CYBER SECURITY PENETRATION TEST REPORT

Hanwha Vision Wisenet Access Control System

February, 2025

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 WACS(Wisenet Access Control System) and achieved meaningful results. During this penetration test, vulnerability assessments were performed for all possible scenarios, so many security issues were identified.

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

- Target
  - Wisenet Access Control System 2.2.2
- Target's system architecture
  - Service
    - ✓ WACS Server & Client, Gateway Server, Web server, Transaction Server
    - ✓ Configuration Manager SW, Visitor Manager SW, Monitoring SW
  - Database: MSSQL, Mongo DB
  - Interface Communication Protocol: RabbitMQ, HTTPS API
- Target's security features
  - Authentication, Encrypt/Decrypt, 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 Server test: input data forgery, memory corruption, memory leak, denial of service, reverse engineering of Software, etc.
- Network test: packet replay, sniffing and spoofing, forgery, etc.
- API 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: Known open-source vulnerability attack, etc.

Summary of findings

There was a problem with insufficient access control. In addition, there was a problem with hardcoding and reusing stored authentication information due to the nature of the installed software. The problem of arbitrary logins possible by reusing authentication information could be linked to malware installation. To supplement this, we believe that it is necessary to improve the encryption logic and module.

During the penetration testing, Findings:

Vulnerability Category	CRITICAL	HIGH	MEDIUM	LOW
Insecure Authentication and Access Control			1	
Insecure Network Interface			1	
Insecure Privilege Management				
Insufficient Privacy Protection				
Insecure Data Transfer and Storage			1	1
Insecure Default Settings				
Lack of Physical Hardening				
Weak Guessable, or Hardcoded Passwords		2		
Use of a Broken or Risky Cryptographic Algorithm				
Exposure of sensitive information				

Mitigation

Hanwha Vision has enhanced the WACS(Wisenet Access Control System) by addressing all identified vulnerabilities. We always recommended to use the latest version of software. The patched WACS software version is 2.3.0.

Version information

Software	Vulnerable software version	Enhanced software version
Wisenet Access Control System	2.2.2 and prior version	2.3.0 and later versions