Hanwha Vision

공급망 보안을 위한 한화 **SBOM**

2024. 9

V1.0

차례

1. 한화 SBOM 의 필요성

1.1. 공급망 위험

1.2. 위험 해결을 위한 SBOM 의 등장

1.3. SBOM 관련 법적 동향

2. 한화비전 SBOM 소개

2.1. 한화비전 SBOM 의 특징

2.2. SBOM 효과적인 사용방법

2.3. SBOM 의 한계와 향후 과제

3. 맺음말

1. 한화 SBOM의 필요성

오픈소스를 잘 활용하여 짧은 개발주기로 양질의 제품을 만드는 것은 조직과 제조사에 선택사항 보다는 필수사항이 되었습니다.

오픈소스 소프트웨어가 소프트웨어 공급망의 중요한 부분이 되면서, 오픈소스 소프트웨어 구성요소를 검증 및 관리하지 않으면 공급망의 소싱 및 조달 측면에서 조직과 제품에 위협이 될 수 있습니다.

이는 한화비전과 같은 감시 장비 제조사의 경우도 마찬가지이며, 사용되는 오픈소스 유형이 증가하고 제공되는 제품 유형이 더욱 다양해짐에 따라 오픈소스 소프트웨어의 보안 취약성을 체계적으로 관리하고 추적할 수 있는 프로세스에 대한 필요성이 요구되고 있습니다.

1.1. 공급망 위험

오픈소스 소프트웨어 구성요소의 위험에는 두가지 주요 유형이 있습니다. 라이선스 위험과 취약성 위험으로, 아래는 각 위험에 대한 설명입니다.

■ 라이선스 위험:

오픈소스 소프트웨어는 무료로 사용할 수 있지만, 그렇다고 해서 따라야 할 요구사항이 없다는 것은 아닙니다. 오픈소스 소프트웨어는 수백 가지 라이선스 중 하나에 따라 배포되거나 라이선스 없이 배포될 수 있으므로 저작권 침해 위험을 줄이기 위해 각 라이선스에 필요한 의무를 이해하고 준수하는 것이 중요합니다.

예를 들어, 대부분의 오픈소스 라이선스는 개발자가 오픈소스 소프트웨어를 복사, 사용, 수정 또는 배포할 때 적절한지 저작권 및 라이선스 고지 사항을 제공하도록 요구합니다.

- **LGPL(GNU Lesser General Public License)** 라이선스는 개발한 독점 소프트웨어가 오픈소스 소프트웨어의 파생물이 되지 않도록 하기 위해 오픈소스 소프트웨어와 결합할 때 동적 링크를 요구합니다.
- **GPL (GNU General Public Licenses)** 라이선스는 오픈소스 소프트웨어를 분리된 작업(Separate Work)으로 사용해야 합니다.

따라서, 조직에서는 이러한 다양한 요구사항을 인식하고 준수하는 것이 중요합니다.

■ **취약성 위험:**

최근 몇 년 동안 일반적으로 사용되는 Log4J, Curl, Apache Struts, and OpenSSL 과 같은 널리 알려진 오픈소스 소프트웨어의 취약성이 많이 발견되었습니다. 이는 기업이나 조직의 소프트웨어 공급망에 취약점이 쉽게 유입될 수 있다는 것을 보여줍니다.

오픈소스 소프트웨어의 보안 품질이 독점 소프트웨어에 비해 더 우수하거나 더 나쁘다고 말할 수는 없지만 한 가지 확실한 것은 소스코드가 공개되어 있는 오픈소스 소프트웨어의 특성상 보안 전문가들에 의해 오픈소스 취약성이 계속 보고되어 오픈소스 생태계를 정화시키는 자정 작용을 할 것이라는 점입니다. 그러나 소프트웨어의 개방성은 공급망을 위협하는 수단으로 사용될 수도 있습니다.

