Hanwha Vision

White Paper

Wisenet 9 기반 제품의 차세대 사이버보안

2025 년 8 월

1. 서론

한화비전 Wisenet SoC(System on a Chip)는 제품 보안 강화를 위해 꾸준히 신기술을 접목하며 발전해 왔다. 특히 최신 Wisenet 9 SoC 가 탑재된 카메라는 제품, 개발 프로세스, 데이터, 공급망에 대한 보안에 더욱 중점을 두어, 한화비전 영상보안 솔루션에 대한 고객 신뢰를 한층 더 높이고 있다.

제품 보안 강화를 위해서는 강력한 보안 표준 및 프로세스에 대한 선제적인 노력이 필요하다. 한화비전은 업계에서 인정받는 수많은 글로벌 표준 중 IoT(사물 인터넷) 디바이스에 대한 보안 표준인 **ETSI EN 303 645** 를 전략적으로 채택했다. 이는 당사 보안 인증에 대한 독립적인 제 3 자 검증을 가능하게 한다.

한화비전은 오랜 기간 업그레이드해 온 개발 프로세스 보안에 대한 공식적인 검증 또한 확보하고자 했다. 이를 위해 ISO/IEC 27001 정보 보안 인증을 이미 보유하고 있음에도 불구하고, 보안 기능의 설계, 개발, 테스트 및 유지보수 방법에 대한 지침을 제공하는 **ISA/IEC 62443-4-1** 인증을 획득했다.

민감한 데이터 보호는 보호가 필요한 자산과 데이터를 체계적으로 식별하는 것에서 시작되며, 이를 보호하기 위한 기술 솔루션 개발로 이어져야 한다. 한화비전은 핵심 보호 계층을 추가하기 위해 **FIPS 140-3 표준 인증을 획득한 시큐어 엘리먼트(Secure Element)**를 통해 RoT(Root of Trust) 기반의 보안 스토리지를 구현한다.

오늘날의 소프트웨어 개발 및 배포 환경에서 소프트웨어 공급망의 보안과 투명성은 점점 더 중요해지고 있다. 소프트웨어 구성 요소를 명확하게 문서화하고 관리하는 **SBOM(Software Bill of**

Materials)은 보안 취약점 해결, 운영 효율성 유지, 오픈소스 라이선스 준수 보장, 소프트웨어 공급망 공격 방지에 핵심적인 역할을 한다.

본 백서는 한화비전 Wisenet 9 기반 카메라의 보안을 강화하기 위해 적용된 주요 전략과 기술을 상세히 다룬다. 특히, ETSI EN 303 645 및 IEC 62443-4-1 표준 준수 과정, FIPS 140-3 인증 시큐어 엘리먼트를 통한 데이터 보호 전략, 그리고 소프트웨어 공급망 보안 강화를 위한 SBOM 의 효과적인 활용에 대해 집중적으로 설명한다.

2. ETSI EN 303 645 표준 준수

한화비전은 Wisenet 9 기반 제품에 ETSI EN 303 645 표준의 요구사항을 구현했다. 유럽전기통신표준화기구(ETSI)가 개발한 이 국제 보안 표준은 IoT 디바이스의 사이버보안을 강화하도록 설계되었다. Wisenet 9 기반의 카메라가 이 표준을 준수함으로써, 고객은 한화비전 플랫폼의 사이버보안을 신뢰할 수 있다.

2.1. ETSI EN 303 645 개요

ETSI EN 303 645 표준은 유럽 연합(EU)에서 처음 제정되었으며, 독일(BSI/IT 보안 라벨), 영국(PSTI 법), 싱가포르(사이버보안 라벨링 제도 Tier 1 및 2)를 포함한 유럽 및 아시아 국가에서 IoT 디바이스의 보안 요구사항으로 널리 채택되었다. 또한 일본(JC-STAR1), EU(사이버복원력법) 등과 같은 다른 지역에서도 채택을 검토하고 있다.

ETSI EN 303 645 표준은 이해관계자들이 보안 요구사항을 이해하고 구현하는 데 도움을 주기 위해 다음 3 가지 문서를 제공한다.

