CYBER SECURITY PENETRATION TEST REPORT

Hanwha Vision Cloud Service

May, 2026

Background

Hanwha Vision has performed penetration test for our products and cloud services 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 products and cloud services 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 and service provider perform penetration tests include:

- Penetration testing can prevent vulnerabilities which can lead to serious personal information leakage due to the nature of surveillance equipment and service.
- 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/service security from a customer perspective and provide trust that their private information and control system will be protected securely on operation.
- Penetration testing allows manufacturer and service provider 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 RaonSecurity

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

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

Testing target and scope

From December 02, 2024 to January 24, 2025, five vulnerability researchers conducted penetration tests on Cloud Services.

Hanwha Vision Cloud Services have a central hub called the Cloud Portal. Sub-services operate under the Cloud Portal, and each service utilizes data from devices connected to the Cloud Portal.

The cloud service's authentication and authorization mechanisms, API security, business logic, and access control have been tested.

- Cloud Service: Registration logic, activation code verification logic, authentication logic, license logic, and security weaknesses in service business logic, etc
- Cloud Connectivity Service : Device registration, API security, and related cloud-to-device communication security, etc

Testing methods

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

- API Security Test: API endpoint authentication and authorization control flaws, API-specific parameter tampering and business logic abuse, excessive data exposure.
- Web Application Test: File upload/download control weaknesses, XSS/CSRF, directory listing/traversal, and web input injection vulnerabilities (e.g., SQL injection, command injection).
- Security Features Test: Cryptographic and account-security weaknesses, including token/signature forgery, privilege escalation via security control bypass, key management flaws
- Others: Known open-source vulnerability attack, etc.

Summary of findings

We discovered vulnerabilities including exposure of sensitive information in the app's local storage and logs, modification of user privileges through parameter tampering, execution of arbitrary commands via command injection, and eavesdropping on other users' video streams through MQTT tampering.

During the penetration testing, Findings:

Vulnerability Category (OWASP Top 10)	CRITICAL	HIGH	MEDIUM	LOW
Broken Access Control	1	3	3	1
Security Misconfiguration			1	
Software Supply Chain Failures				
Cryptographic Failures			1	
Injection	1		3	
Insecure Design	1	3	3	
Authentication Failures			1	
Software or Data Integrity Failures				
Logging & Alerting Failures				
Mishandling of Exceptional Conditions				1
Total	3	6	12	2

Mitigation

Hanwha Vision has enhanced its Cloud Services by addressing all identified vulnerabilities.

The updated versions are listed below.

CloudPortal : v1.10.0

OnCloud : v1.83.3

SightMind : v1.6.0

HealthPro : v1.6.0

OnCAFE : v1.2.14

Updated Service list

CloudPortal, OnCloud, SightMind, HealthPro, OnCAFE