Wisenet Network Video Recorders
CYBER SECURITY PEN TEST REPORT

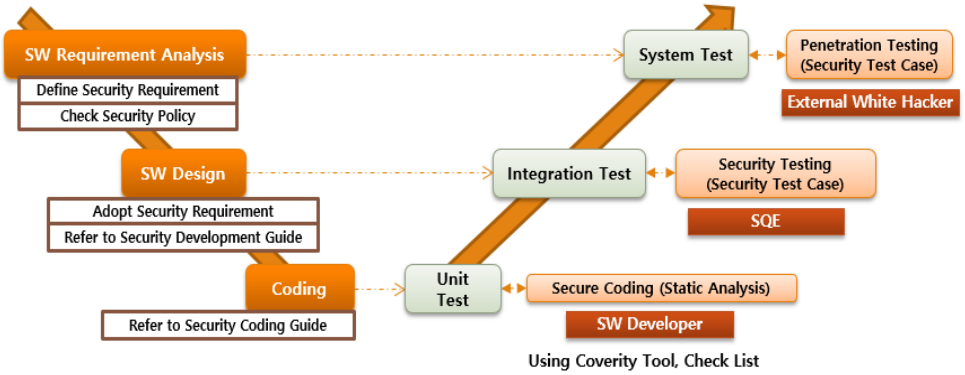
Contents:

November 22th, 2021

INTRODUCTION

Hanwha Techwin have performed penetration test for our products through trusted third party white hacker who can make a professional diagnosis using hacking tools and hacking techniques since long time ago.

We believe this activity will make our product more secure. We expect that disclosure of the processes and results of these activities to our customers will lead to their trust.



TEST PURPOSE

Penetration testing should be performed for a variety of reasons.

Some of the common reasons why Hanwha Techwin as manufacturer perform penetration tests include:

Penetration testing can prevent vulnerabilities which can lead to serious personal information leakage due to the nature of surveillance equipment.

Penetration testing can identify vulnerabilities inadvertently introduced during development process, such as source code changes or platform upgrade.

Some relevant regulatory standards require penetration tests are performed.

Penetration testing can demonstrate a commitment to product security from a customer perspective and provide trust that their private information and control system will be protected securely on operation.

Penetration testing allows manufacturers to proactively assess for emerging or newly discovered vulnerabilities that were not known or have not yet been widely published.

Simple penetration testing can be integrated into the internal QA process of the Software Development Life Cycle to prevent security bugs from entering into production systems.

But, for more robust testing, it is good to be done with the help of a trusted third party security organization.

TEST MODEL

Wisenet AI NVR

TEST MODEL / VERSION

- Wisenet AI Network Video Recorders
  (Total 25 models)
  / Firmware version before fixing

TEST SCOPE

- **Device System**: OS, Firmware, Binary, etc.
- **Device Built-In Service**: Webviewer, RTSP, UPNP, NTP, etc.
- **Other Scope**: Hardware-based access channel (UART), etc.

TEST METHOD

Methodologies for Security Testing

- **Grey Box**: Partial information is given to the tester about the system, and it is a hybrid of white and black box models.
- **OWASP IOT TOP10**: Founded vulnerabilities has classified according to the OWASP Internet Of Things TOP10 2018.

OWASP
Internet of Things Top 10

Test Tool for Security Testing

- Vulnerability scan: Metasploit
- Network scan : Nmap
- Web App Testing : Burp Suite
- Reverse engineering: IDA Pro

Testing Techniques

- 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.

SUMMARY OF FINDINGS

Summary of Identified Vulnerabilities.

Total 12 unknown vulnerabilities have been found in Wisenet Network Video Recorders. Those vulnerabilities are same regarding each listed up recorder model.

The critical impact is one.

The high impact is four.

The middle impact is five.

The low impact is two.

