본 사업은 과학기술정보통신부 및 정보통신기획평가원(IITP)의
정보보호핵심원천기술개발 사업 지원으로 수행되었습니다.

국·내외 SW공급망보안 현황 및 SBOM 도구 실증 결과보고서

2025. 12

kisia 한국정보보호산업협회
Korea Information Security Industry Association

국·내외 SW공급망보안 현황 및 SBOM 도구 실증 결과보고서

목차

※ 이 보고서는 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 보고서임(RS-2022-II220277), SW공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술 개발 과제

I

보고서 개요

국·내외 SW공급망보안 현황 및
SBOM 도구 실증
결과보고서

Ⅰ 보고서 개요

1. 추진 배경

불과 몇 년전까지만 하더라도 사이버보안 공격은 완제품이나 특정 조직을 직접적으로 겨냥하는 경향이 강했다. 하지만 오늘날 대부분의 디지털 제품이 소프트웨어에 크게 의존하며 작동되어 공급망 공격을 통한 광범위하고 지속적인 공격이 손쉽게 가능해진 현재, 공급망 공격은 모든 소프트웨어 기반 산업의 공통적인 리스크로 인식되고 있다. 이에 따라 소프트웨어 공급망보안은 이미 전 세계 사이버보안의 핵심 축으로 자리 잡은 단계가 되었다.

공급망 공격은 제품의 최종 벤더뿐만 아니라 업데이트 서버, 제품에 포함된 오픈소스 또는 제3자 소프트웨어, 코드 리포지토리, 그리고 공급 벤더 내부 접근 권한 등 제품이 개발·빌드·배포·운영되는 전(全) 단계에서 발생할 수 있는 위협이다. 특히 최근에는 빌드 자동화 환경(CI/CD), 패키지 저장소(NPM, PyPI 등)와 같은 개발 인프라가 주요 표적이 되고 있다.

이러한 측면에서 공급망 공격은 의료기기, 산업제어시스템, 핵심 인프라 등 안전·생명에 직접 연계되는 분야에서 훨씬 더 심각한 영향을 초래할 수 있다. 의료기기의 경우 하나의 장비가 단일 병원 네트워크에 국한되지 않고, 클라우드 기반 서비스나 병원정보시스템(HIS), 원격 진단 시스템 등과 연계되어 작동한다. 따라서 의료기기 내부 소프트웨어에 포함된 오픈소스 라이브러리나 서드파티 모듈에 취약점이 존재할 경우, 단일 장비의 장애를 넘어 환자 안전, 의료 서비스 중단, 데이터 유출로 이어질 수 있다.

특히 2023년 이후 미국 FDA를 비롯한 주요국 규제기관은 의료기기 제조 단계에서부터 소프트웨어 구성요소를 투명하게 관리하도록 요구하고 있다. FDA는 「Cybersecurity in Medical Devices: Quality System Considerations」(2023년 개정) 가이드라인을 통해 의료기기 제조사에게 SBOM (Software Bill of Materials) 제출을 의무화하고 있으며, EU와 국내에서도 디지털 헬스케어 제품의 사이버보안 인증 및 사전 심사 시 SBOM 활용 필요성이 지속적으로 강조되고 있다.

이러한 변화 속에서 소프트웨어 공급망 보안은 더 이상 선택이 아닌 필수적 요구사항으로 자리 잡고 있으며, 산업 전반에서 SBOM을 기반으로 한 투명한 구성요소 관리와 취약점 대응 체계 구축은 핵심 과제로 정착되고 있는 상황이다. 이에 본 실증사업은 의료기기 등 안전·생명과 직결되는 분야를 포함하여, 다양한 산업에서 SBOM의 적용 가능성과 실효성을 검증하고, 이를 통해 국내 기업들이 글로벌 규제 환경에 선제적으로 대응할 수 있는 기반을 마련하기 위해 추진되었다.

2. 그간의 성과 및 4차년도 실증 주요 목표

1, 2차년도에는 정보보호기업들의 공급망 보안 위협 대응 현황 조사와 국내·외 공급망보안 정책 동향, 그리고 SBOM 도구 개발에 앞서 상용 도구들의 실효성과 장단점 등의 비교분석을 진행하였다. 1차년도에는 주요 정보보호기업 22개 社 심층 인터뷰를 통해 SBOM 자동생성 기술 도입의 필요성, SBOM 활성화를 위한 정부 지원방안 및 국내·외 공급망보안 정책 동향을 조사하였으며 5개 상용도구의 비교분석을 통해 향후 SBOM 상용화에 필요한 초기 방향성을 제시하였다. 2차년도에는 유/무료 분석 도구를 활용하여 수요기업에 대한 실증을 진행함으로써 SBOM 도구 개발에 대한 기술적 요구사항과 실제 적용 시 고려해야할 개선점을 구체적으로 도출하였다. 해당 결과를 통해 SBOM 도구 개발에 활용 가능한 구체적 인사이트를 확보하였음에 그 의의가 있다.

3차년도에는 R&D 기반으로 개발된 SBOM 생성도구를 통해 솔루션의 SBOM을 실제로 생성·검증하여, 도구가 NTIA 기준에 부합하며 대부분의 컴포넌트 및 취약점 정보를 정상적으로 식별·분석할 수 있음을 확인하였다. 또한 일부 미탐 컴포넌트와 취약점에 대해서는 기능 고도화를 위한 기술적 보완 필요성이 도출되었으며, 공공·민간 영역에서 SBOM의 신뢰성 제고와 활용 확산을 위한 가이드 및 정책 지원의 필요성도 확인되었다. 특히, 3차년도 실증을 통해 기업 내 오픈소스 구성요소 관리의 중요성이 부각되었고, SBOM 기반의 공급망 보안 관리 체계 구축 가능성이 검증되었다는 점에서 의미가 있다.

4차년도에는 이러한 성과를 토대로 실증 범위를 정보보호 산업에 국한하지 않고 의료기기 등 타 산업 분야로 확대하여, 산업별 특성과 규제 요구사항에 따른 SBOM 활용 모델을 검증하였다. 또한, 업데이트된 SBOM 도구의 산업계 적용 실효성을 검증하고, 실증 참여 기업과 함께 SBOM 생성·활용 전 과정을 분석하여 공급망 보안 관리에 실질적으로 기여할 수 있는 방안을 도출하는 것을 목표로 한다. 이를 통해 SBOM의 산업 전반 적용 가능성을 높이고, 공급망 보안 강화 전략 수립에 필요한 근거자료를 마련할 계획이다.

구 분	세부내용
국내·외 SW공급망보안 동향	- 공급망 공격 사례 및 공격 동향 - 주요국가(미국,EU,일본)별 SW공급망보안 정책 기조 및 변화점 - 의료기기 관련 공급망보안 정책 동향
SBOM	- 공급망보안과 SBOM의 연관성 및 SBOM 기본 개념 - NTIA 기준 SBOM 도구 및 CISA 최소구성요소 - IoTcube 플랫폼 소개
SBOM 도구 실증 결과	- 실증개요 - 기업별 실증 세부 결과 - 요약 및 시사점, Lesson Learned

II

공급망 공격 및 주요국 공급망보안 정책

국·내외 SW공급망보안 현황 및
SBOM 도구 실증
결과보고서

Ⅱ 공급망 공격 및 주요국 공급망보안 정책

1. 공급망 공격 주요 사례 및 동향

1-1. 공급망 공격 주요 사례

① XZ Utils 백도어 사건 (2024)

XZ Utils는 리눅스 배포판에서 기본적으로 사용되는 압축 라이브러리로, Debian, Fedora, Red Hat 등 주요 시스템에 포함된다. 공격자는 GitHub에서 Jia Tan이라는 이름으로 활동하며 수년간 기여를 통해 유지관리 권한을 확보한 뒤 악성 코드를 삽입했다. 해당 사건은 MicroSoft 직원인 Andres Freund에 의해 성능 테스트 중 이상 현상이 발견되며 세상에 알려졌다.

[표 1] XZ Utils 백도어 공격 타임라인

〈공격 타임라인〉
- 2021~2023년 공격자가 장기간 커뮤니티 기여를 통해 신뢰와 권한을 확보
- 2024년 2월, XZ Utils 5.6.0/5.6.1에 악성코드가 포함된 릴리즈 준비
- 2024년 3월 29일, 성능 이상을 통해 백도어가 식별·공개, 관련 릴리즈가 문제로 지정
- 2024년 3월 말 ~ 4월, 주요 배포판의 긴급 차단·롤백, CVE-2024-3094로 등록

XZ Utils 5.6.0/5.6.1은 배포판의 안정 채널로 대규모 확산되기 전 발견, 차단되어 실제 침해 보고는 제한적이었다. 하지만 이미 개발 브랜치와 패키징 파이프라인 일부에 병합되어 배포 직전까지 진행된 만큼, 다수의 리눅스 서버가 잠재 위험에 노출된 것으로 평가되었다. 미국 NVD(National Vulnerability Database)는 해당 이슈를 CVE-2024-3094로 등록하고 최고 위험도 수준으로 경고했으며, Red Hat, Debian 등 주요 벤더가 권고 및 완화 지침을 발표했다.

XZ Utils 사건은 단순히 특정 기업이나 서버 몇 대가 위험에 노출된 수준을 넘어, 리눅스 생태계 전체의 신뢰 기반을 흔든 사건이었다. 오픈소스 프로젝트는 전 세계 수많은 기업과 기관이 의존하는 핵심 인프라로, 단일 라이브러리의 변조가 곧 글로벌 서비스 장애와 대규모 정보 유출로 이어질 수 있음을 보여주었다. 특히 이 사건은 “발견이 늦었다면”이라는 가정만으로도 수십만 대 서버와 수천 개 기업·기관이 동시에 침해될 수 있었음을 드러냈다.[1)]

1) Checkmarx 칼럼, “XZ 유틸즈 백도어 악성코드 발견.. 현재까지 알려진 가장 진보된 공급망 공격”

XZ Utils 사건은 공급망 공격이 단순히 외부에서 악성 코드가 유입되는 형태에 국한되지 않음을 보여준다. 이번 사례처럼 내부 유지관리자의 권한 탈취와 장기적인 사회공학적 침투를 통해 정상적인 업데이트 과정에 악성 코드가 삽입될 수 있으며, 이는 외부 감염보다 더 은밀하고 치명적인 결과를 초래할 수 있다. 따라서 공급망 보안은 외부 위협 차단뿐 아니라 내부 권한 관리, 코드 검증 체계, 장기적 신뢰 관계 악용에 대한 대비까지 포함해야 한다.

② npm 악성 패키지 유포 사건 (2025)

npm은 전 세계 수백만 개발자가 사용하는 오픈소스 패키지 관리 플랫폼으로, 현대 소프트웨어 개발의 핵심 인프라다. 2025년 3월, 북한 연계 해커조직 라자루스(Lazarus Group)가 npm에 악성 패키지를 다수 등록해 개발자 환경을 감염시킨 사건이 보고되었다. 공격은 인기 패키지 이름을 모방하는 타이포스쿼팅과 의존성 체인 악용을 통해 정상 설치 과정에 악성 코드를 삽입하는 방식이었다.

[표 2] npm 악성 패키지 유포 사건 타임라인

〈공격 타임라인〉[2)]

- 2025년 1~2월, 라자루스 그룹이 npm에 악성 패키지 업로드 시작
- 2025년 3월 중순, 악성 패키지 6종이 식별되고, 약 330회 다운로드 정황 확인
- 2025년 3월 말, 보안업계가 대규모 탐지 및 경고 발령, npm 측에서 해당 패키지 삭제 및 보안 공지 배포
- 2025년 4월 이후, 추가 악성 패키지 발견, 총 5600회 이상 다운로드된 사례 보고

피해 규모는 정확히 집계하기 어렵지만, 개발자가 해당 패키지를 포함해 애플리케이션을 빌드하면, 최종 사용자도 자신도 모르게 감염된 소프트웨어를 설치하게 되어 간접 피해가 확산될 수 있다. Windows, macOS, Linux 등 주요 개발 환경을 모두 대상으로 했기 때문에, 실제로 일부 기업에서는 내부 개발 환경이 감염되어 소스코드 유출이 발생했고, 악성 코드가 브라우저와 암호화폐 지갑을 겨냥해 디지털 자산 탈취를 시도한 정황도 보고되었다.

npm은 현대 개발의 공용 인프라이므로 단일 레지스트리에서 발생한 공급망 공격이 글로벌 IT 산업 전체에 확산될 수 있다. 특히 의존성 체인 악용은 “직접 설치하지 않아도 전이 감염”을 야기할 수 있어, 개발자 개인의 피해를 넘어 기업 전체 빌드 파이프라인과 최종 제품까지 영향을 미친다. 국가 지원 해커조직의 개입은 단순 범죄를 넘어선 사이버전 양상을 띠며, 국제적 긴장 요소로 작용했다.

이번 사건은 공급망 공격이 단순한 기술적 문제를 넘어 금전적 이득과 국가 전략적 목적을 동시에 추구할 수 있음을 보여준다. 일부 악성 패키지는 암호화폐 지갑을 겨냥해 거래를 탈취하거나 자격증명을 빼내는 기능을 포함하고 있었는데, 이는 공격자가 직접적인 경제적 이득을 노린

2) 로그프레소 위협분석, “북한 라자루스(Lazarus) 그룹이 배포한 악성 npm 패키지 감염 사례”

정황이다. 동시에 공격 주체가 북한 연계 해커조직 라자루스라는 점은 사건을 단순 범죄가 아닌 국가 기반 사이버전의 일환으로 해석하게 한다. 즉, 공급망 공격은 기업과 개인의 피해를 넘어 국제적 긴장과 안보 문제로 확장될 수 있으며, 이는 글로벌 IT 인프라 전체를 위협하는 요소가 된다. 따라서 공급망 보안은 단순한 기술적 과제가 아니라 자산 보호와 국가 안보를 동시에 지키기 위한 핵심 요소임을 다시금 일깨워주는 사례라 할 수 있다.