1.2. 위험 해결을 위한 SBOM의 등장

이러한 위험을 해결하기 위해 유입되는 타사 소프트웨어, 특히 오픈소스 소프트웨어의 구성요소를 관리하는 것이 중요 해졌고, **SBOM (Software Bill Of Materials)** 이라는 관리 도구의 필요성이 대두되었습니다. 비타민, 미네랄, 설탕 등의 식품 라벨링과 같이 제조 및 엔지니어링에 사용되는 BOM(Bill Of Materials)과 유사하게 SBOM 은 해당 구성요소에 대한 주요 정보를 제공할 수 있습니다. 관리 도구로서 SBOM 은 오픈소스 소프트웨어 구성 요소의 라이선싱과 취약성에 대한 정보 제공의 균형을 유지해야 하며, 공급망의 다양한 플레이어 및 이해관계자와의 통합 커뮤니케이션을 위해 일관되고 자동화된 형식으로 배포되어야 합니다.

이를 위해 한화비전은 국제 웹 보안 표준 단체인 오픈 웹 어플리케이션 시큐리티 프로젝트(OWASP, https://owasp.org/)가 주도하는 사이클론 DX 포맷을 SBOM 배포 포맷으로 선정하고 SBOM 유틸리티를 통해 사이클론 DX 표준을 준수하는지 검증하였습니다.

```
Welcome to the sbom-utility! Version `v0.16.0` (sbom-utility) (windows/amd64)
================================================================================
[INFO] Loading (embedded) default schema config file: `config.json`...
[INFO] Loading (embedded) default license policy file: `license.json`...
[INFO] Attempting to load and unmarshal data from: `../SBOM_PNM-C16083RQZ,PNM-C32083RQZ_240722_EN_cyclonedx.json`...
[INFO] Successfully unmarshalled data from: `../SBOM_PNM-C16083RQZ,PNM-C32083RQZ_240722_EN_cyclonedx.json`
[INFO] Determining file's BOM format and version...
[INFO] Determined BOM format, version (variant): `CycloneDX`, `1.6` (latest)
[INFO] Matching BOM schema (for validation): schema/cyclonedx/1.6/bom-1.6.schema.json
[INFO] Loading schema `schema/cyclonedx/1.6/bom-1.6.schema.json`...
[INFO] Schema `schema/cyclonedx/1.6/bom-1.6.schema.json` loaded.
[INFO] Validating `../SBOM_PNM-C16083RQZ,PNM-C32083RQZ_240722_EN_cyclonedx.json`...
[INFO] BOM valid against JSON schema: `true`
```

[그림 1] 사이클론 DX 형식에 대한 유효성 검사

SBOM 표준과 호환성 및 준수를 보장하는 것이 중요하므로 자동화 관리 도구로서 SBOM 의 효율성을 저해할 수 있는 일관성 문제를 방지하기 위해 SBOM 유틸리티를 선택하였습니다.

1.3. SBOM 관련 법적 동향

많은 기업과 정부기관에서 소프트웨어의 보안과 품질을 보장하기 위해 소프트웨어 공급망 관리의 일부로서 SBOM 의 필요성과 중요성을 강조하고 있습니다.

또한, 유럽연합의 사이버 복원력법, 바이든 행정부의 국가 사이버 보안 개선에 관한 행정명령(EO-14028), FDA 의 사이버 기기 규정, PCI-DSS 4.0 등 많은 국가에서 SBOM 사용을 의무화하거나 장려하는 법률과 규정이 개발되고 있습니다. 아래 표에는 각 법률 및 규정의 개요, 영향을 받는 분야, 시행 일정이 나와 있습니다.

이에 한화도 SBOM 보급의 흐름에 동참할 필요가 있다고 판단하였습니다.