- Security Baseline Requirements: ETSI EN 303 645 V3.1.3 (2024-09)
- Conformance Assessment Methodology: ETSI TS 103 701 V2.1.1 (2025-05)
- Guidance on Implementation: ETSI TR 103 621 V2.1.1 (2025-07)

한화비전은 Wisenet 7 제품에 미국 기반의 네트워크 연결 제품 소프트웨어 사이버보안 인증인 UL 2900-2-3 표준을 적용한 경험이 있다. 이 표준은 미국 표준협회(American National Standards Institute, ANSI)와 캐나다 국가표준(National Standard of Canada, NSC)이 채택한 것으로, 주로 취약점, 소프트웨어 약점, 악성코드의 존재 여부, 아키텍처 및 설계 내 보안 위험 제어 유무에 대한 테스트에 중점을 두며 제품에 대한 침투 테스트 수행도 요구한다.

반면, ETSI EN 303 645 표준은 고객의 개인 데이터 보호에 더 큰 비중을 둔다. 이 표준은 제조업체가 제품 및 서비스를 사용하는 고객에게 개인 데이터에 대한 선택권을 제공하도록 요구한다. 여기에는 데이터 수집에 대한 동의 옵션 제공, 항시적인 동의 철회 허용, 데이터 수집 목적 설명 등이 포함된다. (레퍼런스 참조)

이러한 차이에도 불구하고, 두 표준 모두 공통적으로 취약점 공개 정책, 지속적인 취약점 모니터링, 식별 및 해결 활동, 보안 인증 및 권한 부여, 보안 통신, 보안 부팅, 보안 업데이트, 외부 인터페이스 및 서비스에 대한 보호 메커니즘 등 다양한 요구사항을 포함하고 있다.

2.2. ETSI EN 303 645 주요 요구사항

- **기본 패스워드 제거**: 보안 카메라에는 해킹을 쉽게 만드는 사전 설정된 공통 패스워드가 없어야 한다.

- **보안 통신**: 카메라가 영상 및 데이터 전송에 보안 통신 프로토콜을 사용함으로써, 무단 가로채기 및 데이터 조작을 방지해야 한다.
- **취약점 관리**: 제조업체는 카메라에서 발견된 취약점을 해결하고 보고하는 프로세스를 갖춰야 한다.
- **데이터 프라이버시**: 카메라는 무단 접근, 오용, 유출로부터 개인 및 민감한 데이터를 안전하게 보호하는 기능을 갖춰야 한다. 더불어, 데이터가 명확하게 삭제되었음을 사용자에게 알리고 이를 확인할 수 있는 절차를 제공해야 한다.
- **정기적인 소프트웨어 업데이트**: 제조업체는 디바이스의 수명 주기 동안 새로운 취약점으로부터 보호되도록 정기적인 소프트웨어 업데이트를 제공해야 한다.
- **보안 스토리지**: 제조업체는 암호화 키, 사용자 패스워드, 고유 디바이스 ID 와 같은 중요 정보를 안전하게 저장할 수 있는 수단을 제공해야 한다.

2.3. 표준 준수를 통한 제품 신뢰 확보

Wisenet 9 기반 제품은 다양한 보안 요구사항, 고객 요구, 산업 표준을 충족시키며 축적해온 회사의 전문 지식을 기반으로 개발되었다. 한화비전은 시장 동향을 지속 모니터링하고, 고객 요구를 예측하며, 업계 최고 수준의 보안 표준을 유지해 시장에 우수하고 안전한 제품을 제공하기 위해 노력하고 있다.

3. IEC 62443-4-1 표준 준수

한화비전은 Wisenet 9 기반 카메라를 포함해 제품의 보안 개발 프로세스 전반에 걸쳐 IEC 62443-4-1 표준 요구사항을 준수한다. 이 인증 획득을 통해 한화비전은 고객에게 회사의 컴플라이언스 활동을 투명하게 알릴 수 있다.

