule</u>
- Convene countermeasures council immediately in case of security issue
- Firmware issuance within five(5) working days
- Announcement on website of security vulnerability report

*CVE: Common Vulnerabilities and Exposures, https://cve.mitre.org/about/
*KISA: Korea Internet Security Agency
</td></tr>
<tr><td>Detail</td><td>
■ Security vulnerability countermeasure council


</td></tr>
<tr><td>Output</td><td>
■ Security vulnerability report
■ Security response rule
</td></tr>
</table>

2. Cyber Security Enhancement Activities

2.2 Product security quality improvement activity

2.2.1 Internal security check and test

Item	Contents
Overview	■ **Security check(Development Team)** - Check by using product security checklist - Security checklists revised periodically throughout the year ■ **Security test(Test Team/S-CERT)** - Test by using product-specific security test cases - Security test cases revised periodically throughout the year - Perform dynamic and static analysis using specialized reverse engineering tools
Detail	■ **Product security check (required at least once)** - User authentication, communication encryption, storage encryption, backdoor, etc. - Self-check by the development team on whether the security technologies meet security policies ■ **Product security test (at least twice required)** - Test by Test team/S-CERT on whether product security functions meet security policies ■ **Dynamic and static analysis** - Verification of use of important information in process / memory / file - Taint and major binary logic analysis - Verification of vulnerabilities including BOF*, FSB* *BOF: Buffer Over Flow *FSB: Format String Bug
Output	■ Security checklist and security test report ■ Dynamic and static analysis report

2. Cyber Security Enhancement Activities

2.2.2 Penetration testing through an external professional agency

Item	Contents
Overview	■ **Periodic penetration testing** - Diagnose penetration by white hacker hacking tools and techniques - Prepare countermeasures and improvements for vulnerabilities found
Detail	■ Firmware / binary test: Memory corruption, Memory leak, Denial of Service, Reverse engineering of firmware, etc. ■ Network test: Replay attack, Spoofing attack, Sniffing attack, etc. ■ Web application test: File download/upload, XSS/CSRF attack, Directory listing/traversal attack, HTTP header modification, etc. ■ Encryption test: Cryptographic key cracking, Decrypting cipher text, Inference of hashed plain text, etc. ■ Other test: Backdoor analysis, Hardware debug port access, Known open-source vulnerability attack, etc.
Output	■ Product penetration test report and response plan

2.2.3 Cyber security technical guide

Item	Contents
Overview	■ **Distribute cyber security white paper and network hardening guide** - Cyber security white paper for security of video surveillance equipment - Network hardening guide for safe product use
Detail	■ Cyber security white paper - Includes password setting, account privilege separation, authentication and encryption, network set-up and configuration, attack identification and blocking, etc. ■ Network hardening guide - Define cyber security level in 4 steps: Basic / Protection / Safety / Top security - Initial and recommended setting guide for each cyber security level
Output	■ Cyber security white paper, Network hardening guide

2. Cyber Security Enhancement Activities

2.3 Security solution development activity

Item	Contents
Overview	■ **Development of device certification issuance management system** - Applies unique device certificate and unique private key to each device - Adapts FIPS 140-2 Level 3 equipment for certificate generation - Secure security algorithms such as RSA2048 and SHA256 ■ **Development of user authentication, video authentication and firmware electronic signature** - To be developed
Detail	■ Device certificate issuance for replacement boards and certificate injection(CS / Repair manager) ■ Issuance and delivery of device certificate (Production line) ■ Large-scale issuance and backup
Output	■ Hanwha Techwin device certificate issuance management system ■ Hanwha Techwin manufacturer root CA certificate and installation guide

2.4 Security certification acquisition activity

Item	Contents
Overview	■ **Major security certifications acquisition** - Acquire major security certifications to provide products that are formally certified for confidentiality, integrity and availability of cyber security
Detail	■ Domestic security certification contents - Test by national agency in accordance with the certification standards for the video surveillance system - Applies Secured by Default concept such as prohibition of initial connection without authentication, application of SHA2 algorithm for user authentication, session termination at unused time ■ International authorized certification acquisition (planned)

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