③ WannaCry 랜섬웨어 사태

WannaCry는 2017년 5월 전 세계적으로 확산된 랜섬웨어로, 미국 NSA에서 유출된 EternalBlue SMB 취약점을 악용해 Windows 운영체제를 사용하는 시스템을 감염시켰다. 특히 영국의 국민보건서비스(NHS)는 이 공격의 주요 피해 대상이 되었으며, 병원 내에서 사용되던 MRI, CT, 혈액 분석기, 방사선 장비, 정맥주사 펌프 등 다양한 의료기기가 Windows 기반 네트워크에 연결되어 있었기 때문에 직접적인 피해를 입었다.

[표 3] WannaCry 랜섬웨어 공격 타임라인

〈공격 타임라인〉[3]

- 2017년 5월 12일, WannaCry 랜섬웨어가 전 세계적으로 확산되기 시작
- 같은 날 오후, 영국 NHS 산하 병원 다수가 감염되며 의료기기 및 진료 시스템 마비
- MRI, CT, 혈액 분석기, 방사선 장비 등 고가 의료기기가 작동 불능, 수술 일정 취소, 응급실 폐쇄, 환자 이송 지연 등 의료 서비스에 직접적인 차질 발생
- 공격은 EternalBlue SMB 취약점을 통해 네트워크를 타고 확산되었으며, 일부 의료기기 제조사에서 제공한 운영체제 보안 패치가 누락된 것이 주요 원인으로 지목
- 2017년 5월 13~15일, NHS는 일부 병원 시스템 수동 복구, 의료기기 교체 및 네트워크 차단 조치 수행

WannaCry 사태는 단순한 시스템 장애를 넘어, 의료기관의 운영 체계 전반을 마비시키고 환자 안전에 직접적인 위협을 가한 사건으로 평가된다. 영국 NHS는 공식적으로 약 19,000건의 진료가 취소되었으며, 수술 일정 지연, 응급실 폐쇄, 환자 이송 지연 등으로 인해 의료진의 대응 역량이 심각하게 저하되었다.[4]

특히 피해 병원들은 의료기기 작동 중단으로 인해 진료를 수동으로 전환하거나 환자를 타 병원으로 이송해야 했고, 이 과정에서 환자 생명에 위협이 되는 상황도 발생했다. 의료진은 감염된 시스템을 우회하기 위해 종이 문서와 전화 통신에 의존해야 했으며, 이는 의료진의 업무 부담 증가와 진료 오류 가능성을 높였다.

3) https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
4) NHS England, “business continuity management toolkit case study: WannaCry attack”

특히 이 사건은 공급망 보안의 사각지대였던 의료기기 운영체제와 네트워크 연결 구조에 대한 경각심을 불러일으켰다. 감염 경로가 병원 내부 네트워크뿐 아니라, 의료기기 제조사에서 제공한 운영체제 이미지와 보안 패치의 누락을 통해 확산되었다는 점에서, 공급망 내 소프트웨어 구성 요소(SBOM)의 투명성과 검증 체계 부재가 핵심 원인으로 지목되었다.

이후 영국 보건부와 미국 FDA는 의료기기 제조사에게 SBOM 제출 의무화, 보안 설계 내재화, 원격 업데이트 검증 체계 구축 등을 요구하며, 의료기기 사이버보안 가이드라인을 대폭 강화했다. WannaCry는 단일 랜섬웨어 공격으로는 유례없는 규모의 피해를 초래했으며, 의료기기 공급망 보안이 환자 생명과 직결된 핵심 안전 요소임을 전 세계적으로 인식시키는 계기가 되었다.

1-2. 공급망 공격 최신 동향

2025년 현재 공급망 공격은 단순한 악성코드 삽입을 넘어, AI 기반 자동화, 제로데이 취약점 활용, 클라우드·IoT 확산 등 기술적 진화를 통해 정교하고 광범위한 침투 방식으로 진화하고 있다. 공격자는 더 이상 단일 시스템을 노리지 않고, 생태계 전체를 감염시키는 전략적 접근을 취하고 있으며, 탐지 회피와 확산 속도 또한 훨씬 빠르고 은밀해졌다.

[표 4] 공급망 공격 최신 동향

구분	내용
AI 기반 공격 자동화	생성형 AI를 활용해 피싱 이메일, 악성코드 변형, 정상 프로세스 위장등이 자동화되고 있다. 공격자는 탐지 회피를 위해 보안 솔루션의 행동패턴을 학습하고 위협 인텔리전스를 교란하기도 한다.
제로데이 취약점 활용 증가	공급망 내 보안 패치가 지연되는 구조를 노려, 알려지지 않은 취약점(Zero-Day)을 활용한 침투가 증가하고 있다. 특히 의료기기, 산업용 장비, 백업 시스템 등 보안 업데이트가 어려운 장비들이 주요 타깃이 된다.
공격 표면 확대	조직 간 연결성과 자동화가 증가하여 공급망 경계가 모호해지고 있다. SaaS 플랫폼, API 연동, 원격 모니터링 시스템 등이 새로운 진입점으로 떠오르며, 공격자는 이를 통해 다단계 침투와 수평 확산을 시도한다.
플랫폼형 서비스 공격	단일 기업이 아닌 DevOps 도구, 클라우드 백엔드 등 플랫폼형 서비스를 감염시켜 수천~수만개의 고객사에 악성 업데이트를 배포한다. 이로 인해 피해는 산업 전체로 확산되며, 탐지와 대응이 더욱 어려워 진다.

공급망 공격의 타깃은 점점 더 생명·금융·국가 기반 인프라로 집중되고 있으며, 피해는 단순한 시스템 장애를 넘어 운영 중단, 생명 위협, 산업 마비로 이어지고 있다. 특히 보안 수준이 낮거나 업데이트가 어려운 시스템이 집중적으로 공격받고 있으며, 공급망 전체의 신뢰 기반이 흔들리는 구조적 리스크가 부각되고 있다.

[표 5] 주요 타깃 및 피해 경향

구분	내용
의료기기 및 헬스케어 시스템	생명 유지 장비, 환자 모니터링 시스템 등에서 공급망 취약점이 악용되는 사례가 증가하고 있다. 이러한 공격은 기기 자체의 작동 중단과 환자 치료 지연을 초래하며, 의료 현장에 직접적인 혼란을 야기한다.
금융·에너지·정부기관	국가 기반 인프라를 겨냥한 공격이 증가하며, 사이버전 양상으로 확산되고 있다. 공격자는 정찰 → 침투 → 데이터 탈취 → 파괴 또는 협박의 단계적 전략을 구사하며, 피해는 단순한 금전 손실을 넘어 국가 운영 리스크로 확대된다.
SW 개발사 및 배포 플랫폼	개발자 계정 탈취, 패키지 변조, 자동화 배포 경로 감염 등으로 오픈소스 생태계 전체가 공격 표면으로 간주되고 있다. 특히 SBOM이 없는 코드베이스는 추적이 어려워 대응이 지연되며, 다수 사용자에게 피해가 확산된다.

2. 국내·외 공급망보안 정책 및 전략 동향

2-1. 미국

미국은 2021년 공표된 EO 14028(Improving the Nation's Cybersecurity)을 출발점으로 연방정부가 구매·사용하는 소프트웨어의 공급망 보안을 체계적으로 강화하기 시작했다. EO 14028은 안전한 소프트웨어 개발 관행(SSDF) 권고, 연방 조달 시 보안요건 도입, SBOM 도입 촉진을 핵심 지침으로 제시 했으며 이후 NIST·NTIA·CISA 등 여러 기관이 세부 가이드와 기술표준을 발표하도록 했다. 이 행정명령은 '연방 조달'이라는 수단을 통해 시장 전반의 보안 요건 변화를 이끌어 왔다.

[표 6] EO 14028 내 공급망 보안 및 SBOM 관련 주요 내용

〈Sec.4. Enhancing Software Supply Chain Security〉[5]

- SBOM에 대한 최소 구성요소 공표
- 중요 소프트웨어(Critical Software)에 대한 용어 정의 및 목록파악, 관련 보안 지침 발표
- 소프트웨어 공급망 보안을 강화하는 가이드라인 발행
- 소프트웨어 소스코드에 대한 공급업체의 테스트 최소 표준 지침 발표

EO 14028 공표 이후에는 소프트웨어 공급망 보안 정책의 제도적 심화와 지속성 확보가 핵심 동력으로 부상했다. 바이든 행정부는 임기 말 발표한 EO 14144를 통해 EO 14028의 소프트웨어 공급망 보안 요건을 구체화하고 심화했으며 후속 정부인 트럼프 정부에서도 EO 14144를 수정 및 보완하는 행정명령을 발표하여, 소프트웨어 보안 정책이 특정 행정부를 넘어 국가 안보의 핵심 과제로서 지속적인 진화와 확대를 거치고 있음을 명확히 보여주고 있다.[6]

아울러 연방 차원의 권고·프레임을 넘어 조달·국방 영역에서의 실무적 의무화가 빠르게 진행되고 있다. 미 육군은 2024년 8월 발행한 메모를 통해 신규 소프트웨어 계약에 SBOM 제출을 포함하도록 지시하였으며(90일 내 가이드 초안 작성 등 단계적 실행계획 포함)[7], 국방부(DoD)는 'Software Fast Track (SWFT)' 이니셔티브로 소프트웨어 조달·승인 절차를 개편하며 SBOM 제출·자동화된 위험평가·지속적 모니터링을 핵심 요건으로 통합하려는 실무 계획을 발표·시행[8]하고 있어(2025년 중·하반기 관련 조치 가시화), 연방정부의 SBOM 요구는 단순 권고에서 조달 조건·검증 절차로 전환되는 국면에 진입했다.

미 연방정부는 조달요건을 통해 SBOM 제출만을 요구하는 것이 아니라 형식·신뢰성 검증을 점차 요구할 가능성이 크다. 이는 공급업체에게 SBOM 자동화, 식별자 표준 준수, 빌드 무결성 보증

5) The White House, "Executive Order on Improving the Nation's Cybersecurity"
6) Federal Register, "Strengthening and Promoting Innovation in the Nation's Cybersecurity"
The White House, "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144
7) US Army, "Assistant Secretary of the Army(Acquisition, Logistics and Technology) – Sofrware Bill of Materials Policy
8) U,S. Department of War, "Software Fast Track Initiative"

체계 도입을 사실상 '비즈니스 요구'로 전환시키는 결과를 낳는다. 따라서 미국 시장을 염두에 둔 제조사는 SBOM의 기계적 표준화뿐 아니라 SBOM을 취약점 관리, 패치관리 프로세스와 연동하는 운영적 준비가 필요하다.

2-2. 유럽

유럽연합은 CRA(Cyber Resilience Act)를 통해 디지털 요소가 포함된 제품의 全 수명주기 보안에 법적 구속력을 부여하는 접근을 선택했다. CRA는 시장에 유통되는 소프트웨어, 하드웨어 제품에 대해 개발·유지보수·보안 업데이트 의무를 부과하고, 기술문서에 SBOM 또는 동등한 구성요소 투명성 입증 자료를 포함시키는 방향을 규정했다. CRA는 발효시점과 의무적용시점을 갖추고 있어 EU 역내·역외 모두에 직접적 영향력을 행사한다.

[표 7] 사이버복원력법 내 공급망 보안 및 SBOM 관련 주요 내용

〈사이버복원력법(CRA, Cyber Resilience Act)〉[9]

- 제조업체가 수명 주기 전체에 걸쳐 디지털 요소가 포함된 제품의 보안을 개선하도록 보장 (적합성평가를 통해 CE 마크 부착 여부를 결정하는데 이때 SBOM 제출 의무화 계획)
- 일관된 사이버보안 프레임워크를 보장하여 하드웨어 및 소프트웨어 생산자의 규정 준수를 용이하게 함
- CRA의 필수 사이버 보안 요건이나 책임 의무를 준수하지 않을 시, 최대 1,500만 달러 이상의 벌금 부과

유럽연합의 공급망보안 기조가 되는 CRA 법은 24년 12월 발효되었으며 본격적인 의무 적용은 2027년을 전후로 계획되어 있다. 유럽은 CRA라는 전반적 입법 프레임을 운영하는 한편, 제품 안전(무선기기)와 금융 운영 복원력이라는 실무 축에서 구체적이고 즉시 적용가능한 조치를 잇달아 내놓고 있다.

유럽연합은 RED(Radio Equipment Directive)를 통해 무선장비의 사이버보안 필수 요건을 활성화 하였고 조치를 취한 제품만 CE마크를 부착할수 있도록 하여 제조사들이 제품 설계 단계부터 네트워크 위해 방지, 개인정보 및 프라이버시 보호 등의 메커니즘을 증빙하도록 요구한다. 이 조치는 2025년 8월부터 적용되도록 공표되었다.[10]

또한 금융부문에서는 DORA(Digital Operational Resilience Act)가 2025년 1월 적용되면서 금융회사의 ICT 제 3자 리스크 관리, 사고보고, 디지털 복원력 등을 법적 의무로 규정했다. 특히 3rd Party에 대한 EU 차원의 감독 체계를 도입하여 금융 생태계 전반의 공급망 보안 관리 수준을 끌어올리고 있다.[11]

9) European Parliament(2022.9.), "Regulation of the European Parliament and of the council : on horizontal cybersecurity requirements for products with digital elements and amending Regulation(EU) 2019/1020"
10) European Commission, "Radio Equipment Directive"
11) European Insurance and Ocuupational Pensions Authority, "Digital Operational Resilience Act(DORA)"

이처럼 유럽연합은 CRA를 중심으로 RED와 DORA를 실무 축으로 연결하며, 산업 전반에 걸친 공급망 보안의 법제화와 운영 내재화를 병행하고 있다. CRA가 디지털 제품 전반의 '기본보안 의무'를 설정했다면, RED는 이를 개별 제품 수준으로, DORA는 산업(특히 금융) 수준으로 구체화함으로써 공급망 보안을 전 산업군에 확산시키는 구조를 구축하고 있다. 이러한 다층적 접근은 소프트웨어 구성요소의 투명성과 제품 보안의 '책임소재'를 명확히 하여, SBOM을 비롯한 기술적 증빙 체계를 규제의 핵심 수단으로 자리매김시키고 있다.