3.1. IEC 62443-4-1 개요

IEC 62443-4-1 은 산업 자동화 및 제어 시스템(Industrial Automation and Control Systems, IACS)의 보안 개발 수명 주기(Security Development Lifecycle, SDL) 요구사항을 정의한 국제 표준이다. 유럽의 선박, 유통, 철도와 같은 보안 카메라 분야 고객들 사이에서 이 표준 준수 요구가 점차 증가함에 따라, 관련 인증의 필요성 또한 커지고 있다. 이 표준은 하드웨어, 소프트웨어, 펌웨어 등 제품 개발 전 과정에 보안을 체계적으로 반영하도록 하며, 개발 조직은 제품이 설계 단계부터 보안을 내재하도록 프로세스를 구현할 것을 요구한다.

3.2. IEC 62443-4-1 주요 요구사항

IEC 62443-4-1 표준의 요구사항은 총 47 개의 요구사항을 포함하는 8 가지 주요 프로세스 영역으로 구성된다. 각 프로세스 영역 및 주요 요구사항은 다음과 같다.

[표 1] IEC 62443-4-1 요구사항 요약

프로세스 영역	주요 요구사항
보안 관리	보안 정책 및 절차 수립, 보안 역할 및 책임 정의, 보안 교육 및 인식 프로그램 운영, 보안 요구사항 및 위험 관리
보안 요구사항 명시	보안 요구사항 식별, 문서화, 검토, 승인 및 추적
보안 설계	보안 설계 원칙 적용 및 보안 아키텍처 설계, 보안 설계 검토, 검증, 추적 및 위험 분석 수행
보안 구현	보안 코딩 표준 적용 및 코드 검토, 정적 분석 도구 사용
보안 검증 및 유효성 검사 테스트	보안 요구사항, 위협 완화, 취약점, 침투 등에 대한 테스트
보안 이슈 관리	보안 이슈 보고, 검토, 평가, 해결 및 공개, 보안 결함 관리 관행에 대한 주기적 검토
보안 업데이트 관리	보안 업데이트 및 문서 제공
보안 지침	제품 보호 및 보안 강화(폐기/운영) 가이드 제공

3.3. 보안 인증을 통한 제품 개발 신뢰 확보

한화비전은 IEC 62443-4-1 표준 준수를 통해 이 국제 표준을 충족하는 SDL 프로세스를 갖춘 제품 개발 조직으로 공식 인증 받았다.

이 인증은 한화비전 제품의 개발 신뢰성을 보장한다. 또한, 요구사항 식별부터 보안 기능 설계 및 구현, 보안 문제 검토 및 관리, 문제 해결을 위한 펌웨어 및 문서 배포에 이르는 견고한 보안 프로세스를 갖추고 있음을 의미한다.

한화비전은 앞으로도 제품 수명 주기 전반에 걸쳐 보안 관리를 지속적으로 강화해, 고객과의 신뢰와 책임에 대한 약속을 이행하고 글로벌 시장에서 우수한 서비스를 제공할 것이다.

4. 보안 스토리지 구현을 위한 시큐어 엘리먼트 활용

보안 스토리지(Secure Storage)는 민감한 데이터를 안전하게 저장하고, 무단 접근 또는 유출로부터 데이터를 보호하기 위한 필수 기술이다.

한화비전은 Wisenet 7 부터 HTPM(Hanwha Trusted Platform Module)을 개발, SoC 와 독립적인 하드웨어 TPM 모듈을 통해 하이엔드 제품에 보안 스토리지를 구현했다. 이러한 광범위한 경험을 바탕으로, 한화비전은 Wisenet 9 기반 제품에 최신 FIPS 140-3 레벨 3 표준 인증을 획득한 하드웨어 시큐어 엘리먼트(Secure Element)를 적용했다. 시큐어 엘리먼트를 통해 한화비전 IP 카메라는 민감한 데이터 저장을 위한 안전한 저장소를 제공하게 된다.

4.1. FIPS 140-3 인증

FIPS 140-3 은 보안 스토리지와 같은 암호화 모듈의 보안을 평가하기 위한 국제 표준으로, 글로벌 시장에서 신뢰성을 보장한다. FIPS 140-2 에 비해 FIPS 140-3 은 다음과 같이 다양한 영역에서 중요한 개선 사항과 강화된 보안 요구사항을 필요로 한다.