[표 1] SBOM 규정 준수 환경[1]

법률 및 규정	영향 받는 분야	제공형태	시행일정
EO 14028	미국 연방 정부에 판매하는 공급업체; 2022 년 9 월 14 일 이후에 출시되거나 업데이트된 SW	준수를 확인하는 자체 증명 양식을 제출하고, 요청 시 SBOM 을 제공	중요 인프라의 경우 2024 년 6 월 11 일, 기타 모든 경우 2024 년 9 월 11 일
Cyber Resilience Act	EU 에서 판매하는 디지털 제품 제조사	최상위 SBOM 제공	발행 후 36 개월, 2024 년 봄 또는 여름에 예상(취약성 보고 요구사항은 더 일찍 발효됨)
FDA	사이버 장치에 대한 시판 전 제출 절차를 거치는 의료 기기 제조사	NTIA 준수 SBOM 과 모든 구성요소에 대한 지원 정보 및 취약성 평가 (제어 및 완화 단계 포함)	요구사항은 2023 년 3 월 29 일 또는 그 이후에 제출하는 경우에 적용됨. FDA 는 2023 년 10 월 1 일에 “수락거부” 권한을 부여 받음
PCI-DSS	결제 소프트웨어 제공자; CDE(Cardholder Data Environment)의 일부이거나 CDE 에 부정적인 영향을 미칠 가능성이 있는 모든 SW	범위에 있는 모든 맞춤형 개발 및 타사 SW 구성 요소의 목록	2025 년 3 월 31 일 의무적 시행

[1] 이 표는 https://fossa.com/learn/sboms#the-sbom-regulatory-compliance-landscape 를 참조하여 작성되었습니다.

2. 한화비전 SBOM 소개

2.1. 한화비전 SBOM의 특징

한화비전은 오픈소스 소프트웨어 컴포넌트의 이름과 버전, 출처, 기능설명, 라이선스, 저작권 소유자, 플랫폼 식별자(Common Platform Enumeration (CPE)), 패키지 URL (purl) 및 취약성 패치 정보 등 SBOM 에 필수적인 정보를 명시하고 관리합니다.

■ **SBOM 에서 제공하는 정보**

✓ Name (components > name)

```
name:                    "lighttpd"
```

✓ Version (components > version)

```
version:                 "1.4.53"
```

✓ Source url (components > supplier > url)

```
▼ supplier:
  ▼ url:
      0:                 "https://www.lighttpd.net"
```

✓ Functional description (components > description)

```
▼ description:           "lighttpd (pronounced /lighty/) is a secure, fast, compliant, and very flexible web server
                         that has been optimized for high-performance environments. lighttpd uses memory and CPU
                         efficiently and has lower resource use than other popular web servers. Its advanced
                         feature-set (FastCGI, CGI, Auth, Output-Compression, URL-Rewriting and much more) make
                         lighttpd the perfect web server for all systems, small and large."
```

✓ License (components > licenses > license > name)

```
▼ licenses:
  ▼ 0:
    ▼ license:
        name:            "BSD 3-clause License"
```

✓ Copyright holder (components > copyright)

```
▼ copyright:             "Copyright (c) 1991-1992, RSA Data Security, Inc.\nCopyright (c) 1995-1996 Open Market,
                         Inc.\nCopyright (c) 2010, Norio Kobota\nCopyright (c) 2017, Glenn Strauss\nCopyright (c)
                         2004, Jan Kneschke, incremental "
```

✓ CPE [Common Platform Enumeration] (components > cpe)
[※ 존재하는 경우만 제공]

```
cpe:                     "cpe:2.3:a:lighttpd:lighttpd:1.4.53:*:*:*:*:*:*:*"
```

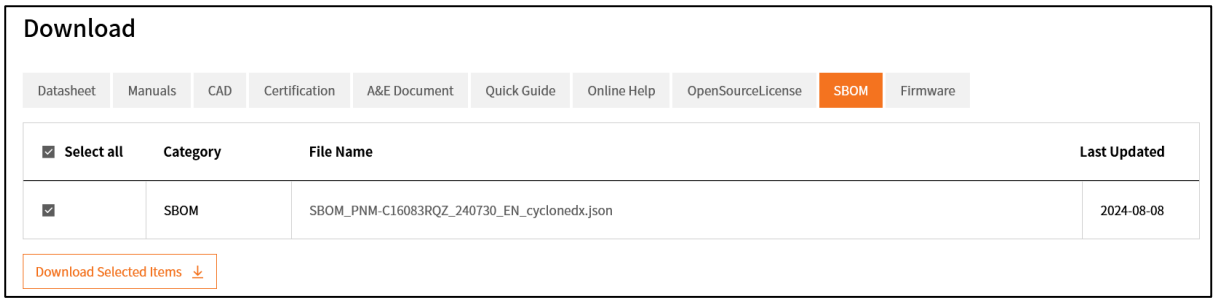
✓ Purl [Package Uniform Resource Locators] (components > purl)
[※ 존재하는 경우만 제공]

```
purl:                    "pkg:deb/debian/lighttpd@1.4.53-4%2Bdeb10u1"
```