IMPACT ASSESSMENT CRITERIA

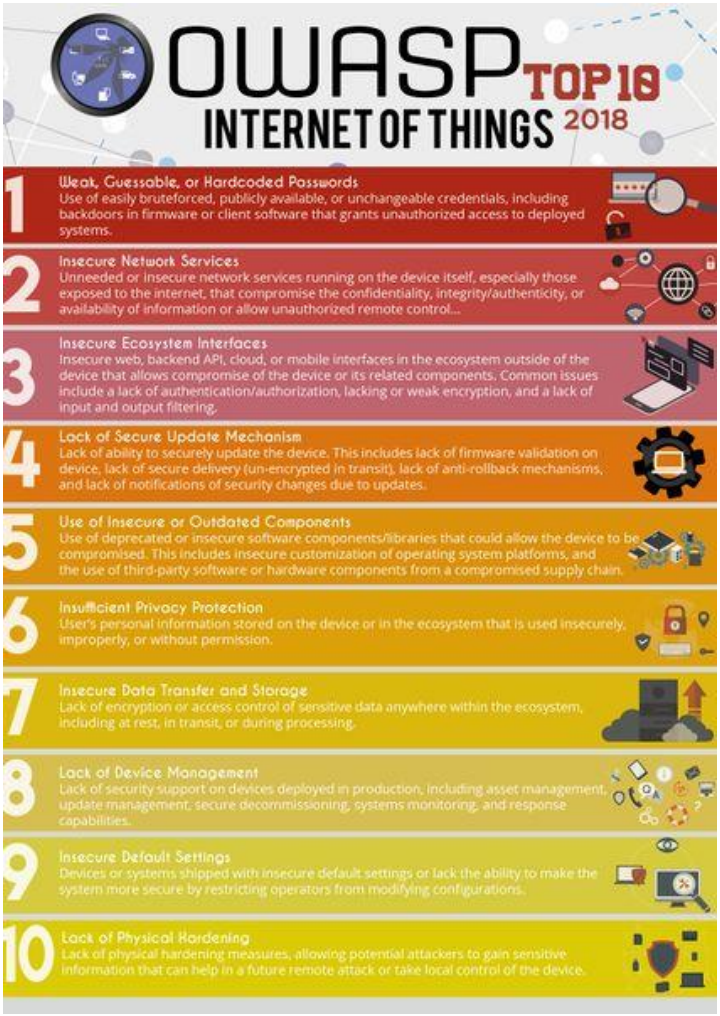
IMPACT	ASSESSMENT CRITERIA
Critical	• If backdoor exists • If unauthorized user - can access the system (OS, service, etc.) - can obtain the administrator authority - can obtain the full video information - can obtain all resources (development code, setting information, etc.) • Due to design errors or improper use(abuse) of the service - If full video information can be obtained - If valid authentication information can be obtained - If the system/service can be shut down or prevented from being restored permanently • If you can get permission or distribute malware on a targeted device
High	• If unauthorized user - can obtain the user authority - can obtain the some video information - can obtain some resources containing crucial information • Due to design errors or improper use(abuse) of the service - If some video information can be obtained - If the system/service can be stopped or interrupted as desired • If you can get permission or distribute malware on a arbitrary device
Middle	• If authorized normal user - can access the unauthorized system (OS, service, etc.) - can obtain the unauthorized video information - can elevate the privilege with administrator maliciously - can obtain resources (development code, setting information, etc.) • Due to design errors or improper use(abuse) of the service - If the system/service can be interrupted limitedly - If resources can be obtained - If there is a possibility of additional vulnerability because the security setting / policy of system or service is not applied
Low	• If authorized normal user - can obtain some resources (development code, setting information, etc.) • Due to design errors or improper use(abuse) of the service - If general information can be obtained - If some resources can be obtained - If the security setting / policy of system or service is not applied

VULNERABILITY SUMMARY

During the first assessment, RaonSecurity has classified identified 12 unknown vulnerabilities according to the OWASP Internet Of Things TOP10 2018*1. After complementary work, RaonSecurity has performed assessment one more time to confirm the original findings be cleared up.

Founded vulnerabilities have could cause authentication bypass, deny of service, use of weak cryptographic algorithms, crucial data expose etc. Fortunately, these vulnerabilities have been unknown to the public due to our proactively penetration test. Hanwha Techwin has resolved all issues as releasing latest Firmware. We recommend customers always to use with Recorder's latest version for the security safe

* 1) Reference sites:
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project



OWASP IOT TOP10 2018

NO	Vulnerability Diagnostics Item	Critical	High	Middle	Low
1	Weak, guessable, or hardcoded passwords			2	
2	Insecure network services		3	2	
3	Insecure ecosystem interfaces				
4	Lack of secure update mechanism				
5	Use of insecure or outdated components				1
6	Insufficient privacy protection				
7	Insecure data transfer and storage				1
8	Lack of device management				
9	Insecure default settings	1			
10	Lack of physical hardening		1	1	
Total		1	4	5	2

NO	Vulnerability Diagnostics Item	Critical	High	Middle	Low
1	Weak, guessable, or hardcoded passwords			0	
2	Insecure network services		0	0	
3	Insecure ecosystem interfaces				
4	Lack of secure update mechanism				
5	Use of insecure or outdated components				0
6	Insufficient privacy protection				
7	Insecure data transfer and storage				0
8	Lack of device management				
9	Insecure default settings	0			
10	Lack of physical hardening		0	0	
Total		0	0	0	0

TEST MODEL / FIXED VERSION

TEST MODEL		MODEL #	FIXED FIRMWARE VERSION
AI NVR	XRN-1620SB1, XRN-1620B2, XRN-820S, XRN-6410DB4, XRN-6410B4, XRN-3210B4, XRN-6410RB2, XRN-3210RB2, XRN-6410B2, XRN-3210B2, PRN-6410DB4, PRN-6410B4, PRN-3210B4, PRN-3210B2, PRN-1610B2, PRN-6400DB4, PRN-6400B4, PRN-3200B4, PRN-3200B2, PRN-1600B2, PRN-6405DB4, PRN-6405B4, PRN-3205B4, PRN-3205B2, PRN-1605B2	25	4.10.10

RAON SECURITY

ABOUT RAONSECURITY

DEFCON (also written as DEFCON, Defcon or DC) is one of the world's largest and most notable hacker conventions, held annually in Las Vegas, Nevada.