- **ISO/IEC 19790 및 ISO/IEC 24759 통합:** FIPS 140-3 은 ISO/IEC 19790(암호화 모듈 보안 요구사항) 및 ISO/IEC 24759(암호화 모듈 테스트 요구사항) 표준을 기반으로 한다. 이를 통해 국제 표준과의 부합성이 더욱 높아졌다.
- **모듈 유형 분류:** 암호화 모듈을 하드웨어, 소프트웨어, 펌웨어, 하이브리드 모듈 유형으로 정밀하게 분류해 평가 기준을 세분화했다.
- **소프트웨어/펌웨어 보안:** 소프트웨어 및 펌웨어 무결성 검증 방법에 대한 명확한 정의를 포함한다. 특히, 레벨 2 는 디지털 서명 기반과 메시지 인증 코드 기반 무결성을 모두 인정하는 반면, 레벨 3 은 디지털 서명 기반 무결성만 인정한다는 차이가 있다.
- **자체 테스트:** 암호화 모듈은 작동 전에 사전 작동 자체 테스트를 수행해야 하며, 특정 기능을 제공할 때 조건부 자체 테스트를 수행해야 한다.
- **수명 주기 보증:** 설계, 개발, 배포부터 폐기에 이르는 암호화 모듈의 전체 수명 주기를 포괄하는 보안 요구사항이 강화되었다.

4.2. FIPS 140-3 보안 레벨

FIPS 140-3 은 암호화 모듈을 4 가지 점진적인 레벨로 분류하며, 각 레벨에 따라 보안 요구사항의 엄격성이 높아진다. 한화비전이 사용하는 시큐어 엘리먼트는 레벨 3 을 달성하도록 설계되었는데, 이 레벨은 다음과 같은 주요 영역에서 레벨 2 에 비해 향상된 보안을 제공한다.

- 역할(Roles)/서비스(Services)/인증(Authentication)
- 소프트웨어/펌웨어 보안

- 물리적 보안
- 비침해 보안(Non-Invasive Security)
- 보안 매개변수 관리(Security Parameter Management)
- 수명 주기 보증

[표 2] FIPS 140-3 요약[1]

Requirement Area		Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification		Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes of operation. Description of cryptographic module including all hardware, software, and firmware components. All services provide status information to indicate when the service utilizes an approved cryptographic algorithm, security function, or process in an approved manner.			
Cryptographic Module Interfaces		Required and optional interfaces. Specification of all interfaces and of all input and output data paths		Trusted channel	
Roles, Services, and Authentication		Logical separation of required and optional roles and services	Role-based or identity-based operator authentication	Identity-based operator authentication	Multi-factor authentication
Software / Firmware Security		Approved integrity technique, or EDC based integrity test. Defined SFMI, HFMI and HSMI. Executable code	Approved digital signature or keyed message authentication code-based integrity test	Approved digital signature-based integrity test	
Operational Environment		Non-modifiable. Limited or Modifiable Control of SSPs	Modifiable. Role-based or discretionary access control. Audit mechanism		
Physical Security		Production-grade components	Tamper evidence. Opaque covering or enclosure	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing EFP or EFT	Tamper detection and response envelope. EFP. Fault injection mitigation
Non-Invasive Security		Module is designed to mitigate against non-invasive attacks specified in Annex "F".			
		Documentation and effectiveness of mitigation techniques specified in Annex "F"		Mitigation testing	Mitigation testing
Security Parameter Management		Random bit generators, SSP generation, establishment, entry & output, storage & zeroization			
		Automated SSP transport or SSP agreement using approved methods			
		Manually established SSPs may be entered or output in plaintext form		Manually established SSPs may be entered or output in either encrypted form, via a trusted channel or using split knowledge procedures	
Self-Tests		Pre-operational: software/firmware integrity, bypass, and critical functions test			
		Conditional: cryptographic algorithm, pair-wise consistency, SW/FW loading, manual entry, conditional bypass & critical functions test			
Life-Cycle Assurance	Configuration Management	Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout lifecycle		Automated configuration management system	
	Design	Module designed to allow testing of all provided security related services			
	FSM	Finite State Model			
	Development	Annotated source code, schematics or HDL	Software high-level language. Hardware high-level descriptive language		Documentation annotated with pre-conditions upon entry into module components and postconditions expected to be true when components is completed
	Testing	Functional testing		Low-level testing	
	Delivery & Operation	Initialization procedures	Delivery procedures		Operator authentication using vendor provided authentication information
	Guidance	Administrator and non-administrator guidance			
Mitigation of Other Attacks		Specification of mitigation of attacks for which no testable requirements are currently available			Specification of mitigation of attacks with testable requirements

