CYBER SECURITY PENETRATION TEST REPORT

Hanwha Vision Network Video Recorder

December, 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

STEALIEN performed a penetration test on Hanwha Vision's NVR and achieved meaningful results. During this penetration test, vulnerability assessments were performed for all possible scenarios, so many security issues were identified.

The NVR'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, 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

There was an issue with the firmware encryption logic. using this, firmware analysis was possible. And input value validation for web UI and user-input parameters was somewhat inadequate, allowing for remote code execution and DoS attacks. In addition, some script files within the file system contain sensitive information in plaintext.

During the penetration testing, Findings:

Vulnerability Category	CRITICAL	HIGH	MEDIUM	LOW
Insecure Authentication and Access Control				
Insecure Network Interface	1		4	
Insecure Privilege Management				
Insufficient Privacy Protection				
Insecure Data Transfer and Storage				
Insecure Default Settings				

Lack of Physical Hardening				
Weak Guessable, or Hardcoded Passwords				
Use of a Broken or Risky Cryptographic Algorithm		2		
Exposure of sensitive information			1	

Mitigation

Hanwha Vision has enhanced the NVR by addressing all identified vulnerabilities. This enhanced firmware can be downloaded from the homepage. It is always recommended to use the latest firmware for NVR.

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

Updated model list

Model	Vulnerable firmware version	Enhanced firmware version
XRN-420S	5.01.62 and prior versions	5.01.72 and later versions
QRN-430S	5.01.62 and prior versions	5.01.72 and later versions
HRX-1632	4.52.62 and prior versions	4.52.72 and later versions
HRX-835	4.52.62 and prior versions	4.52.72 and later versions
HRX-435	5.31.72 and prior versions	5.31.82 and later versions
HRX-434	5.31.72 and prior versions	5.31.82 and later versions
HRX-1635	5.31.72 and prior versions	5.31.82 and later versions
HRX-1634	5.31.72 and prior versions	5.31.82 and later versions
HRX-835A	5.31.72 and prior versions	5.31.82 and later versions
HRX-435L	5.31.72 and prior versions	5.31.82 and later versions
XRN-426S	5.33.12 and prior versions	5.33.22 and later versions
PRN-6410B4	5.34.12 and prior versions	5.34.22 and later versions
PRN-3210B4	5.34.12 and prior versions	5.34.22 and later versions
PRN-3210B2	5.34.12 and prior versions	5.34.22 and later versions
PRN-1610B2	5.34.12 and prior versions	5.34.22 and later versions
PRN-6405DB4	5.34.12 and prior versions	5.34.22 and later versions
PRN-6405B4	5.34.12 and prior versions	5.34.22 and later versions
PRN-3205B4	5.34.12 and prior versions	5.34.22 and later versions

PRN-3205B2	5.34.12 and prior versions	5.34.22 and later versions
PRN-1605B2	5.34.12 and prior versions	5.34.22 and later versions
PRN-6400DB4	5.34.12 and prior versions	5.34.22 and later versions
PRN-6400B4	5.34.12 and prior versions	5.34.22 and later versions
PRN-3200B4	5.34.12 and prior versions	5.34.22 and later versions
PRN-3200B2	5.34.12 and prior versions	5.34.22 and later versions
PRN-1600B2	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410DB4	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410B4	5.34.12 and prior versions	5.34.22 and later versions
XRN-3210B4	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410RB2	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410B2	5.34.12 and prior versions	5.34.22 and later versions
XRN-3210RB2	5.34.12 and prior versions	5.34.22 and later versions
XRN-3210B2	5.34.12 and prior versions	5.34.22 and later versions
XRN-1620B2	5.34.12 and prior versions	5.34.22 and later versions
XRN-1620SB1	5.34.12 and prior versions	5.34.22 and later versions
XRN-820S	5.34.12 and prior versions	5.34.22 and later versions
ARN-1610S	5.31.42 and prior versions	5.31.52 and later versions
ARN-810S	5.31.42 and prior versions	5.31.52 and later versions
ARN-410S	5.31.42 and prior versions	5.31.52 and later versions
XRN-815S	5.06.52 and prior versions	5.06.62 and later versions
QRN-1630S	5.06.52 and prior versions	5.06.62 and later versions
QRN-830S	5.06.52 and prior versions	5.06.62 and later versions
XRN-425S	5.31.32 and prior versions	5.31.42 and later versions
SPD-152	5.10.32 and prior versions	5.10.42 and later versions
ARD-1610	5.31.32 and prior versions	5.31.42 and later versions
ARD-810	5.31.32 and prior versions	5.31.42 and later versions
ARD-410	5.31.32 and prior versions	5.31.42 and later versions
HRX-1635/TE	5.31.72 and prior versions	5.31.82 and later versions

HRX-835/TE	5.31.72 and prior versions	5.31.82 and later versions
HRX-435FN/TE	5.31.72 and prior versions	5.31.82 and later versions
XRN-6410DR/TE	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410R/TE	5.34.12 and prior versions	5.34.22 and later versions
XRN-3210R/TE	5.34.12 and prior versions	5.34.22 and later versions
XRN-1620S/TE	5.34.12 and prior versions	5.34.22 and later versions
XRN-820S/TE	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410B4/TU	5.34.12 and prior versions	5.34.22 and later versions
HRX-1635/TU	5.12.22 and prior versions	5.12.32 and later versions
XRN-425SFN/TE	5.31.32 and prior versions	5.31.42 and later versions