2-3. 국내

국내의 소프트웨어 공급망 보안정책은 과학기술정보통신부, 국가정보원을 중심으로 국가 차원의 공급망 보안관리체계 확립을 목표로 추진되고 있다. 두 기관과 함께 디지털플랫폼정부위원회는 2024년 'SW 공급망 보안 가이드라인'을 공동 발간하며 정부 차원의 공급망보안 기본 프레임을 제시하였다. 해당 가이드라인은 SBOM을 중심으로 구성요소 투명성 확보, 취약점 패치·관리, 공급자 평가 및 테스트베드 기반 실증을 통한 공공·민간의 보안관리 역량을 제고할 것을 제시한다.

[표 8] SW 공급망 보안 가이드라인 v1.0 주요내용

〈SW 공급망보안 가이드라인 v1.0〉[12]

- 공급망 위기 대응의 필요성과 주요국 정책 동향
- 안전한 SW 개발 환경과 SBOM을 통한 공급망 보안 강화 방안
- SBOM 기반 SW 공급망보안 실증 사례
- 소프트웨어 소스코드에 대한 공급업체의 테스트 최소 표준 지침 발표

기조정책 발표 이후(2024~2025)에는 실무적 제도화가 빠르게 진전되었다. 인력·직무 표준화 측면에서 SW 공급망보안 직무가 국가직무능력표준(NCS)에 반영되어 '계획수립·인프라보안·개발보안자동화·취약점관리·구성명세서관리·운영'의 6개 능력 단위로 세분화되었고, 이는 산업계 인력양성 및 자격체계 정비의 기초가 되고 있다.[13]

또한 검증·평가 체계의 재정비가 진행 중으로서 국가정보원은 SW 공급망 보안 로드맵을 중심으로 정보보호제품 검증체계를 재편하겠다고 밝혔고, 다만 이는 올해 12월까지 SW공급망보안 로드맵이 수립되며 변경될 수 있는 사항이지만, 이는 SBOM 제출과 검증을 포함한 공급망 보안 검증의 효율성과 신뢰도를 높이려는 조치로 해석된다.[14]

산업별·영역별 규범·제도화로서는 예컨대 디지털 의료제품 관련 법·가이드(예: 디지털 의료제품법 등)의 시행[15]으로 의료기기 분야에서는 SBOM·소프트웨어 안전성 증빙 요구가 확대되고 있으며,

12) 국가정보원, 과학기술정보통신부, 디지털플랫폼정부위원회, "SW 공급망 보안 가이드라인 v1.0"
13) 고용노동부 보도자료, "산업변화에 발맞춰 변화하는 2024년 국가직무능력표준(NCS)"
14) https://www.etnews.com/20250103000035?
15) https://www.lawtimes.co.kr/LawFirm-NewsLetter/205209

공공조달 영역에서는 공급망 보안 요건이 조달 심사 항목으로 연계될 가능성이 높아졌다.

한국의 소프트웨어 공급망 보안 정책은 이제 '가이드라인 제시' 단계를 넘어 제도화·운영 내재화·산업 확산이라는 다음 국면으로 진입하고 있다. 특히 각 부처가 분절적으로 추진하던 정책을 통합해, 공급망 전 단계에 걸쳐 보안을 내재화하려는 움직임이 강화되고 있다. 이러한 변화는 공급망 보안을 국가 핵심 인프라 수준의 '지속가능한 관리체계'로 전환하려는 전략적 의지를 반영하며, 나아가 산업 전반의 신뢰성과 자율적 보안역량을 높이는 방향으로 기조가 형성되고 있다. 기업들은 이에 맞춰 자사 개발·운영 전 과정에서 보안 거버넌스를 강화하고, SBOM 중심의 투명한 소프트웨어 관리체계를 확보해야할 것이다.

2-4. 기타 주요국

미국, EU 외의 여타 국가들도 자국 내 소프트웨어 공급망의 복잡성과 오픈소스 의존도 증가에 대응하기 위해, SBOM기반의 투명성 강화와 서드파티 리스크 관리 체계 고도화를 핵심축으로 한 정책을 추진하고 있다. 영국, 일본, 호주, 캐나다, 싱가포르 등도 각국의 산업·기술 환경에 맞춰 공급망보안 가이드라인과 실행규범을 마련하며, 조달·인증·감독 체계와 연계해 실효성을 높이는 단계로 전환하고 있다.

[표 9] 기타 국가 공급망 보안 정책 및 전략 동향

국가	주요내용
영국	영국은 NCSC(국가사이버보안센터)를 중심으로 Software Security Code of Practice 및 관련 실행 가이드를 2024-2025년에 걸쳐 정비·배포하며 소프트웨어 공급망 취약점 예방과 제조·공급자의 보안 책임을 강조하고 있다.[16]
일본	일본은 METI(경제산업성) 주도로 SBOM 도입 가이드를 지속적으로 갱신해 왔으며, 산업별 실증과 표준화 논의를 통해 제조·임베디드·IoT 분야에서 SBOM과 취약점관리의 실무적 적용을 촉진하고 있다.[17] 또한 일본은 METI 주관으로 1차 협력업체 대상 5단계 사이버보안 등급제 도입 및 해외 제조업체 임베디드 SW 검증 강화[18]로 SW공급망보안의 전반적인 강화 절차를 밟고 있다,.
호주	호주의 ASD/ACSC(국가사이버안보기구)는 SBOM 통합 가이드와 공급망 리스크 관리 지침을 발표하며, 소프트웨어 조달·운영에서 SBOM을 어떻게 생성·분석·활용할지에 관한 실무 지침을 제공하고 있다. 특히 공공·국가중요시설을 중심으로 SBOM을 도입·활용함으로써 공급망 가시성 확보와 취약점 대응 속도 개선을 목표로 하고 있다.[19]
캐나다	캐나다 사이버보안센터(Canada Centre for Cyber Security)와 관련 기관들은 국제 공동 가이드(다수 국가와의 공동선언)에 참여하며, SBOM의 채택·분석·공유를 권장하는 지침을 발표했다. 캐나다는 정부 조달·국가 인프라 보호 차원에서 SBOM 활용을 장려하고, 국제 파트너와의 기술·정책 정렬을 통해 공급망 투명성 제고에 주력하고 있다.[20]

16) GOV.UK, "Software Security Code of Practice"
17) METI, "Revised Guide Formulated on Specific Methods for Managing Software Vulnerability Utilizing 'Software Bill of Materials (SBOM),'"
18) 정보통신산업진흥원, "국가별 ICT 시장동향, 일본"
19) Australian Signals Directorate, "New guidance on integrating a Software Bill of Materials(SBOM)"
20) Joint guidance on a shared vision of software bill of materials for cyber security - Canadian Centre for Cyber Security

미국, EU 외의 여타 국가들도 SBOM과 서드파티 리스크 관리를 중심으로 소프트웨어 공급망의 투명성과 대응역량을 강화하는 정책을 추진 중이다. 법제화보다는 표준·가이드·조달 연계 중심의 실무 적용에 초점을 두고 있으며, 국제 정합성과 상호운용성 확보를 통해 글로벌 공급망 보안 생태계 구축으로 나아가고 있다. 이에 따라 기업은 SBOM을 기반으로 한 공급망 보안 관리 체계를 내재화 하여 리스크 관리체계를 구축해야하며 이러한 기반을 갖춘 기업만이 향후 각국의 조달·감독 기준 변화에 능동적으로 대응하고, 글로벌 시장에서의 신뢰성과 경쟁력을 확보할 수 있을 것이다.

3. 의료기기 도입 관련 정책과 SBOM

3-1. 미국

미국은 디지털 헬스·연결형 기기의 증가에 따라 23년 통합세출법(Omnibus)의 3305절(의료기기의 사이버보안 보장)에 524B절(기기의 사이버보안 보장)을 추가하여 FD&C법을 개정하였다. 이에 따라 사이버보안은 의료기기 인허가 시 법적 요구사항으로 격상되었으며, 해당 조항은 제조자가 기기 허가·심사 시 보안 설계, 취약점 관리 계획, 업데이트 체계, SBOM 제출 등을 포함해야 함을 명시했다.

[표 10] FD&C법 524B절(b) 주요 내용

〈FD&C법 524B절(b) 주요 내용〉[21]

- 기기 및 관련 시스템이 사이버공격으로부터 안전하다는 합리적 보증을 제공하기 위한 프로세스 및 절차를 설계, 개발, 유지
- 시판 후 사이버보안 취약성 및 악용을 모니터링, 식별 및 해결하기 위한 계획 제출
  ※ 협동적 취약성 공개 및 관련 절차 포함
- 기기 및 관련 시스템에 대한 시판 후 취약점 업데이트 및 패치 제공
- 상용, 오픈소스 및 기성 소프트웨어 구성요소를 포함한 SBOM 제출
- 기기 및 관련 시스템이 사이버보안에 대한 합리적인 보증을 입증하기 위해 요청되는 추가 사항 제출

이와 함께 FDA는 2023년 Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions 최종 가이던스를 발표하여, 524B절의 법적 요구사항을 구체적인 심사·제출 단계에 반영하였다. 해당 문서는 의료기기 개발·설계 단계에서부터 사이버보안 위험관리를 수행하고, 이를 품질시스템 내 절차로 운영할 것을 권고하고 있다.[22]

특히 이 사이버보안 가이드는 SBOM 내에 NTIA에서 제시한 일반적인 SBOM 최소구성요소와 더불어 ▲SW 컴포넌트 제조업체의 모니터링 및 유지관리를 통해 제공되는 SW 지원 수준 ▲SW 컴포넌트 지원종료(EOS, End-of-Support) 일자, 두가지의 추가요소를 요구하였다.

이처럼 의료기기 도입, 심사 및 허가에 대해 미국은 법제화를 통해 SBOM을 필수적으로 요구하고 있으며, SBOM 뿐만 아니라 취약점 조치 계획 등의 문서를 추가적으로 요구하고 있다. 미국 시장에 진입하려는 의료기기 제조사는 SBOM을 단순한 규제 대응 서류로 볼 것이 아니라 제품의 전 생애주기에 통합된 관리체계로서 SBOM을 활용하여야 한다. 특히, FDA는 SBOM을 실시간 취약점 대응의 '운영 도구'로 인식하고 있어 SBOM 자동생성·검증·패치 프로세스 연계가 이루어져야 승인 및 사후 평가에서 리스크를 최소화 할 수 있을 것이다.

21) FD&C Act, Section 524B, 2022
22) FDA, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, Final Guidance, 2023; FD&C Act §524B, 2022

3-2. EU

EU는 기존 3종의 의료기기 지침(MDD)를 대체하여 의료기기 규제의 근간인 MDR(2017/745)와 IVDR(2017/746)을 발행하였다. 해당 지침들은 의료기기에 대한 필수 안전 요구사항을 규정하고 있으며 고위험군 의료기기 전환은 27년 말, 중위험 및 저위험기기 전환은 28년 말 까지로 시행을 바라보고 있다.

[표 11] MDR 부속서 주요 내용

〈Ⅰ. 일반 안전 및 성능 요구사항 주요 내용〉

- 17.2) 소프트웨어를 통합한 기기 또는 그 자체로 기기인 소프트웨어의 경우, 소프트웨어는 정보보안 검증을 포함한 개발 수명 주기, 위험 관리 원칙을 고려하여 최신 기술에 따라 개발 및 제조되어야 합니다.
- 17.4) 제조업체는 의도한 대로 소프트웨어를 실행하는 데 필요한 하드웨어, IT 네트워크 특성 및 무단 접근방지를 포함한 IT 보안 조치와 관련된 최소 요구사항을 설정해야 합니다.
- 23.4 (ab)) 소프트웨어 또는 그 자체로 기기인 소프트웨어를 포함하여 전자 프로그래밍 기능 시스템을 통합하는 기기의 경우 하드웨어, IT 네트워크 특성 및 무단접근으로부터의 보호를 포함하는 IT 보안 조치와 관련된 최소 요구사항은 의도한 대로 소프트웨어를 실행하는데 필요합니다.

이후 유럽위원회는 의료기기 사이버보안 체계를 구체화하기 위해 “MDCG 2019-16 Rev.1 Guidance on Cybersecurity for Medical Devices”를 발표하였다. 해당 가이드라인은 MDR과 IVDR에서 규정한 내용을 기술적으로 해석한 문서로, 의료기기 제조자가 개발부터 사용·폐기까지의 전 생애주기에서 사이버보안 위험을 관리해야 함을 명시한다.

또한 MDCG-2019-16 Rev.1은 SBOM을 직접적인 제출 의무 항목으로 규정하고 있지는 않지만 기기 보안정보의 예시로 SBOM을 명시하였다. 구체적으로 제4.2절에서는 특정 보안정보의 별도 공유와 SBOM을 명시함으로서 제조자가 SBOM을 통해 의료기기 사용자에게 기기 내 SW 구성요소 및 보안지원 상태를 투명하게 공개해야 함을 의미한다.[23)]

이에 따라 EU 내 의료기기 제조사는 SBOM을 단순한 기술문서 보조자료가 아닌, 공급망 투명성과 취약점 관리의 핵심 도구로 인식하고 활용할 필요가 있다. MDR·MDCG 가이드라인은 의료기기 안전성을 ‘사이버보안 확보’와 동일 선상에서 평가하므로, 제조사는 SBOM을 통해 기기 구성요소의 보안지원 상태 등을 명확히 관리하고 취약점 발생 시 신속히 영향 범위를 파악하여 대응하여야 한다. 이뿐만 아니라 CRA법에 디지털 의료기기가 포함됨에 따라 CRA 발효 시, SBOM의 기계판독 형식 제출이 기술문서 요건에 포함될 가능성이 높으므로, SBOM을 내부 품질관리와 위험관리 파일에 통합하고 이를 의료기관·감독기관과 안전하게 공유할 수 있는 절차를 조기에 구축하는 것이 가장 중요하다.

23) 스마트의료보안포럼 발표자료, “의료기기 SBOM 동향, 방지호 박사, 2024.05”

3-3. 국내

국내에서는 2024년 제정된 디지털의료제품법을 통해 소프트웨어 기반 의료기기의 안전관리 및 사이버보안 체계가 법제화되었다. 해당 법은 소프트웨어, AI 의료기기를 포함한 디지털 의료제품에 대한 인허가 절차, 사후관리, 보안 유지 의무를 명문화하고 있다. 해당 법은 25년 1월부터 시행되고 있으며 한국 의료기기안전정보원(NIDS)가 인증 등의 대행 업무를 수행하고 있다.[24)]

디지털의료기기 전자적 침해행위 보안지침은 디지털의료제품법 제14조를 근거로 제정된 세부 운영기준으로, 의료기기가 사이버공격·악성코드 감염 등 전자적 침해행위로부터 안전하게 보호되도록 하기 위한 절차를 규정하고 있다. 이 지침은 디지털의료기기의 설계·개발 단계부터 운영·유지보수·폐기 단계까지 보안조치를 체계적으로 관리하도록 요구하며, 물리적·기술적 보호조치, 침해사고 대응, 취약점 신고 및 패치관리 절차를 포함한다.