[1] 참고: https://lightshipsec.com/fips-140-3-is-here/

각 레벨별 보안 요구사항을 요약하면 다음과 같다.

- **레벨 1:** 가장 낮은 보안 레벨로, 기본적인 암호화 및 키 관리 기능을 요구하며 소프트웨어 전용 모듈에 적합하다.
- **레벨 2:** 무단 접근을 방지하고 물리적 변조를 감지하기 위한 물리적 보안 조치(잠금 장치, 변조 방지 스티커 등)와 역할 기반 인증을 요구한다.
- **레벨 3 (한화비전 시큐어 엘리먼트에 적용):** 더 높은 수준의 물리적 보안을 요구한다. 물리적 침입 시도를 감지하는 변조 방지 저항, 신원 기반 인증, 온도 및 전압 변동을 포함한 환경 공격에 대한 보호를 요구한다.
- **레벨 4:** 가장 높은 보안 레벨로, 매우 정교한 공격을 방지하는 데 중점을 둔다. 변조 방지 기능, 다중 인증, 환경 공격 또는 오류 주입 감지 시 민감한 데이터를 삭제하는 기능을 포함한다.

4.3. 시큐어 엘리먼트 활용 사례 및 시나리오

최종 사용자가 디바이스에 내장된 시큐어 엘리먼트의 세부적인 활용 방식이나 구체적인 역할을 알 필요는 없다. 제품 전반에 걸쳐 강력한 사이버보안을 보장하는 것은 전적으로 제조업체의 책임이다. 때문에, 보안 기능은 복잡성이나 불편함을 초래하지 않으면서 사용자를 보호하도록 설계되어야 한다.

한화비전은 책임감 있는 제조업체로서 암호화 키, 사용자 설정 패스워드 등을 통해 보호가 필요한 민감한 데이터를 선제적으로 식별해 왔다. 아래 표3은 이러한 데이터 범주를 자세히 보여준다.

민감한 데이터를 보호하기 위한 가장 효과적인 방법 중 하나는 디바이스에 데이터가 저장될 때 암호화하는 것이다. 그러나 암호화 키 자체도 안전하게 보호되어야 한다. 이를 해결하기 위한 가장 효과적인 솔루션은 디바이스에 내장된 시큐어 엘리먼트를 활용해 민감한 데이터를 저장하고 관리하는 것이다.

[표 3] 민감 데이터 유형

범주	민감 데이터
사용자 설정 패스워드	디바이스 접근을 위한 로그인
	SMTP/FTP/NAS 서버 접근
사용자 설정 암호화 키	802.1x 접근을 위한 개인 키/인증서
	HTTPS/TLS 를 위한 개인 키/인증서
	802.1x 인증 서버의 진위 확인을 위한 CA 인증서
제조업체 설정 암호화 키	HTTPS/TLS, 디바이스 인증을 위한 개인 키/인증서
	보안 부팅/서명된 펌웨어 검증을 위한 공개 키

	오픈 플랫폼 앱의 진위 확인을 위한 CA 인증서
	상호 인증의 진위 확인을 위한 CA 인증서
	백업/복구를 위한 비밀 키

한화비전 시큐어 엘리먼트는 제조 과정에서 생성되는 고유한 대칭 키를 사용해 디바이스별로 민감한 데이터를 암호화한다. 이 키는 FIPS 140-3 레벨 3 인증을 받은 시큐어 엘리먼트에 의해 보호되므로 노출될 가능성이 극히 낮다. 만에 하나 유출되더라도 해당 특정 디바이스에만 영향을 미치게 된다. 이러한 격리(isolation)는 잠재적인 보안 사고의 영향을 크게 제한하고 전반적인 위험을 최소화한다.

