CYBER SECURITY PENETRATION TEST REPORT

Hanwha Vision Network Camera

September 2, 2024

Background

Hanwha Vision has 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.

Testing purpose

Penetration testing should be performed for a variety of reasons. Some of the common reasons why Hanwha Vision 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.
- 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.

For more robust testing, we conduct testing with the help of trusted third-party security agencies.

About STEALIEN

STEALIEN has specialized technology to analyze vulnerabilities in various service environments such as web, mobile, IoT, and cloud services. STEALIEN also creates realistic threat scenarios based on these technologies and suggests appropriate countermeasures and improvement measures.

STEALIEN has won awards in international hacking CTFs such as CodeGate and DefCon, and has experience in discovering vulnerabilities in products from global vendors such as Windows Kernel, Google Chrome, Adobe, and VMware.

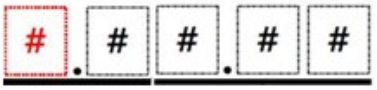
STEALIEN has a good relationship with Hanwha Vision and have conducted this penetration testing with them.

Testing target and scope

From June 12, 2023 to August 4, 2023, six vulnerability researchers conducted penetration tests on network cameras in the X.XY.YY format, and from September 18, 2023 to October 27, 2023, five vulnerability researchers conducted penetration tests on network cameras in the XX.XY.YY format.

Hanwha Vision network cameras have different camera SW Platform depending on the version type. The important thing is, Cameras developed with version of same type guaranteed to operate in the same manner.

- **Target network camera #1**
  - version types in the X.XY.YY format
  - targeting firmware is 2.XY.YY



- **Target network camera #2**
  - version types in the XX.XY.YY format
  - targeting firmware is 23.XY.YY

The camera's system and services, network, security functions, etc., have been tested.

- Device System: OS, firmware, and root file system, etc.
- Device Built-In Service: http/s, rtp/rtsp, onvif, ntp, upnp, onvif, running environment, etc.
- Security features: secure boot, secure update, digital signature, authentication, secure communication, secure store by sensitive information, etc.

Testing methods

Testing was performed using STEALIEN's standard methodology for a black box security assessment and STEALIEN's security techniques.

- System and Firmware test: firmware forgery, memory corruption, memory leak, denial of service, reverse engineering of firmware, etc.
- Network test: packet replay, sniffing and spoofing, forgery, etc.
- Web application test: File download/upload, XSS/CSRF, Directory listing/traversal, SQL Injection, parameter Injection, etc.
- Security features test: authentication bypass/forgery, privilege escalation, secure boot/update, cipher key cracking, decrypt cipher text, Inference of hashed plain text, etc.
- Others: Hardware debug port access, Known open-source vulnerability attack, etc.

Summary of findings

Target network camera #1

- version types in the X.XY.YY format
- targeting firmware is 2.XY.YY

User input value validation is properly applied, and memory protection techniques are applied to respond well to memory-based attacks. In particular, attack codes are filtered in advance by data validation logic, and many attack techniques are neutralized. Security functions such as encryption are appropriately reflected in firmware / communication / authentication processing / video transmission/reception logic. However, a problem was discovered where uart shell could be acquired due to misconfiguration in the boot stage.

During the penetration testing, Findings:

Vulnerability Category	CRITICAL	HIGH	MEDIUM	LOW
Insecure Authentication and Access Control				
Insecure Network Interface			1	
Insecure Privilege Management				
Insufficient Privacy Protection				
Insecure Data Transfer and Storage				
Insecure Default Settings				
Lack of Physical Hardening			1	
Weak Guessable, or Hardcoded Passwords				
Use of a Broken or Risky Cryptographic Algorithm				
Exposure of sensitive information				

Target network camera #2

- version types in the XX.XY.YY format
- targeting firmware is 23.XY.YY

Firmware file protection is excellent. Digital signature, secure boot and firmware encryption have been securely implemented. Hardware debug physical ports are also access controlled. Most input value validations are well implemented, protecting against many memory-based attacks such as Buffer Overflow, but some WEB UI input sections have incorrect validation logic and access to the hardware debug physical port was not well controlled at the time of the firmware update.

During the penetration testing, Findings:

Vulnerability Category	CRITICAL	HIGH	MEDIUM	LOW
Insecure Authentication and Access Control	1			
Insecure Network Interface		2		
Insecure Privilege Management				

Insufficient Privacy Protection				
Insecure Data Transfer and Storage				
Insecure Default Settings				
Lack of Physical Hardening			1	
Weak Guessable, or Hardcoded Passwords				
Use of a Broken or Risky Cryptographic Algorithm				
Exposure of sensitive information				1

Mitigation

Hanwha Vision has enhanced the network camera by addressing all identified vulnerabilities. Network cameras in the X.XY.YY format have been updated firmware from October 2023, and network cameras in the XX.XY.YY format have been updated firmware from November 2023. These firmware can be downloaded from the homepage. It is always recommended to use the latest version firmware for your camera.

