CYBER SECURITY PENETRATION TEST REPORT

Hanwha Vision BLAZE

January, 2026

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 identifies vulnerabilities that may cause serious data breaches, protecting the integrity of our products and solutions.
- 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 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 March 13, 2025 to April 23, 2025, five vulnerability researchers conducted penetration tests on BLAZE.

The BLAZE's Application and services, network, security features, etc., have been tested.

- BLAZE Server
  - API and Protocols
  - Database and "Device / Stream / Event / Gateway / Media / Proxy / Auth" Application
- BLAZE Client
  - Desktop Software
  - Mobile App (Android, iPhone)
- Cloud Integration
  - CloudConnector
  - Cloud Portal + onCloud
  - BLAZE Cloud
- Service: HTTP/HTTPS, RTP/RTSP, ONVIF, NTP, UPNP, running environment, etc.
- Security features: authentication, secure communication, secure store by sensitive information, etc.

Testing methods

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

- 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, cipher key cracking, decrypt cipher text, Inference of hashed plain text, etc.
- Others: Known open-source vulnerability attack, etc.

Summary of findings

Sensitive information within the system was properly encrypted, and RSA key management was excellently maintained. Furthermore, input filtering for string-based attacks, such as Injection, was robustly implemented across the platform. However, access control mechanisms and exception handling were inadequate. Specifically, granular permission settings for individual APIs and overall account privilege management need to be significantly strengthened to ensure a secure and resilient operational environment.

During the penetration testing, Findings:

Vulnerability Category (OWASP Top 10)	CRITICAL	HIGH	MEDIUM	LOW
Broken Access Control		4	4	
Security Misconfiguration				
Software Supply Chain Failures				
Cryptographic Failures			3	
Injection				
Insecure Design			3	
Authentication Failures		1		
Software or Data Integrity Failures				
Logging & Alerting Failures				
Mishandling of Exceptional Conditions		4		

Mitigation

Hanwha Vision has enhanced the security of BLAZE by addressing all identified vulnerabilities. We recommend keeping your BLAZE application updated to the latest version.