5. 소프트웨어 공급망 보안 강화

한화비전은 Wisenet 9 제품군을 시작으로 소프트웨어 플랫폼에 대한 SBOM(Software Bill of Materials) 배포를 시작했다.

5.1. SBOM 소개

SBOM 은 소프트웨어 제품을 구성하는 모든 소프트웨어 구성 요소, 특히 모든 오픈소스 및 서드파티 라이브러리를 명확하게 식별하는 상세 목록이다. 이러한 구성 요소는 다양한 소스에서 개발 저장소로 유입될 수 있으며, 이 과정에서 알려진 오픈소스 취약점이 의도치 않게 제품에 포함될 수 있다.

이러한 이유로 오픈소스 취약점 관리는 소프트웨어 공급망 보안의 핵심적인 부분이 되었으며, SBOM 은 효과적인 통제를 가능하게 하는 데 중요한 역할을 한다. SBOM 을 관리하고 유지함으로써 소프트웨어 공급망의 투명성과 보안이 향상되며, 다음과 같은 이점을 제공한다.

- **소프트웨어 투명성 및 신뢰성 향상:** 최신 소프트웨어는 오픈소스 및 서드파티 라이브러리에 크게 의존한다. SBOM 은 소프트웨어에 포함된 모든 구성 요소를 명확하게 나열해, 보안 취약점이나 악성 코드가 포함된 구성 요소를 신속하게 식별할 수 있도록 한다. 이는 소프트웨어 공급망의 신뢰성을 높이고, 고객 및 사용자에게 더 큰 투명성을 제공한다.

  예시: Log4j 취약점(Log4Shell, 2021)과 같은 보안 문제가 발생했을 때, SBOM 을 활용하면 해당 라이브러리를 포함하는 소프트웨어를 신속하게 식별하고 대응할 수 있다.

- **규제 준수 및 산업 표준 충족**: 많은 국가에서 규제 준수를 위해 SBOM 사용을 요구하고 있다.

  예시: 미국 행정명령 14028(2021)에 따라, 연방 정부와 계약하는 소프트웨어 공급업체는 SBOM 을 제공해야 한다. 또한, SBOM 을 사용해 표준 준수 여부를 확인하면 소프트웨어 라이선스 위반과 관련된 법적 문제를 예방할 수 있다.

  예시: SBOM 은 산업 표준 ISO/IEC 5230 [Linux Foundation OpenChain Specification 기반 오픈소스 소프트웨어 라이선스 준수 표준]의 핵심 요소이다.

- **취약점 관리 및 보안 사고 대응:** 소프트웨어 구성 요소의 버전 정보를 포함함으로써, SBOM 은 고객이 일반 취약점 인덱스(Common Vulnerability Index)와 비교해 보안 취약점을 신속하게 식별할 수 있도록 한다. 보안 사고 발생 시, SBOM 은 고객이 영향을 받는 소프트웨어를 즉시 식별하고 대응하는 데 도움을 준다.

- **효율적인 소프트웨어 유지보수:** SBOM 은 고객과 제조업체 모두 소프트웨어 구성 요소에 대한 정보를 체계적으로 관리하는 데 도움을 주어, 오래된 구성 요소를 업데이트하거나 더 이상 사용되지 않는 구성 요소를 제거하는 등의 유지보수 작업을 더 쉽게 수행할 수 있도록 한다.