[표 12] 디지털의료기기 전자적 침해행위 보안 지침 주요 내용

〈디지털의료기기 전자적 침해행위 보안 지침 주요 내용〉[25)]

▸ 제16조 (소프트웨어 구성요소 명세서 관리 활동)

(1) 디지털의료기기제조업자 등은 디지털의료기기 내 취약점 발견, 보안 및 침해사고 및 이를 해결하기 위한 활동을 수행하는데 **소프트웨어 구성요소 명세서**를 활용할 수 있다.
(2) 의료서비스제공자는 디지털의료기기에 대해 디지털의료기기제조업자 등이 작성한 소프트웨어 구성요소 명세서를 구매 및 설치 이전에 확인하는 것을 고려할 수 있다.
(3) 소프트웨어 구성요소 명세서 정보는 보호되어야 하며 소프트웨어 구성요소 명세서의 생성, 저장, 송수신 등의 과정에서 데이터 보안을 고려할 수 있다.

3-4. 시사점

미국, EU, 한국의 정책 동향을 종합하면, 의료기기 산업에서 사이버보안이 제품 안전성 평가의 핵심 요소로 제도화되고 있다는 공통점이 드러난다. 이는 의료기기가 단일 제품이 아니라 다양한 SW 구성요소와 외부 공급망이 얽힌 복합 시스템이라는 점에서, 보안위험의 식별과 책임소재를 명확히 하기 위한 필수조건으로 해석된다. 결과적으로 SBOM은 규제 이행뿐 아니라, 의료기기 신뢰성과 시장 접근성을 판단하는 핵심 자료로 기능하게 된다.

현재로서는 미국을 제외하고는 의료기기 허가·승인 관련하여 SBOM을 의무화하고 있는 규제는 명문화되지 않았으나, 보안 규제가 기술 중심에서 운영·관리 중심으로 전환되고 있다는 점도 중요한 시사점이다. 이에 따라 의료기기 제조사는 SBOM을 중심으로 한 '지속적 보안관리 체계(Continuous Cybersecurity Management)'를 구축해야 하며, 이를 품질경영(QMS)과 위험관리(RMF) 전반에 통합해야 한다. 이러한 접근은 단순한 규제 대응을 넘어, 글로벌 시장에서 신뢰받는 의료기기 공급망 경쟁력을 확보하는 핵심 수단이 될 것이다.

24) 법률 제20331호, "디지털의료제품법"
25) 식품의약품안전처, "디지털의료기기 전자적 침해행위 보안지침"

III

SBOM 및
SBOM 실증 도구 IoTcube

국·내외 SW공급망보안 현황 및
SBOM 도구 실증
결과보고서

Ⅲ SBOM 및 SBOM 실증 도구 IoTcube

1. SBOM의 기본 개념

SBOM(Software Bill of Materials)은 소프트웨어의 구성요소와 의존관계를 체계적으로 식별하고 관리하기 위한 핵심 관리 명세서로, 제품 내부의 소프트웨어 자산을 '투명하게 가시화'하기 위한 기반 자료이다. 이는 제조업에서 부품의 원산지와 조합을 추적하기 위해 사용되는 자재명세서(Bill of Materials, BOM) 개념을 소프트웨어 분야로 확장한 것으로, 각 구성요소의 이름, 버전, 공급자, 라이선스, 종속관계 등 기본 속성을 목록화하여 소프트웨어의 구조적 투명성을 확보한다.

오늘날 소프트웨어는 다수의 오픈소스, 상용, 서드파티 구성요소가 복합적으로 결합된 형태로 개발되고 있으며, 단일 코드베이스만으로는 전체 보안위험을 파악하기 어렵다. SBOM은 이러한 복잡한 공급망 구조 속에서 어떤 구성요소가, 누구에 의해, 어떤 버전으로 사용되고 있는가를 명확히 함으로써 취약점 식별과 위험평가의 기준점을 제공한다.[26)]

최근에는 SBOM이 개발자나 보안담당자뿐만 아니라, 구매자·감독기관·인증기관 등 다양한 이해관계자 간의 신뢰 기반 데이터 교환 도구로 활용되고 있다. 공급자는 SBOM을 통해 제품의 보안 지원 상태(EOS 등)를 명확히 제시하고, 이용자는 이를 기반으로 취약점 대응 계획을 수립하거나 조달 리스크를 평가한다. 즉, SBOM은 더 이상 보안 문서의 '부속 항목'이 아니라, 소프트웨어 공급망의 신뢰성과 지속가능성을 증명하는 운영 문서로 인식되고 있다.

2. 표준형식과 최소구성요소

현대 소프트웨어 공급망은 다층적 종속성과 자동화된 배포 과정으로 인해 구성요소의 출처·변경 이력을 명확히 파악하기 어렵다. 이에 따라 소프트웨어 명세의 표준화된 표현방식이 보안관리와 규제 대응의 핵심 수단으로 부상하고 있으며, 국제 사회는 SBOM 형식 표준의 상호운용성과 일관성을 확보하기 위한 논의를 지속하고 있다.

NTIA의 Software Transparency Working Group은 주요 SBOM 형식으로 SPDX, CycloneDX를 제시하며, 이들이 각각 다른 생태계에서 활용되고 있음을 확인하였다. SPDX는 라이선스 관리와 규제 대응 중심의 오픈소스 추적 표준으로, 2021년 ISO/IEC 5962로 공식 채택되어 법적 신뢰성이 확보되었다. 반면 CycloneDX는 보안·위협정보 교환 및 취약점 관리에 최적화된 경량 형식으로,

26) CISA, "Software Supply Chain Security Update, 2025"

OWASP 커뮤니티를 중심으로 빠르게 확산되고 있다.[27]

[표 13] SBOM 표준 형식

SPDX (Software Package Data Exchange)[28]	- LINUX 재단에서 운영하는 프로젝트로서 출처, 라이선스, 보안 및 기타 관련 정보를 포함한 SBOM 정보를 전달하기 위한 개방형 표준 - ISO/IEC 5962:2021으로 채택된 국제 표준 - SPDX 프로젝트의 구성 • SPDX 사양 자체 • SPDX 라이선스 목록 • SPDX 문서 및 SPDX 라이선스 목록 작업을 위한 SPDX 도구 및 라이브러리
CycloneDX[29]	- OWASP(Open Web Application Security Project) 커뮤니티에서 개발된 보안과 신뢰성에 중점을 둔 경량 SBOM 표준 - Ecma International에 의해 표준화되었으며 글로벌 보안 커뮤니티가 지원 - 패키지 URL, CPE, SWID, SPDX 라이선스 ID 및 표현과 같은 기존사양 포함 - 소프트웨어 구성 요소들을 XML, JSON, Protobuf 등 다양한 형식으로 표현 컴포넌트 이름, 버전, 설명, 라이선스, 제작자, 보안취약점 정보

NTIA는 2021년 미국 행정명령 EO 14028에 따라 “The Minimum Elements for a Software Bill of Materials” 보고서를 발행하였다. 이 문서는 SBOM 내 포함되어야 할 7개의 기본 요소를 제시하며, 해당 구성요소가 기술적 형식과 관계없이 상호운용성과 일관성을 보장하기 위해 SBOM에서 공통적으로 유지되어야 할 기본 속성 집합임을 명확히 하였다.[30]

[표 14] NTIA SBOM 최소 구성 요소

Data Field	Description
공급자 이름(Supplier Name)	- 컴포넌트를 생성, 정의, 식별하는 개인 또는 조직의 이름 (작성자, 제조업체)
컴포넌트 이름 (Component Name)	- 원래 공급자, 제조업체가 정의한 소프트웨어 요소에 할당된 이름 소프트웨어에 여러 이름과 별칭이 있는 경우 내용도 함께 표시
컴포넌트 버전 (Version of the Component)	- 이전 식별번호와 구분할 수 있도록 소프트웨어 제조업체가 지정한 식별자
기타 고유 식별자 (Other Unique Identifiers)	- 컴포넌트를 식별하거나 DB에서 구성요소를 찾기위한 조회키로 사용되는 컴포넌트 이름 및 버전 이외의 추가 식별자
의존성 (Dependency Relationship)	- 컴포넌트가 상위 컴포넌트에 종속되어 있다는 관계에 대한 설명
SBOM 작성자 (Author of SBOM Data)	- SBOM 데이터를 생성한 개인 또는 조직의 이름
타임스탬프(Timestamp)	- SBOM 데이터가 생성된 날짜와 시간에 대한 기록

27) NTIA, “Survey of Existing SBOM Formats and Standards, 2021”,
28) The Linux Foundation Projects “About SPDX”
29) OWASP “CycloneDX One Pager”
30) NTIA, Department of Commerce “The Minimum Elements For a Software Bill of Materials” (2021.07)

CISA는 NTIA가 제시한 2021년 SBOM 최소구성요소를 토대로 4년 만에 해당 권고를 현대화하는 초안을 공개했다. 그 차이는 단순한 항목 나열을 넘어 운영적 활용성과 무결성 검증을 강화한 데 있다. 기존 명시되었던 Component Name, Component Version 등의 업데이트와 더불어 License, Tool name 등도 명시하도록 하였다.[31]

[표 15] CISA SBOM 최소구성요소와 NTIA 최소구성요소 변경점 비교

구분	변경 CISA 최소구성요소
공급자 이름 (Software Producer)	- 기존 Supplier Name에서 Software Producer로 용어 변경 - 명확한 표시가 없는 경우 구성요소 출처 알 수 없음 표기
컴포넌트 이름 (Component Name)	- 사람이 읽을 수 있는 방식으로 식별, 식별자 필드와 구분
컴포넌트 버전 (Component Version)	- 버전 미제공 시 파일생성날짜로 대체
기타 고유 식별자 (Software Identifiers)	- 기계처리 가능하고 고유한 식별자, CPE, purl, UUID 등 - 동일형식 식별자 또는 다른 형식의 식별자가 여러개 있는 경우 모두 명시
의존성 (Dependency Relationship)	- 포함관계는 종속성 그래프를 사용하여 표기 - 포함관계 외에도 파생되거나 다른 소프트웨어의 하위 구성요소임을 반영
SBOM 작성자 (SBOM Author)	- 소프트웨어 생산자 필드와의 구분 (동일할 수는 있음)
타임스탬프 (Timestamp)	- 데이터를 수동 또는 자동으로 마지막으로 변경한 시점
컴포넌트 해시 (Component Hash)	- (신규) 소프트웨어 구성요소의 해시를 가져옴으로서 생성된 암호화 값
라이선스 (License)	- (신규) 소프트웨어 구성요소를 사용할 수 있음을 나타내는 라이선스
도구 이름 (Tool Name)	- (신규) SBOM을 생성하는데 사용된 도구 이름
생성 컨텍스트 (Generation Context)	- (신규) SBOM 생성 당시의 상대적 소프트웨어 수명주기와 데이터 ex.) 빌드 전, 빌드 중, 빌드 후

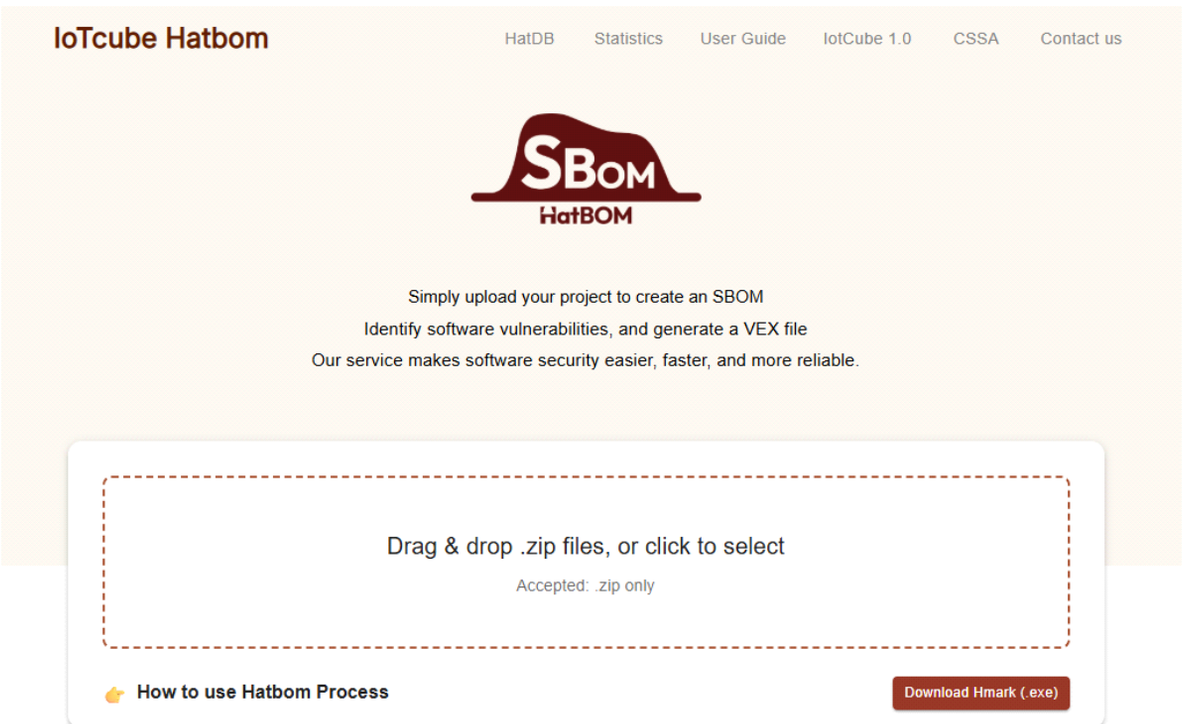
CISA의 2025년 SBOM 최소구성요소 개정은 SBOM을 단순한 구성정보 목록이 아닌 검증 가능한 보안 데이터 자산으로 취급하였다는 점에서 의미가 있다. 해시, 라이선스 등 신뢰성 중심의 항목을 추가하고 기존 항목을 변경으로써 SBOM의 데이터 무결성·활용 가능성·자동화 연계성이 강화되었으며, 이는 단순한 규제 준수를 넘어 SBOM이 실제 보안운영과 취약점 대응의 실질적 도구로 기능하도록 하는 방향으로 진화했음을 보여준다. 즉, 이번 개정은 SBOM을 형식적 표준에서 운영 품질 기준으로 전환하는 변화를 촉발할 수도 있을 것이다.