✓ Vulnerability patch (components > pedigree > patches) [※ 존재하는 경우만 제공]

2.2. SBOM 효과적인 사용방법

SBOM 은 한화비전 홈페이지[2]에서 각 제품별로 다운로드 받을 수 있습니다.



[그림 2] SBOM 다운로드 페이지

SBOM 은 소프트웨어 투명성을 높이는데 중요한 역할을 하며, 고객이 사용하는 소프트웨어에 대해 정보에 따라 결정을 내릴 수 있도록 지원합니다. 따라서 고객은 제조사에서 제공하는 SBOM 에 언급된 소프트웨어에 대한 정보를 사용하여 제품 취약성을 파악하고 다음과 같은 후속조치를 취할 수 있습니다.

■ **SBOM 고객 사용 시나리오:**

1. 고객이 특정 오픈소스 소프트웨어의 알려진 CVE(Common Vulnerabilities and Exposures)로 인해 자사 제품이 영향을 받는지 확인하고자 합니다. 고객은 공급업체에 문의할 필요 없이 공급업체가 배포한 제품별 SBOM 을 검색하여 어떤

[2] 한화비전 홈페이지 - https://www.hanwhavision.com

오픈소스 소프트웨어가 해당 취약점의 영향을 받는지 확인할 수 있습니다. 그리고 해당 취약점의 영향을 받는 오픈소스 소프트웨어와 버전을 확인합니다.

2. 해당 오픈소스 소프트웨어가 취약점의 영향을 받았다면, 취약성에 대한 패치(SBOM 의 유래(pedigree) 정보)가 있는지 확인합니다. 종종 보안 CVE 가 이전 버전으로 백포트 되어 취약하지 않음을 나타내는 경우도 있습니다.

3. SBOM 에 취약점 패치가 없는 경우 취약점 관련 코드가 빌드 시 컴파일러에 포함되지 않았거나 취약점이 외부에 노출되지 않은 경우가 있을 수 있으므로, 제조사에 문의하여 해당 취약점이 실제로 제품에 영향을 미치는지 확인해야 합니다. 실제 영향이 있는 경우 제조사에 오픈소스 소프트웨어의 업데이트 또는 패치를 요청할 수 있습니다. 단, 단종된 모델인 경우에는 장기 펌웨어 지원 정책의 적용 여부와 기간에 따라 지원 여부가 결정됩니다.

   [자세한 내용은 **장기 펌웨어 지원 정책** 문서를 참조하세요.]

■ SBOM 대응 프로세스 소개:

1. 한화는 각 제품에 사용된 오픈소스 소프트웨어를 파악하여 SBOM 을 작성합니다.

2. 한화는 SBOM 에 등재된 오픈소스 소프트웨어의 취약점을 정기적으로 모니터링하고 평가하여 위험을 식별합니다.

3. 식별된 위험에 대해서는 고객에게 미치는 영향과 해당 취약점을 이용한 제품의 공격 가능성을 고려하여 취약점의 위험 수준을 결정합니다.

4. 영향력이 있다고 판단되는 위험은 오픈소스 소프트웨어에 버전 업데이트 또는 패치 형태로 개선된 펌웨어를 배포하거나 공격 가능성을 제거하는 방법을 보여주는 보안 가이드를 배포하여 위험을 완화합니다.