- **오픈소스 라이선스 준수:** SBOM 은 제품에 포함된 오픈소스 라이브러리 및 관련 라이선스를 명확하게 문서화해 라이선스 준수를 보장한다. 이는 제조업체가 GPL, Apache, MIT 와 같은 라이선스의 요구사항을 충족하는 데 도움을 준다.
- **소프트웨어 공급망 공격 방지:** 최근 소프트웨어 공급망 공격(SolarWinds, Log4j, Kaseya 사건 등)이 증가함에 따라, SBOM 은 공급망 전반의 취약점을 식별하고 방지하는 데 중요한 역할을 한다. 이는 소프트웨어 구성 요소의 출처를 추적하고 신뢰할 수 없는 구성 요소를 제거하는 데 도움을 준다.

5.2. 한화비전 SBOM 특징

한화비전은 고객이 필수 정보를 쉽게 접근하고 관리할 수 있도록 SBOM 을 공개했다. 여기에는 오픈소스 소프트웨어 구성 요소의 이름과 버전, 출처, 기능 설명, 라이선스, 저작권자, CPE(Common Platform Enumeration), 패키지 URL(purl), 취약점 패치 세부 정보 등이 포함된다.

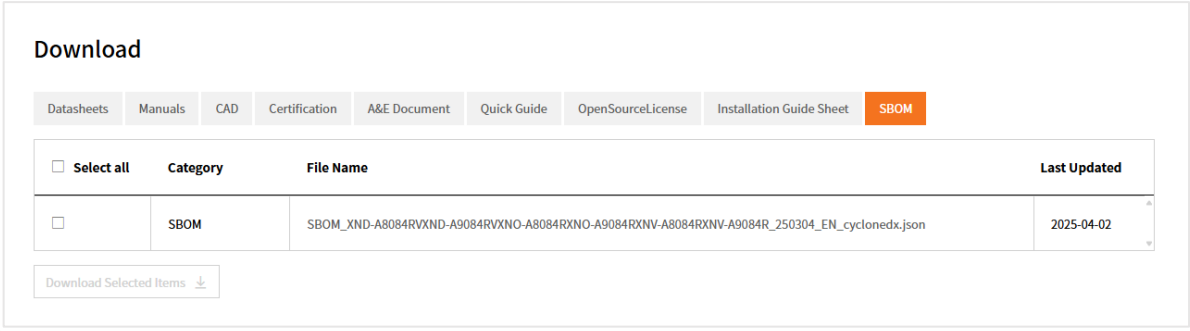

그림 1. 한화비전 웹사이트에 공개된 XNV-A9084R SBOM

한화비전은 단순히 SBOM 제공을 넘어, 각 제품의 장기 펌웨어 지원 정책에 따라 정기적인 펌웨어 업데이트를 통해 알려진 오픈소스 취약점을 선제적으로 해결하는 데 전념하고 있다.

- 한화비전 SBOM 은 OWASP(Open Web Application Security Project, https://owasp.org/)가 주도하는 표준인 Cyclone DX 형식을 사용하며, JSON 파일로 제공된다.
- SBOM 유틸리티 또는 뷰어를 사용하여 내용을 쉽게 확인하고 검색할 수 있다.

5.3. 한화비전 SBOM 활용법

고객은 한화비전 SBOM 을 효과적으로 활용해 보안을 강화하고 소프트웨어 구성 요소 관리를 간소화할 수 있다.

1. **취약점 영향 평가**: 특정 오픈소스 소프트웨어에 알려진 CVE(Common Vulnerabilities and Exposures)가 발생했을 때, 고객은 공급업체가 제공하는 제품별 SBOM 을 참조해 해당 제품이 영향을 받았는지 확인할 수 있다. 이를 통해 어떤 오픈소스 소프트웨어 및 버전이 영향을 받았는지 신속하게 파악할 수 있다.