31) CISA, “2025 Minimum Elements for a Software Bill of Materials (SBOM)”

3. IoTcube 2.0

고려대학교 소프트웨어보안연구소(CSSA, 소장 이희조 교수)는 과학기술정보통신부 및 정보통신기획평가원이 지원하는 'SW공급망보안을 위한 SBOM 자동생성 및 무결성 검증기술 개발' 정부과제에 참여하여 SBOM 자동생성도구 및 취약점 분석 도구인 IoTcube를 개발하였다.

해당 도구는 1.0 버전으로 릴리즈 되어 보안 전문가가 아닌 누구라도 소스파일을 '드래그 앤 드롭' 형태로 보안취약점을 식별하고 소프트웨어 보안을 관리할 수 있도록 제공하였다. 해당 버전을 통해 IoTcube는 실제 정보보호산업계 솔루션의 실증을 거치면서 개선점을 도출, 기능 개선 후 2025년 HatBOM이라는 이름으로 2.0버전 업데이트 되었다.



[그림 1] IoTcube 플랫폼

HatBOM은 SBOM을 통한 취약점 및 컴포넌트 관리를 통한 SW공급망의 투명성 확보를 목표로 한다. 기존 1.0 버전에서 SBOM 생성도구와 취약점 관리 도구를 별도로 사용하여 기능을 제공했던 것과 달리 소프트웨어 파일을 드래그 앤 드롭 하는 형태로 분석 기능을 이용할 수 있다. 기능은 SBOM 생성, 취약점 탐지와 더불어 VEX 문서 생성이 추가되어 탐지된 취약점이 실제로 소프트웨어에 Exploit 되는지 확인 할 수 있다.

〈VEX (Vulnerability Exploitability eXchange〉

- 특정 제품에 포함된 컴포넌트의 취약성이 제품에 영향을 미치는지, 영향이 있다면 수정책의 유무에 대한 설명 또는 사용자에게 추가정보를 제공하는 것
- 취약성 status로서 Not Affected / Affected / Fixed / Under investigation으로 나누어 설명

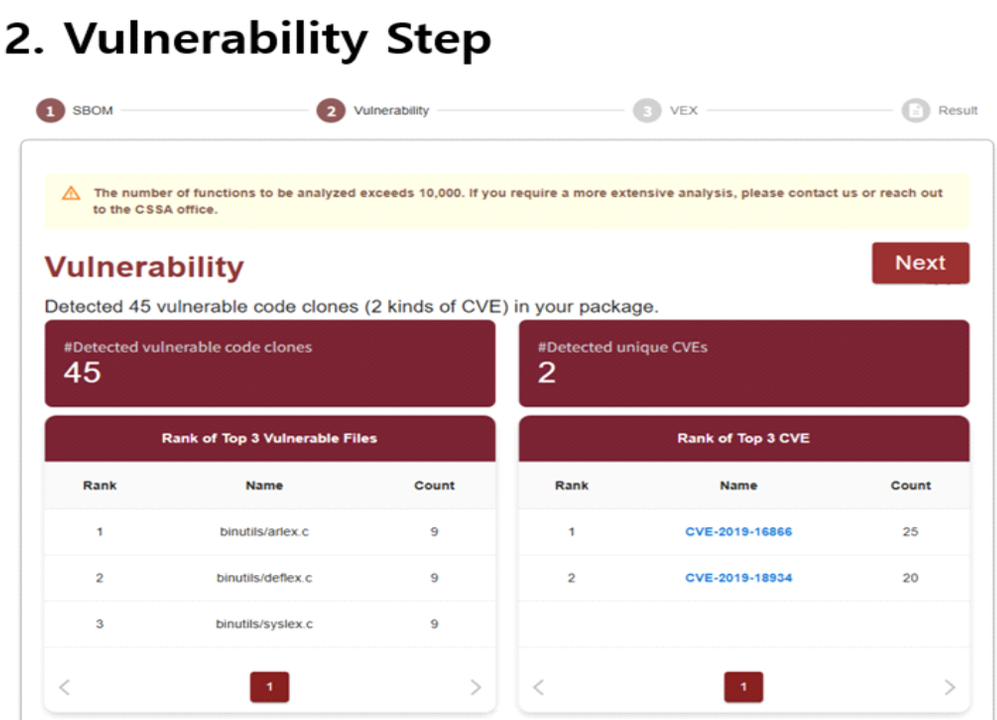
3-1. SBOM 생성

[그림 2] SBOM 생성

프로젝트 코드가 있는 프로젝트 파일을 .zip 파일로 압축해서 드래그 앤 드롭 형태로 업로드하면 소프트웨어 파일 내의 OSS를 탐지하고 그에 대한 SBOM 문서를 생성하여준다. SBOM 문서는 트리 형태로 각 OSS의 의존성 또한 파악 할 수 있다.

※ 소프트웨어 프라이버시를 고려하여 해싱프로그램 Hmark를 이용하여 해시화 후 업로드하는 기능도 제공하고 있다.
※ 현재 버전에서는 입력으로 소스코드만 지원하며, 점차 바이너리, 도커이미지까지 확대될 예정.
현재 지원가능한 언어 : C/C++, Java, Python, GO, PHP (추후 추가 예정)

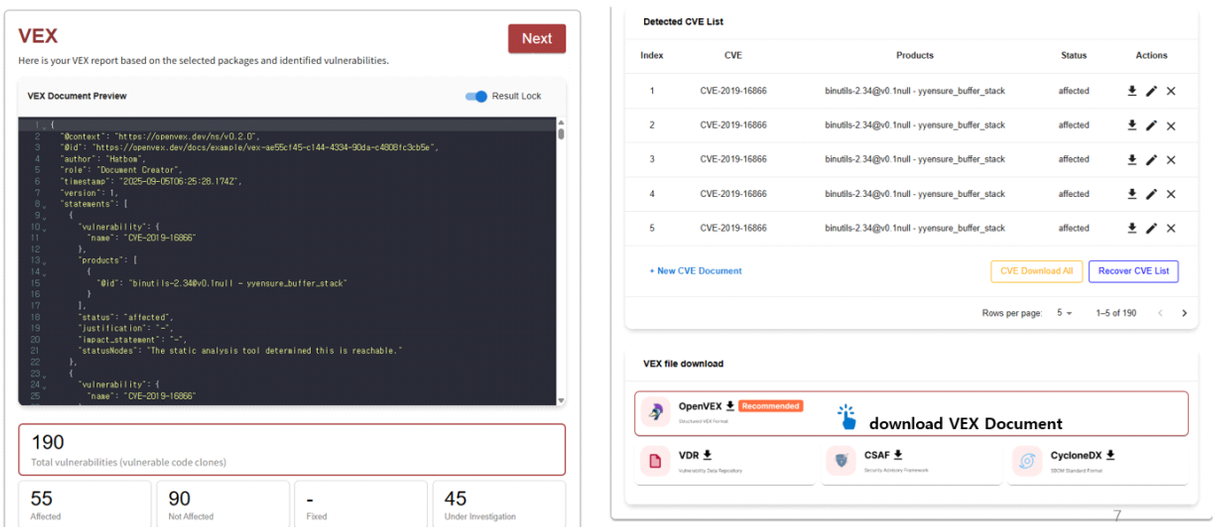
3-2. 취약점 탐지



[그림 3] 취약점 탐지

SBOM 생성 후 Next 버튼 클릭을 통해 소프트웨어에 내재된 취약점을 탐지 할 수 있다. build 된 프로젝트이면 정적분석이 자동으로 수행되어 발견된 취약점과 CVE 그리고 가장 많이 발견된 취약점과 CVE를 확인 할 수 있다.

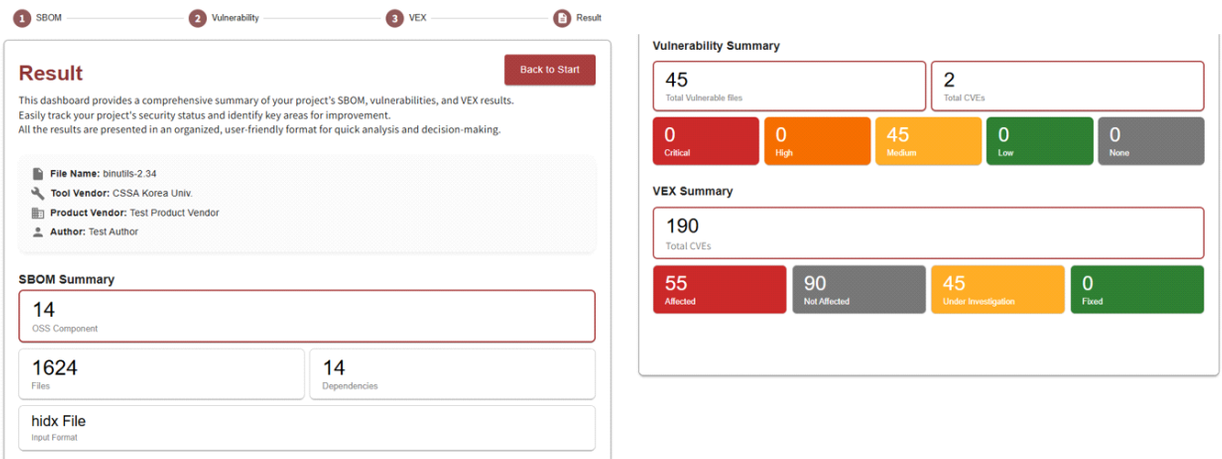
3-3. VEX 생성



[그림 4] VEX 생성

취약점 생성과정에서 선택한 CVE들의 유효성을 직접 개발자들이 분석 및 검증할 수 있도록 하였다. 선택된 CVE들에 대한 Status가 기입되어 출력되며 Status가 변경될 필요가 있다고 판단되었을 때는 해당 CVE에 대한 수정 아이콘을 클릭한 후 4가지(Not Affected/Affected/Fixed/Under Investigation) Status List 중에서 선택한 후 수정할 수 있는 기능을 제공하고 있다. 최종적으로 모든 CVE Status 값이 조정된 후에는 VEX 문서를 다운로드할 수 있다. (OpenVEX 포맷 지원)

3-4. Result Step



[그림 5] Result Step

지금까지 분석한 내용들을 요약하여 보여주는 최종 Result Step이다.

Ⅳ

SBOM 도구 실증 결과

국·내외 SW공급망보안 현황 및 SBOM 도구 실증 결과보고서

Ⅳ SBOM 도구 실증 결과

1. 실증 개요

본 연구를 통해 개발된 도구를 통해 기업 솔루션의 SBOM을 추출, 취약점을 비교하여 개발한 도구의 실효성을 검증하고 추출된 SBOM과 취약점, VEX를 통해 기업별 SW 공급망보안 관리 체계를 구축하고 의료기기 제조업체의 경우 의료기기 인허가 계획을 수립하는데 의의를 두었으며, 기업별 실증 세부 결과는 다음과 같다.

2. 기업별 실증 세부 결과

2-1. A사 실증 세부 결과 (정보보호기업)

기업별 도입 배경

참여배경

최근 보안취약점 관리 및 소프트웨어 공급망 투명성 강화의 중요성이 대두됨에 따라 SBOM 기반의 소프트웨어 관리체계 구축의 필요성을 인식 또한 최근 OSS 사용 비율이 증가함에 따라 구성요소의 라이선스 및 취약점 관리 공백이 발생하고 있어 이를 체계적으로 식별하고 관리하기 위한 방안으로 SBOM 기술을 도입하고자 실증사업에 참여

실증대상 및 환경

C언어, PHP언어로 이루어진 보안 웹 게이트웨이(SWG) 제품을 대상으로 Linux 기반에서 개발된 C언어 소스를 Windows PC환경을 통해 IoTcube 웹 플랫폼에 업로드

실증목적

IoTcube 플랫폼을 활용해 SBOM 생성·검증 절차가 실제 운영환경에서 적용가능한지 실효성을 확인하고 분석 결과가 SBOM 요구사항과 부합하는지 확인. 또한 SBOM 기반의 취약점 연계 분석 가능성을 확인하고 해시화된 코드 기반의 SBOM 생성·관리와 실제 활용성을 검증

기대성과

SBOM 구성요소 식별을 자동화하여 관리 효율성을 향상시키고 분석 정보를 SBOM에 매핑하여 취약점 정보와 연계함으로써 개발 단계에서 공급망 취약점 조기 제거 기반 마련. 또한 Hmark를 사용해 코드를 해시화하여 비식별화된 형태의 분석이 가능함을 검증함으로서 외부 플랫폼 사용 시 소스 유출 위험을 최소화

실증 주요 결과

SBOM 생성 단계

Result Details

File Name	보안상 생략
Files	2681
Dependencies	84
Input Format	ZIP File
Output Format	CycloneDX format SBoM

- 총 2,681개의 파일 중 84개의 컴포넌트, 의존성 발견
- 사전 수동으로 파악한 OSS 리스트와 비교하여 검증 데이터로 활용한 결과 주요 라이브러리의 일부는 정확하게 버전까지 일치하여 탐지됨을 확인
- C언어 기반 라이브러리 뿐만 아니라 광범위한 생태계의 OSS까지 포함하여 탐지
- 일부 라이브러리는 버전이 다르거나 오탐 등의 현상이 발생하였으나 해당 현상은 탐지된 버전과 기존 버전의 코드가 같으므로 동일 해시값을 가지거나 3rd party OSS를 가진 OSS가 상위 OSS의 이름으로 탐지되는 현상이 발생한 것으로 추정

취약점 분석 결과

Detected 102 vulnerable code clones (30 kinds of CVE) in your package.