(https://en.wikipedia.org/wiki/DEF_CON, https://www.defcon.org)

RaonSecurity attended at CTF of DEF CON 16 in 2008 with the name of Taekwon-V and was ranked 4th.

(https://www.defcon.org/html/defcon-16/dc-16-contest-results.html)

RaonSecurity provides security solution development and penetration test consulting services and is an IT information security company that conducts various latest hacking techniques research and hacking competitions.

RaonSecurity was ranked 1st at Wechall in 2018 and 1st at Noe.systems in 2019.

Wechall and Noe.systems are the famous hacking challenge and problem solving sites in globally.

(http://www.wechall.net/site/ranking/for/1/ WeChall, https://noe.systems/Rank)

RaonSecurity has been providing consulting services to global companies such as Samsung Electronics, Hyundai motors, KIA motors, SK Telecom etc.

GRADING REPORT

The grade below is a representation of the Hanwha Techwin Network Video Recorders (latest, post-remediation) security posture.

RaonSecurity calculates grades with **Level A** based on each detailed assessment items.

Level A means that the proper protection against anticipated protection threats has been implemented in surveillance equipment, ensuring that the customer's sensitive information is kept safe for operation.

Lucas . Yang

CEO & Founder, RaonSecurity

Lucas @ Raonsecurity.com

131, GASAN DIGITAL 1-RO,
GEUMCHEON-GU, SEOUL,
REPUBLIC OF KOREA

GRADING REPORT

Classification	Opinion	Details	Result
Authentication process	Digest authentication are applied between Device and Client (webviewer, VMS, etc..)	Unfair use of crudentials	Pass
		Arbitary use of crudentials	Pass
		Weak authentication logic	Pass
		Expose crudentials	Pass
Authorization management	Secure authority management for users (administrators and users) is possible	Improper elevation of privilege	Pass
		Abuse of administrator privilege	Pass
		Improper permission handling	Pass
Cryptography applying	Secure encryption algorithm is used for authentication, access control, and when communication.	Use weak cryptographic algorithm	Pass
		Improper encryption key management	Pass
		Ciphertext Exposure	Pass
Communication protection	Secure encryption communication is applied for the authentication and important information	Missing encryption of crucial data	Pass
		Unnecessary network resource usage	Pass
Data protection	The encryption on credentials is applied and managed securely. Access control is securely applied to important information. In addition, valid check for external input values has been applied.	Missing crudentials encryption	Pass
		Credentials and sensitive data exposure	Pass
		Insufficient input verification	Pass
Platform protection	Firmware is distributed only through designated servers. And SourceCode cannot be leaked because firmware encryption is applied.	Unfair license use	Pass
		Development code exposure	Pass
		Insecure update Scheme	Pass
		Missing / Incomplete Security Settings	Pass
Firmware protection	Firmware was encrypted AES based algorithm. and CRC-based forgery prevention technology is applied.	Insufficient protect on firmware forgery	Pass
		Insufficient firmware encryption	Pass
		Firmware exposure	Pass
Physical protection	Unnecessary H / W PORT has been removed, and authentication is performed when UART is connected.	Unnecessary H/W communication port	Pass
		Unauthenticated use of internal port	Pass

LEVEL	Criteria
LEVEL S: Excellent	Defense against the security weaknesses of the device, and having an excellent security design
LEVEL A: Very Good	Proper defense against security vulnerabilities in devices
LEVEL B: Good	Selective defense against the vulnerability of the device
Level C: Poor	Being aware of a security vulnerability in your device

Hanwha Techwin

13488 Hanwha Techwin R&D Center,6 Pangyoro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do

TEL 070.7147.8771-8
FAX 031.8018.3715
https://hanwha-security.com

Notice

Please refrain from asking the manufacturer for more information as it could be exploited like a known vulnerability.

The results of this penetration test do not prove to be a flawless product without vulnerabilities, and are intended to create products with better security through trusted third parties.

Please note that exploiting the vulnerability information mentioned in this report or illegally accessing the operating system can cause legal problems.

Our Business

Hanwha Techwin's world class imaging technology is now applied to more diverse business areas including Access Control and Intruder Detection.

Our products play an important role for the safety and happiness of people by protecting cities, airports, seaports, industrial areas and military installations.

We will continuously provide high resolution, high performance and highly reliable premium security products and achieve the social value of "safety and the comfort".

Hanwha Techwin will advance towards becoming the world's best total security solutions provider by offering a one-stop security solution, facilitating the global network, and continuously conducting research and development.

About S-CERT…

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.

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.