2. **패치 확인**: 영향을 받은 버전이 식별되면, 고객은 SBOM 에서 사용 가능한 취약점 패치 (pedigree) 정보를 확인해야 한다. 경우에 따라 CVE 에 대한 보안 패치가 이전 버전으로 백포팅될 수 있으므로, 사용 중인 특정 버전이 실제로는 취약하지 않을 수도 있다.
3. **영향 미확인 시 제조업체 문의**: SBOM 에 취약점 패치가 명시되어 있지 않다면, 이는 빌드 시 컴파일러에 의해 취약한 코드가 포함되지 않았거나 해당 취약점이 외부로 노출되지 않았음을 의미할 수 있다. 이러한 경우, 고객은 제조업체에 문의해 제품이 실제로 영향을 받았는지 확인해야 한다.
4. **소프트웨어 업데이트 요청**: 실제 영향이 확인되면, 고객은 제조업체에 영향을 받은 오픈 소스 소프트웨어의 업데이트 또는 패치를 요청할 수 있다. 단종된 모델의 경우, 지원 여부는 장기 펌웨어 지원 정책의 적용 가능성 및 기간에 따라 달라진다.

보다 자세한 내용은 Long-Term Firmware Support Policy 문서를 참고하면 된다.

6. 결론

제품 보안은 단순히 제품 취약점을 막는 것을 넘어선다. 여기에는 소프트웨어 구성 요소의 공급망 보안 관리, 개발 환경 및 인력에 대한 보안, 그리고 제품 내에 저장되고 처리되는 데이터를 보호하는 것까지 포괄적으로 포함된다.

보안 취약점이 어떻게 발생하는지 이해하면 왜 포괄적인 보호 조치가 필수적인지 명확히 알 수 있다. 취약점은 제품 기획 및 설계 단계부터 구현, 유통, 심지어 운영에 이르는 모든 단계에서 유입될 수 있다. 물론, 비용 절감을 위해 이러한 취약점을 선제적으로 제거하는 것이 이상적이지만, 현실적으로는 어려운 경우가 많다. 그렇기 때문에 새로운 취약점이 발견되었을 때 신속하게 대응할 수 있는 개발 및 취약점 대응 프로세스를 갖추는 것이 매우 중요하다. 글로벌 보안 표준은 이러한 통제를 의무화하고 있으며, 한화비전은 우수한 솔루션을 제공하기 위해 이러한 요구사항을 제품 및 개발 프로세스에 지속적으로 통합하고 있다.

한화비전은 제품 취약점 식별을 위한 침투 테스트 수행, 개발자를 위한 내부 버그 바운티 프로그램(Bug Bounty Program) 운영, 철저한 보안 검토 등 선제적인 보안 노력을 계속하고 있다. 또한, CVE Numbering Authority(CNA)로서 취약점 식별 및 공개에 대한 역할을 충실히 이행하고 있다. 한화비전은 신뢰할 수 있는 공급망과 사이버보안에 대한 확고한 집중을 통해, 세계적 수준의 영상보안 솔루션 제공업체로서 선두 자리를 굳건히 지키고 있다.

7. 레퍼런스

- [5.11-1] Providing a function to easily delete user information.
  ※ User information: password, key, environment configuration information, personal information, etc.
- [5.11-2] Providing a function to easily remove personal information stored in related services
  ※ Case only when the user's personal information (account information, video, etc.) is stored in a cloud service connected to the device
- [5.11-3] Providing concise and accurate user documentation on how to delete personal information.
  ※ Case only when personal information is stored.
- [5.11-4] Providing clear confirmation and successful completion messages for all deletion functions that the personal information has been deleted.
  ※ Case only when personal information is stored.
- [6-1] Providing transparent information on personal information processing.
  ※ Personal information list, purpose/method/subject of use, etc.
  ※ Case only when personal data is processed.
- [6-2] Obtaining customer’s consent for personal information processing.
  ※ Customer’s consent must be obtained in a valid manner.
  ※ Case only when personal information is processed based on the customer's consent.
- [6-3] Providing customers with the right to withdraw consent to personal information processing at any time.
  ※ Case only when personal information is processed based on the customer's consent.
- [6-4] Personal information processing must be kept to the minimum necessary for the intended function.
  ※ Case only when telemetry data is collected.
- [6-5] Providing customers with information on telemetry data.
  ※ List of telemetry data, purpose/method/subject of use, etc.
  ※ Case only when telemetry data is collected.

Hanwha Vision
13488 Hanwha Vision R&D Center,
6 Pangyo-ro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
www.HanwhaVision.com