#Detected vulnerable code clones
102

#Detected unique CVEs
30

Rank of Top 3 Vulnerable Files

Rank	Name	Count
1	보안상 생략	6
2		6
3		6

1

Rank of Top 3 CVE

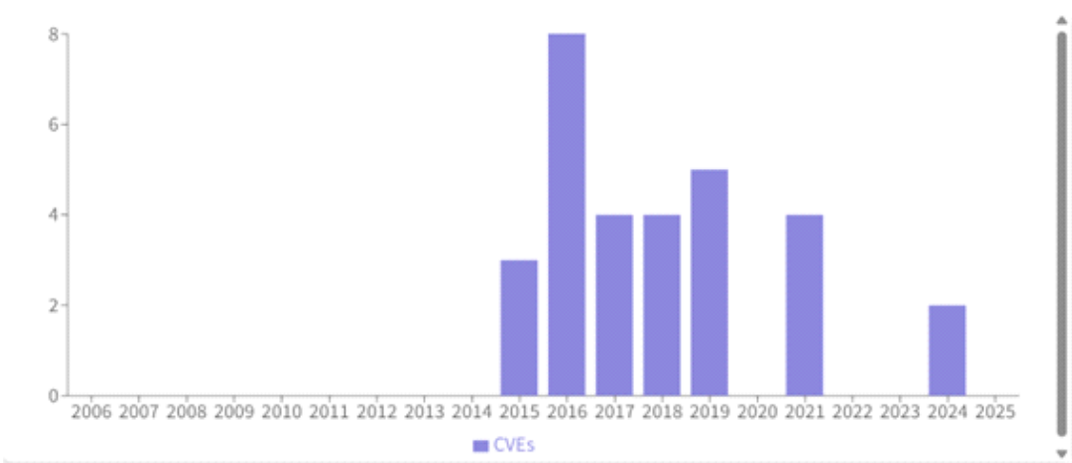
Rank	Name	Count
1	보안상 생략	45
2		12
3		9

1

VUDDY Vulnerable Files

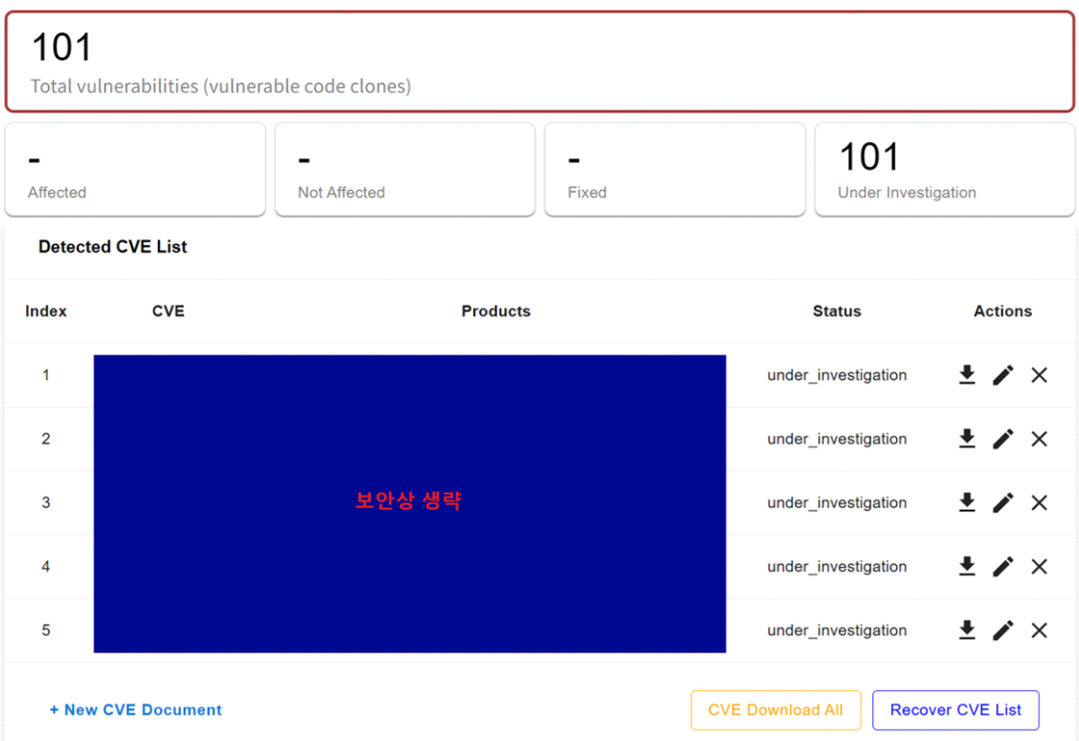
id	File Path	CVE	CVSS ▲	KEV ⓘ	☐
1	보안상 생략		Medium	None	☐
2			Medium	None	☐
3			Medium	None	☐
4			Medium	None	☐
5			Medium	None	☐
6			Medium	None	☐
7			Medium	None	☐
8			Medium	None	☐
9			Medium	None	☐
10			Medium	None	☐

Hide Charts



- 총 30종류의 101개 취약점 코드 클론 발견
- 취약점 모두 CVSS 레벨 Medium으로 표시
- 연도별 CVE 발견 건수를 시각화하여 제공하나 연도별 건수만으로는 위험도, 영향도를 직접적으로 판단할 수 있는 시각화 자료가 필요
- 일부 시각화 자료나 결과 상태에서 UI 오류로 인해 수치가 다르게 출력되는 경우에 대한 UI 개선 필요

VEX 문서 생성 결과



- 총 101개의 취약점 모두 Under-Investigation 상태로 분류
- 취약점 가능성은 존재하나, 실제 위험성을 단정할 수 없고 검토가 필요한 상태

취약점 조치 및 공급망보안 관리 계획

패치정보 확인 및 취약점 조치 계획

SBOM 및 VEX 분석 과정에서 도출된 취약점 목록을 기반으로 KISA 보안공유센터, NIST NVD(National Vulnerability Database), OSV(Open Source Vulnerabilities) 등 외부 VDB와 각 OSS 공식 저장소 등을 활용하여 패치 여부 및 대응방안 주기 점검 계획

- 취약점 매칭 및 심각도 확인
  SBOM 기반 VDB 조회, CVSS 점수 기반 심각도 분류, VEX Status 기반 우선순위 결정
- 패치 버전 또는 안전 버전 확인
  NVD 또는 해당 OSS 공식 저장소에서 취약점 해결 버전(Fixed Version) 확인
  패치 미존재 경우, PoC·공격 코드 공개 여부 및 Exploit 가능성 여부 조사
- 조치 계획 수립
  VEX Status 기반하여 즉시 업데이트 및 보안 조치 또는 모니터링 수행

SBOM 및 VEX 문서를 활용한 SW 공급망보안 관리 계획 수립

추출된 SBOM과 VEX 문서를 기반으로 SW 공급망 보안 관리 체계를 다음과 같이 수립하고 운영할 예정

- SBOM 기반 구성요소 투명성 확보
  개발·배포되는 모든 SW에 대해 SBOM을 주기적으로 생성하여 OSS, 의존성 등 체계적으로 관리 신규 모듈, 업데이트 모듈 포함 시 자동 SBOM 갱신 및 외부 SW 도입 시 SBOM 제출 요구
- VEX 문서를 활용한 실제 위험성 판단
  SBOM에 포함된 취약점 중 실제 실행 경로, 바이너리 포함여부 판단 시 추후 VEX Status 활용 자동 탐지된 취약점 중 Exploit 된 취약점만 선별하여 대응 우선순위를 조정
- 조직 내 공급망 보안 프로세스 정착
  OSS 도입 시 사전 검토 절차(라이선스, 취약점, 버전 안전성)를 문서화하여 관리
  취약점 대응 이력 및 패치 적용 내역을 SBOM 버전으로 관리
  공급망 파트너, 외부개발사에 SBOM 및 VEX 제출 요구하여 외부소스 투명성 확보
- 릴리즈 승인 절차 강화
  SW 릴리즈 시 SBOM과 VEX 제출을 의무화, 내부 보안 담당자 승인 후 배포
  Affected 상태 취약점은 조치 완료 여부 검증을 거칠 예정
  Under-Investigation 항목은 추가 분석 결과를 첨부하여 승인 판단

- 운영 환경의 지속적 보안 상태 관리
  운영 중에도 SBOM과 VEX를 활용하여 지속적으로 취약점 판단 및 모니터링
  정기보안 점검 시 SBOM을 기준으로 구성요소 신뢰성 검증

실증결과를 통한 시사점

Lesson-Learned

본 실증을 통해 SBOM, VEX가 단순한 문서 생성 도구가 아닌 SW 보안의 핵심 자산이자 지속가능한 공급망 관리체계로 발전시키기 위한 발판임을 확인

- SBOM 자동화 도구의 필요성 절감
  기존에는 OSS 리스트를 수동으로 도출하는 방식을 사용하였으나 SBOM 자동화 생성 도구와 비교하였을 시 누락, 추가 식별, 종속 라이브러리 계층 구조 등에서 차이가 존재함을 발견, 의존성 트리 기반의 시각적 구성요소 식별 절차가 필요함을 확인
- VEX 문서를 통한 취약점 우선순위 결정의 중요성 체감
  식별된 취약점은 101건이나 실제 서비스 맥락에서 Exploit 가능한 취약점은 극히 제한적인 것으로 판단, 기존에는 CVSS 점수만을 기준으로 패치 우선순위를 판단하였으나 실제 위험성이 낮은 항목을 분류하고 패치 대상을 좁혀 리소스의 효율적 사용에 대한 가능성 확인
- SBOM과 VEX를 공급망 보안 프로세스 핵심요소로서의 활용
  SBOM, VEX 문서를 통해 자체 개발 소스 뿐 아니라 외부 라이브러리 보안 추적에도 필수정보로 활용할 수 있었으며 이를 통해 보안점검, 인증 심사, 고객 대상 품질 보증(BotA)에도 활용할 수 있을 것으로 기대
- 사내 개발 프로세스 내 SBOM 및 VEX 내재화하기 위한 체계적 관리 필요성
  개발 초기 단계에서 OSS 선정 → SBOM 자동 생성 → VEX 기반 취약점 점검 → 배포 시점에 최신 SBOM/VEX 문서 제출의 형태로 개발 프로세스에 통합하여 공급망 리스크 관리를 지속적으로 수행

실증사업 간 애로사항 및 개선 사항

- 분석 대상 소스와 SBOM 결과의 불일치 문제
  직접 도출한 OSS 리스트와 SBOM 자동 생성 결과가 상이하여 빌드 기반의 SBOM 생성 방식 지원과 정적, 동적 분석의 병행이 필요함
- 일부 취약점의 실제 영향도 판단 어려움
  VEX 문서를 통해 Exploit 가능 여부를 확인할 수 있었으나 경로 기반의 영향 분석, 환경 의존성 고려 등의 정보가 충분하지 않아 구체적인 근거를 제공할 수 있으면 좋을 듯함

- 플랫폼 사용 시 업로드 과정의 제약
  업로드 가능한 파일 크기, 비표준 빌드환경에서 생성되는 파일 처리, 해시화 후 파일 구조 변경 등의 제약 사항이 존재, API 기반 자동 업로드 기능을 추후 제공하거나 CLI 제공, 대용량 소스 지원 등이 필요할 것으로 사료
- 이해 및 활용을 돕는 추가 가이드의 제공
  실행 중 에러의 발생 원인이나 사용 가이드 등을 안내해주는 Notice GUI의 제공과 비전문가도 쉽게 이해할 수 있도록 용어에 대한 설명이 추가된다면 좋을 것

SBOM 및 VEX 문서를 활용한 SW 공급망보안 관련 정책적, 제도적 개선사항 제언

본 실증을 통해 국내 공급망 보안 강화를 위해서는 SBOM·VEX 기반 체계를 산업 전반으로 확대하고 이를 지속적으로 관리할 제도적 기반이 필요함을 확인

- SBOM 제출·관리 체계의 제도화 필요성
  현재 일부 분야에 한정된 SBOM 제출 규정을 산업 전반으로 확대하여 공급업체 제출 의무, 표준 형식 준수, 제출 주기 마련 등의 제도적 기반이 필요
- VEX 기반 실효성 중심 취약점 평가 체계 구축 필요성
  취약점 개수 중심 평가가 실제 위험도와 괴리가 있음, VEX 제출 의무화, 표준 형식 지원, 자동생성 도구 보급 및 인식 제고 등을 통해 실효성 기반 평가체계가 필요
- SBOM 중앙 저장소 및 검증 인프라 구축
  제출된 SBOM 변조 여부, 최신성, 패치 반영 상태를 검증할 수 있는 국가 단위 중앙 저장소 및 검증 시스템이 필요, 공공기관 주도로 이를 운영할 필요 존재
- SBOM, VEX를 활용한 SW 공급망보안 체계 구축 지원
  중소·중견 기업이 OSS를 독자적으로 관리하기 어려운 현실을 고려하여 취약점 모니터링 자동화, 패치 정보 제공 및 정부 차원의 무료 도구 지원, 자동 업로드 API 구축, 교육 및 컨설팅 제공 등 지원형 플랫폼의 확산이 필요

2-2. B사 실증 세부 결과 (정보보호기업)

기업별 도입 배경

참여배경

SW 공급망 보안의 중요성이 높아지고 SBOM 기반 자산 가시성 확보 필요성이 대두됨에 따라 실증사업에 참여하였으며 특히 기존 개발·운영 환경에서 OSS 사용 규모 파악의 어려움과 취약점 대응에 소요되는 시간과 비용을 줄이기 위한 목적으로 참여

실증대상 및 환경

방화벽 + VPN 제품으로 펌웨어 형태로 전용 하드웨어 일체형 장비에 탑재되어 배포, C언어, Java, Python 등의 언어로 구성되어 있으며 펌웨어 소스코드에 대해 SBOM 도구를 사용하여 분석을 수행

실증목적 및 기대성과

- 솔루션 구성요소 가시성 확보
- OSS 기반 취약점 조기 식별 및 대응 효율화
- VEX를 통한 취약점 실제 영향도 판단 고도화
- 장기적인 SW 공급망보안 내재화 체계 마련