The model names of the enhanced cameras can be found in the update list.

Update model list

PNO-A9311R	TNO-L4040T	XNV-8030R	XNP-6400R
PNM-C7083RVD	TNO-L4050T	XNV-8040R	XNP-6400
PNM-C12083RVD	TNS-9050IBC	KND-5080RN	XNP-9300RW
PNM-C9022RV	TNV-C8011RW	XND-8080R	XNP-8300RW
PNM-7002VD	XNV-9083RZ	XND-8080RV	XNP-6400RW
PNM-8082VT	XNV-8083RZ	XND-8080RW	TNV-C7013RC
PNM-9000QB	XNV-8083Z	XNV-8080R	XNP-C6403
PNM-9002VQ	XNV-6083RZ	XNV-8080RS	XNP-C6403R
PNM-9022V	XNV-6083Z	XNV-8080RSA	XNP-C6403RW
PNM-9031RV	XNB-6002	XNV-8080RW	XNP-C8253
PNM-9084QZ	KNB-2000	XNV-9083R	XNP-C8253R
PNM-9084RQZ	XNB-6000	XNV-8093R	XNP-C8303RW
PNM-9085RQZ	KNO-2080RN	XNV-8083R	XNP-C9253
PNM-9084QZ1	XNO-6080R	XND-9083RV	XNP-C9253R
PNM-9084RQZ1	XNO-6080RA	XND-8093RV	XNP-C9303RW
PNM-9085RQZ1	XNO-6080RS	XND-8083RV	XNO-6123R

PNM-9322VQP	KNB-5000N	XNO-9083R	XNV-6123R
PND-A9081RV	KNO-5080RN	XNO-8083R	XNB-8002
PND-A9081RF	XNB-8000	XNB-9003	XNB-9002
PNO-A9081R	XNO-8080R	XNB-8003	XND-8082RF
PNV-A9081R	XNO-8080RW	XND-C6083RV	XND-8082RV
QNV-6012RG	XND-6080	XND-C7083RV	XND-9082RF
TNO-7180RLP	XND-K6080N	XNV-C6083R	XND-9082RV
XNB-6001	KND-2080RN	XNV-C7083R	XNO-8082R
XNP-9300RWG	XND-6080R	XNO-C6083R	XNO-9082R
XNP-8300RWG	XND-6080RW	XNO-C7083R	XNV-8082R
XNP-6400RWG	XND-6080RV	XNV-C6083	XNV-9082R
QNV-C9083R	XND-6080V	XND-C8083RV	PNO-A9311RLP
QNO-C9083R	XNV-6080	XND-C9083RV	QNE-C8013RL
QNV-C8083R	XNV-6080R	XNV-C8083R	QNE-C9013RL
QNO-C8083R	XNV-6080RW	XNV-C9083R	QNV-C8011RMG
QNV-C9011R	XNV-6080RS	XNO-C8083R	TNM-C3620TDR
QNV-C8011R	XNV-6080RSA	XNO-C9083R	TNM-C3622TDR
QNV-C8012	XND-6083RV	XNF-9010RV	TNM-C4940TDR
KNO-5020RG	XNV-6083R	XNF-9010RVM	TNM-C4942TDR
XNV-8020RG	XNO-6083R	XNF-9010RS	TNO-C3010TRA
PNM-C16013RVQ	XNB-6003	XNF-9013RV	TNO-C3012TRA
PNV-A6081RE	KND-5020RN	KNO-5020RN	TNV-C7013RCG
XNO-8080RG	XND-8020R	XNO-8020R	XNP-C9303RWG
PNM-7082RVD	XND-8020RW	XNO-8030R	XNP-C9310R
PNM-12082RVD	XND-8030R	XNO-8040R	XNP-L6322RG
TNF-9010	XND-8040R	XNP-9250R	PNM-C16083RVQ
TNO-L4030TR	XNV-8020R	XNP-8250R	PNM-C32083RVQ
TNO-L4040TR	XNV-8020RMN	XNP-9250	PNM-C34404RQPZ
TNO-L4030T	XNV-8020RMP	XNP-8250	PNM-C32084RQZ
QNO-C6083R	QNV-C6083R		