2.3. SBOM의 한계와 향후 과제

모든 SBOM 에는 한계가 있을 수 있지만, 한화비전은 고객과 협력하여 소프트웨어 공급망 관리 문제를 해결하고 제품에 내재된 보안 취약점을 투명하고 선제적으로 해결하기 위해 노력할 것입니다.

■ 한화비전 SBOM 배포 대상 과제:

SBOM 은 펌웨어 버전 v24.00.00 부터 배포됩니다.
※ 펌웨어 버전 v24.00.00 이전 제품은 배포 대상에서 제외

■ SBOM 장점 vs 단점:

- **장 점:** 고객에게 소프트웨어 구성요소에 대한 투명성을 제공하고 제조사가 오픈소스 취약성에 대해 사전 대응할 수 있습니다.
- **단 점:** 악의적인 공격자는 소프트웨어 구성요소에 대한 공개 정보를 공격에 악용할 수 있으며, 공개된 정보로 인해 특정 디바이스를 표적으로 삼을 수 있습니다. CPE 를 통해 제공되는 오픈소스 취약성에 대한 정보는 완전하지 않으므로 잘못된 정보로 인해 디바이스가 취약한 것으로 잘못 진단(오탐)될 가능성이 있습니다.

■ 한화비전 SBOM 의 한계 및 향후 계획:

SBOM 에는 오픈소스 소프트웨어에 대한 정보만 포함되어 있습니다. 모든 독점 소프트웨어는 제외됩니다. 또한 현재 버전의 SBOM 에는 종속성 정보가 포함되어 있지 않습니다. 향후 종속성 정보를 포함한 추가 정보를 제공하고 더 많은 모델에 대해 확장할 계획입니다.

■ 제품 보안을 강화하기 위한 지속적인 보안 활동의 중요성:

제품에 존재하는 오픈소스 취약점은 제품 취약점 및 사이버 보안을 평가하는 데 있어 한가지 요소일 뿐 전부는 아니므로 오픈소스 취약점을 고려하면서 실제 제품에 대한 취약점 평가를 수행하는 것이 중요합니다. 즉, 오픈소스 업데이트나 패치도 중요하지만 오픈소스 취약점이 실제 제품에서 어떻게 나타나고 있는지를 제품 관점에서 평가하는 것이 더 중요합니다.

3. 맺음말

오픈소스 취약점과 관련하여 제품 사이버 보안을 고려할 때, 이러한 취약점의 대부분은 현실 세계에서 악용하거나 접근할 수 없다는 점에 유의하는 것이 중요합니다. 그러나 공급망의 일부 오픈소스 취약점은 매우 위협적일 수 있으며, 이러한 위험에 대한 관리와 가시성의 필요성에 대해 업계와 여러 국가에서 공감대가 형성되고 있습니다. 하지만, 이제 새로운 고위험 취약점이 공개되면 SBOM 을 검색하여 제품에 해당 오픈소스 구성요소가 포함되어 있는지 확인할 수 있습니다.

한화비전은 단순히 SBOM 을 배포하는 것에 만족하지 않고 제품의 장기 펌웨어 지원 정책에 따라 정기적인 펌웨어 업데이트를 통해 오픈소스 소프트웨어 구성요소의 알려진 취약점으로 인한 위험을 제거하기 위해 노력할 것입니다. 또한 제품 취약점을 찾기 위한 모의 침투테스트, 내부 개발자를 대상으로 버그 바운티 프로그램, 보안 점검, 보안 리뷰 등을 지속적으로 실시하며 신뢰의 공급망과 사이버 보안에 대한 지속적인 관심을 통해 CNA(CVE Numbering Authority: CVE 번호 부여 기관)로서 주어진 역할에 충실하고 세계적인 영상 감시 제조 리더로 거듭날 것입니다.

Hanwha Vision Co., Ltd.
13488 Hanwha Vision R&D Center,
6 Pangyo-ro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do
TEL 070.7147.8771-8
FAX 031.8018.3715
www.HanwhaVision.com