실증 주요 결과

SBOM 생성 단계

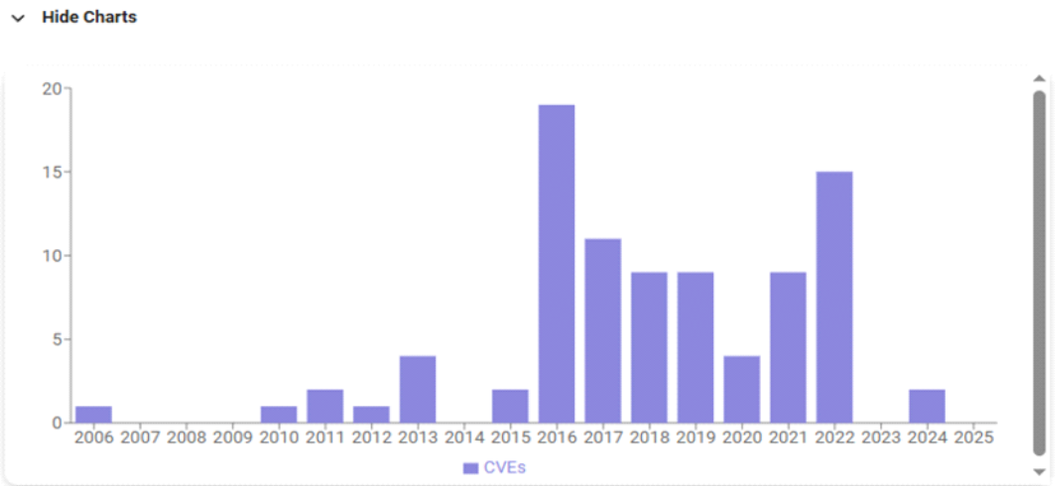
Result Details

File Name	보안상 생략
Files	9274
Dependencies	37
Input Format	ZIP File
Output Format	CycloneDX format SBoM

- 총 9,274개의 파일 중 37개의 컴포넌트, 의존성 발견
- 일부 라이브러리가 미검출되긴 하였으나 해당 미검출 내용은 현재 미지원 언어로 구성되어있거나 프로젝트 내 코드가 없는 등 미검출 원인을 확인하여 문제없음을 파악

- 초기 실증 시 30개 컴포넌트만 검출 되었으나 CNEPS 도구의 Gateway Time-out 및 파일 제한 조건을 제거하고 Batch 기반 병렬 알고리즘을 적용하여 성능 개선 후 모든 구성요소가 정상적으로 추출되고 Dependency 그래프도 정상적으로 생성, SBOM 분석의 정확성과 신뢰성이 크게 향상됨을 확인

취약점 분석 결과

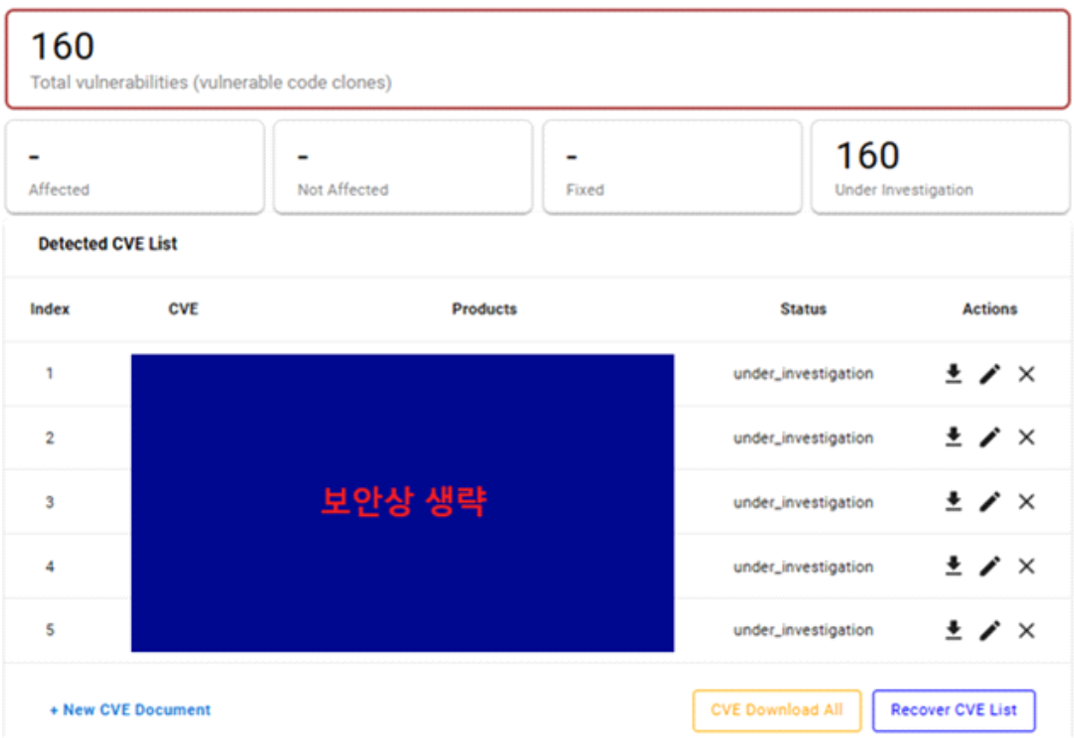


- 총 89종류의 157개 취약점 코드 클론 발견
- 취약점 모두 CVSS 레벨 Low로 표시
- 연도별 CVE 발견 건수를 시각화하여 제공하나 연도별 건수만으로는 위험도, 영향도를 직접적으로 판단할 수 있는 시각화 자료가 필요

VEX 문서 생성 결과


```
  "author": "Hatbom (lotcube 2.0)",
  "statements": [
    {
      "vulnerability": {
        "name": "CVE
      },
      "timestamp": "2025-11-14T00:59:41.478Z",
      "products": [
        {

        }
      ],
      "status": "under_investigation",
      "justification": "detected_cve_file",
      "impact_statement": "Detected by Vuddy; may be considered a vulnerability if included in the binary."
    },
    {
      "vulnerability": {
        "name": "CVE
      },
      "timestamp": "2025-11-14T00:59:41.478Z",
```



- 총 160개의 취약점 모두 Under-Investigation 상태로 분류
- 취약점 가능성은 존재하나, 실제 위험성을 단정할 수 없고 검토가 필요한 상태

취약점 조치 및 공급망보안 관리 계획

패치정보 확인 및 취약점 조치 계획

VDB 및 NVD 등 신뢰성 있는 취약점 데이터베이스를 활용하여 제품 및 내부 소프트웨어 구성요소에 대한 최신 취약점 정보를 주기적으로 수집하고 분석할 예정

식별된 취약점에 대해서는 CVSS 점수, 공격 가능성, 영향 범위를 기반으로 위험도를 평가하고 벤더 패치 정보 또는 보안 권고를 확인하여 적절한 조치 계획을 수립. 패치 적용이 가능한 경우에는 변경 관리 절차에 따라 검증 후 반영하며, 패치가 제공되지 않는 경우에는 구성 설정 변경, 접근통제 강화 등 대체 완화조치를 마련하여 제품의 보안성 지속 유지

SBOM 및 VEX 문서를 활용한 SW 공급망보안 관리 계획 수립

제품에 포함된 모든 소프트웨어 구성요소를 SBOM을 통해 체계적으로 관리, 취약점이 탐지된 경우 VEX 문서를 활용하여 해당 취약점이 실제 제품에서 Exploitable 한지 여부를 판단

SBOM을 기반으로 구성요소 버전, 업데이트 이력, 라이선스 정보를 투명하게 파악, VEX Status에 따라 우선순위 기반의 공급망보안 대응 전략을 수립 예정. 이를 통해 외부 오픈소스 및 제3자 소프트웨어로부터 유입될 수 있는 공급망 위험을 사전에 식별하고 취약점 대응의 정확성과 효율성을 높이는 기업 맞춤형 SW 공급망보안 관리체계를 구축

실증결과를 통한 시사점

- Lesson-Learned

  SBOM과 VEX를 적용한 결과, 소프트웨어 공급망 전반의 구성요소를 투명하게 파악할 수 있었으며, 기존 개별 개발자, 외주업체에 의존하던 라이브러리 관리 방식이 체계적으로 개선되었음. 특히 SBOM을 통해 제품에 포함된 패키지와 버전 정보를 자동화된 방식으로 식별함으로써 취약점 대응 시간을 크게 단축할 수 있었으며, VEX 문서 활용을 통해 취약점 존재 여부와 실제 exploitable 여부에 대한 개념 정립. 이를 통해 불필요한 패치 적용을 줄이고 중요 취약점에 대한 우선순위 기반 대응체계를 구축함에 대한 가능성 확인. 또한 실증을 통해 SBOM 생성 도구 간 정확성 차이, VEX 문서 표준화의 필요성 등 개선점을 확인하며 향후 공급망 보안 프로세스 정착을 위해 내부 관리 절차의 중요성을 체감하였음

- 실증사업 간 애로사항 및 개선 사항

  소스코드를 분석 시 결과에 대한 설명과 사용법 안내가 자세히 추가되어 있으면 해석에 도움이 될 것 같으며 또한 취약점 점검 결과로 제공되는 원형 그래프·막대 그래프는 수치가 표시되더라도 의미가 명확하게 설명되지 않아 이해가 어렵다는 문제가 있었음

- SBOM 및 VEX 문서를 활용한 SW 공급망보안 관련 정책적, 제도적 개선사항 제언

  SBOM과 VEX 문서의 표준화와 활용 가이드라인을 마련하여 기업이 도구를 보다 쉽게 활용하고 결과를 정확히 해석할 수 있도록 지원해야 함. 또한 취약점 데이터베이스와의 연계성을 강화하고, 오픈소스 라이선스 및 출처 정보 관리와 관련한 법적·제도적 근거를 명확히 하여 책임 소재를 분명히 할 필요가 있음. 아울러 기업이 SBOM·VEX 기반으로 보안 점검과 취약점 대응을 체계적으로 수행할 수 있도록 교육 및 인증 제도를 마련하는 방안도 요구됨. 이러한 제도적 개선을 통해 소프트웨어 공급망 전반의 투명성과 안전성을 높임이 필요

2-2. C사 실증 세부 결과 (의료기기 제조업체)

기업별 도입 배경

참여배경

2011년 제롬 래드클리프의 무선 통신 취약점을 이용한 인슐린 펌프 해킹 시연은 의료기기 연결성이 환자 생명을 직접적으로 위협할 수 있다는 사실을 각인 시킴. 오늘날 의료기기가 하드웨어 중심에서 AI, 클라우드 기반의 소프트웨어 기기로 진화함에 따라 오픈소스를 포함한 복잡한 시스템에 대한 보안의 중요성이 대두됨. 자사 의료기기의 구성요소를 시각화하고 CVE를 사전에 식별·조치함으로서 피해를 최소화하기 위해 실증에 참여

실증대상 및 환경

비침습적 심혈관 영상 분석을 지원하는 의료기기 소프트웨어(SaMD)로서 의료 영상 데이터를 정밀하게 분석하기 위해 딥러닝 아키텍처를 적용하였으며 Analyze, Detecion, Visualization, Modeling 등 기능별로 특화된 오픈소스 모듈을 활용하여 개발됨

실증목적 및 기대성과

'SBOM 실증 사업' 참여를 통해 제품 소프트웨어 자재 명세서(SBOM)를 정밀하게 작성하고 구성요소를 명확히 시각화. 이를 통해 알려진 취약점(CVE)을 사전에 식별·조치하고, 잠재적 위험을 차단하며 보안 사고 발생 시 피해를 최소화할 수 있는 대응 체계를 마련. 또한 국제 표준에 부합하는 SBOM과 보안 문서화 역량을 확보하여 해외 인허가 규제 리스크를 완화하고 글로벌 시장 진출 기반을 확보함. 마지막으로 개발부터 운영까지 일관성 있는 소프트웨어 공급망 보안 관리체계를 구축하여, 내부적으로는 개발 생산성과 유지보수 효율을 높이고 외부적으로는 소프트웨어 신뢰성을 입증할 수 있는 자산을 확보

실증 주요 결과

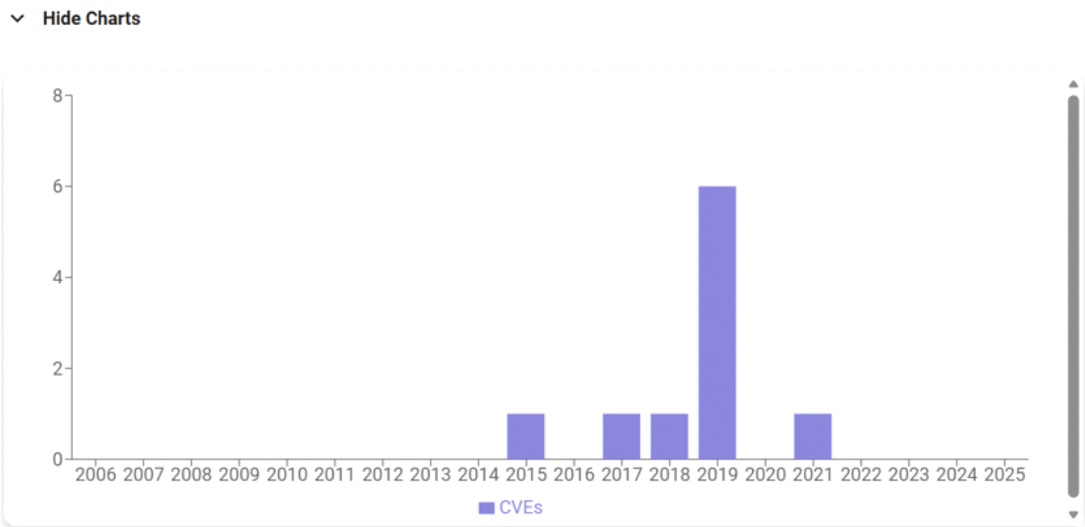
SBOM 생성 단계

Result Details

File Name	보안상생략
Files	1497
Dependencies	39
Input Format	ZIP File
Output Format	CycloneDX format SBoM

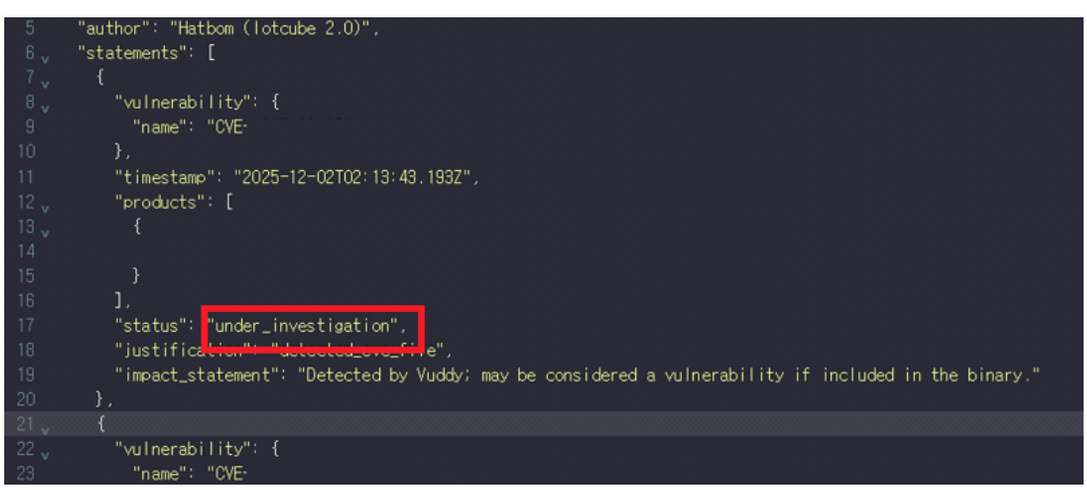
- 총 1,497개의 파일 중 39개의 컴포넌트, 의존성 발견
- 최상위 루트에서 파생되는 수십여 개의 직접 의존성과 이에 연결된 하위 종속성들이 트리 구조로 명확하게 시각화 및 SBOM Download 버튼을 통해 리스트를 자세히 확인
- 기존 수동관리되던 주요 모듈 외에도 30여 개 이상의 주요 라이브러리 패키지와 수백 개 이상의 하위 종속성 파일이 식별, 인지가 없던 종속성 파일에 대한 식별 계기, 이는 기능을 구현하는 모듈외에도 구동을 위한 보조 라이브러리로서 탐지된 것으로 파악
- 라이브러리 패키지의 구체적인 버전 정보가 명시되어 확인이 가능

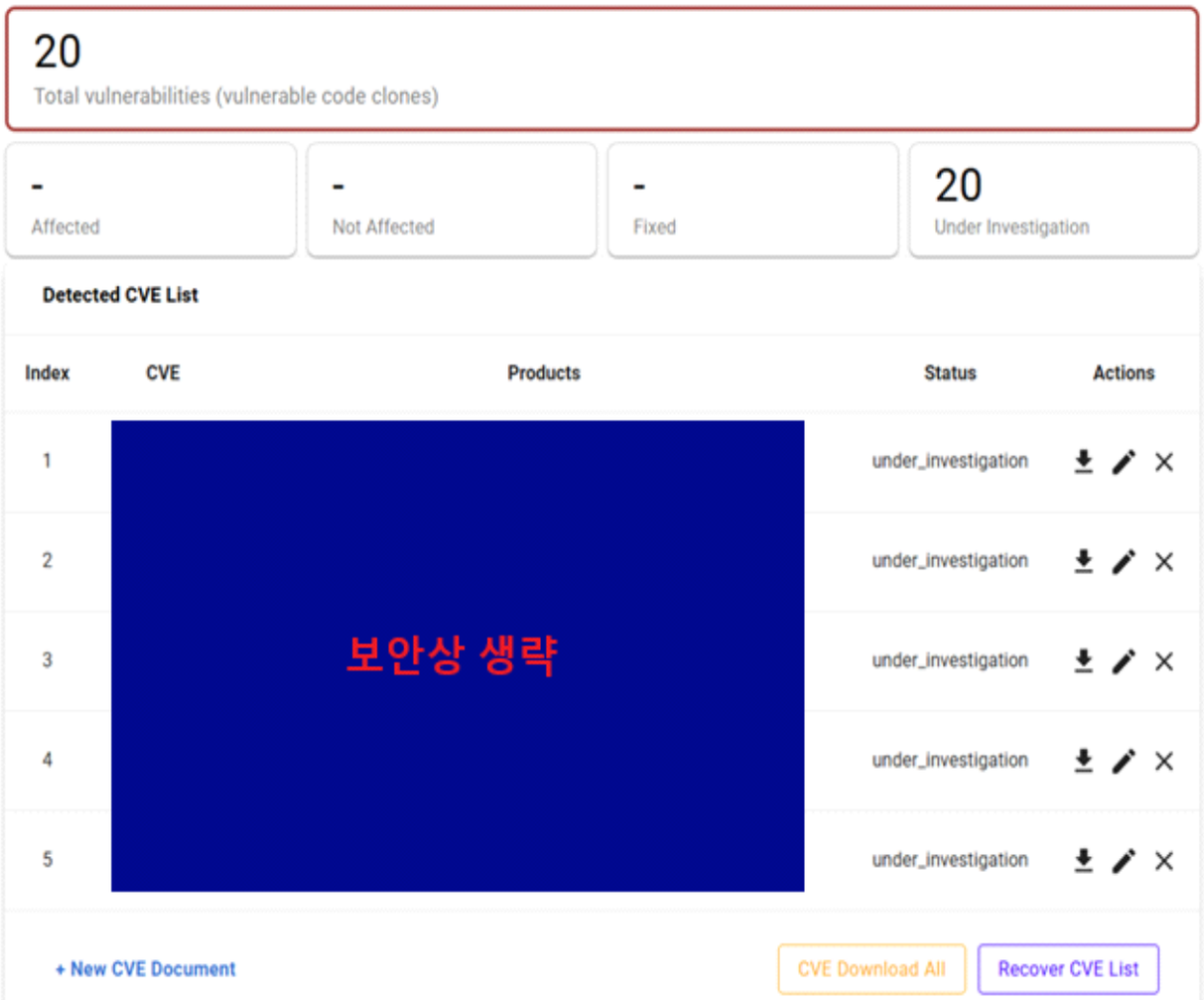
취약점 분석 결과



- 총 10종류의 20개 취약점 코드 클론 발견
- 발견된 취약점의 대다수 CVSS 레벨은 Low 등급이며 2개 CVE의 경우 Medium 등급, CISA에서 관리하는 KEV(Known Exploited Vulnerabilites)는 발견되지 않음
- 발견된 취약점은 2015년부터 2021년 사이에 분포되며 파일경로와 CVE 연도를 종합하였을 때 구동되는 패키지는 이미 공식 지원이 종료(EOL)된 상태로 취약점들이 패치되지 않은 상태이며 대부분의 경우 기기 특성을 고려할 때 위험하지 않거나 조치 가능한 것으로 판단

VEX 문서 생성 결과





- 총 20개의 취약점 모두 Under-Investigation 상태로 분류
- 취약점 가능성은 존재하나, 실제 위험성을 단정할 수 없고 검토가 필요한 상태

공급망보안 규제 분석 및 대응방안 수립

○ 국제 SBOM 관련 규제 및 가이드라인 관련 인허가시 필요사항 분석

의료기기 소프트웨어의 판매를 위해서는 의료기기 사이버보안 적용과 함께 의료기기에 대한 SBOM을 의료기기 규제기관에 제출하는 것이 필수. 국내도 「디지털 의료제품법」의 하위 규정으로 행정 예고된 「디지털의료기기 전자적 침해행위 보안 지침(안)」 제16조에서 SBOM을 활용하고 고려할 수 있다고 명시. 미국 FDA는 「의료기기 사이버보안 관리를 위한 시판 전 제출자료」의 내용과 「의료기기 사이버보안의 시판 후 관리」를 위해 제출해야하는 SBOM 요소를 요구하고 있음.

요구 내용으로는 기기에 포함된 모든 SW에 대한 포괄적이고 기계판독 가능한 SBOM을 생성해야하고 개발 코드, 외부 상용 SW, OSS, 상위 종속성 등이 포함되어야 하며 이는 NTIA에서 제시한 최소 구성요소를 충족하는 표준화된 형식으로 작성되어야 함. 일반적인 SW의 최소 구성요소와는 달리 FDA는 의료기기에 대해 구성요소가 유지보수 되는지에 대한 '지원 수준'과 기술지원이 끝나는 일자인 '지원 종료일'까지 반드시 추가적으로 기입하도록 하고 있음. 정보를 제공할 수 없는 경우 시판전 제출 자료에 대한 타당한 사유 소명. SBOM 외 취약점 발견 정보 및 방법, 그에 대한 보안 패치 및 보완 통제와 같은 구체적인 위험 통제 방안을 마련하여 문서화함이 필요

EU의 경우 새로운 의료기기 규정(MDR 2017/745)과 체외진단 의료기기 규정(IVDR 2017/746)을 채택하여 발표, 정보보안 조치를 강구해야하며 SBOM이라는 용어가 명시적으로 포함되어 있지는 않으나 관련 가이드라인에서 SBOM을 예시로 언급하며 사실상 제조사가 SBOM을 구비하고 제공할 것을 권고하고 있음. 또한 24년 10월 등장한 사이버복원력법 (CRA)에서는 디지털 요소가 포함된 모든 하드웨어 및 소프트웨어에 대해 SBOM 관리를 의무화하고 취약점을 식별하여 조치하도록 규정하고 있음. 이는 의료기기도 예외가 아니며 유럽시장에 진출하려는 의료기기 제조업체는 MDCG 가이던스의 권고와 CRA의 법적 요구사항을 충족하기 위해 SBOM을 생성하고 관리하는 체계를 필수적으로 갖추어야 함

과거의 의료기기 보안이 단순 방화벽, 백신 설치에 머물렀다면 현재는 SW 개발부터 공급망 전체의 투명성을 요구하며 국제적으로 규제 장벽이 높아지고 있기에 기존의 수동적인 관리 방식으로는 요구사항을 충족하기 어려움. 개발자가 인지하지 못하는 숨겨진 종속성에서 보안 취약점이 발생할 경우 신속한 식별과 대응이 불가능하여 환자의 안전을 위협하는 사고로 이어질 수 있기 때문에 자사 제품내에서 모든 소프트웨어 자산을 정확히 식별하고 가시성을 확보하고자 함. 실시간으로 업데이트되는 위협정보에 실시간으로 대응하기 위해 SBOM과 취약점 데이터베이스가 연동된 자동화 관리체계를 이용할 계획이며 이를 기반으로 SBOM 및 관련 문서를 작성, 인허가 시 관련 자료를 활용할 계획에 있음

실증결과를 통한 시사점

Lesson-Learned

실증을 통해 기존 수동 대장 관리로는 파악하지 못했던 전이적 종속성과 보조 라이브러리를 다수 식별. 특히 의료 SW의 특성상 설치 라이브러리와 실제 런타임 종속성이 어떻게 연결되는지 시각적으로 확인함으로써, 당사가 관리해야 할 공급망 보안의 실질적 범위를 재정의할 수 있었음. 단순히 CVE를 나열하는 방식에서 벗어나, VEX를 활용해 취약점이 실제 제품에 영향을 미치는지 기술적으로 설명하는 절차를

경험함으로써 규제 대응의 핵심이 '취약점 존재 여부'가 아닌 '통제 가능성 입증'에 있음을 명확히 이해함. 또한 Not Affected, Fixed 등 상태값을 기계판독 가능한 형식(JSON)으로 산출해 글로벌 규제 기관과 교차검증 가능한 공통 언어를 확보할 수 있었음

- **실증사업 간 애로사항 및 개선 사항**

  패키지 매니저 정보와 실제 바이너리 파일 간 불일치가 종종 발생하여, 일부 라이브러리의 버전이 잘못 식별되거나 정적 분석 도구가 특정 모듈을 놓치는 문제가 발생. 또한 SBOM·VEX 도구가 보안 전문가 중심으로 설계되어 있어 의료기기 개발자나 QA 담당자가 사용하기에는 진입 장벽이 높았고, 오류 발생 시 참고할 수 있는 트러블슈팅 가이드가 부족해 도구 활용에 상당한 리소스가 소요. 실무자 관점에서 따라 하기 쉬운 UI 개선, 단계별 매뉴얼, 케이스 기반 안내서 보완 시 실증 결과의 활용성이 크게 높아질 것으로 판단

- **SBOM 및 VEX 문서를 활용한 SW 공급망보안 관련 정책적, 제도적 개선사항 제언**

  사이버보안 전담 인력이 부족한 중소 의료기기 기업의 현실을 고려하면, SBOM 관리를 기업 자율에만 의존할 경우 형식적 문서 작성에 그칠 우려가 큼. 따라서 이론 중심의 SBOM 개념 설명을 넘어서, 의료기기 개발 생명주기(SDLC) 단계별 실무 기준, 오픈 소스 선정, SBOM 자동 생성, 취약점 모니터링, VEX 발행, 변경 이력 관리가 포함된 구체적 가이드라인 마련이 필요. 또한 의료기기 제품 특성상 EOL 언어와 구버전 라이브러리를 완전히 배제하기 어려운 만큼, 이를 안전하게 격리·통제할 수 있는 기술적 요구사항과 함께 SBOM 기반의 위험관리 절차를 공식적으로 인정하는 제도적 장치가 마련된다면 중소 제조업체의 규제 대응 부담을 실질적으로 완화할 수 있을 것으로 판단

3. 요약 및 시사점

[표 16] 기업별 SBOM 실증 결과 요약

구 분	A사 (정보보호기업)	B사 (정보보호기업)	C사 (의료기기 제조업체)
참여 목적	- SBOM 기반의 SW 관리체계 구축 필요성 인식 - OSS 라이선스 및 취약점 식별 및 관리방안으로 SBOM 도입	- SBOM 기반 자산 가시성 확보 - 개발·운영환경에서 OSS 규모 파악 및 취약점 대응 시간 절감	- SW 중심 의료기기 산업에서 보안 중요성 대두 - 자사 의료기기 구성요소 시각화 및 CVE 조치
실증 대상 및 환경	- 보안 웹 게이트웨이(SWG) - C언어, PHP 언어로 구성 - Linux기반에서 개발된 소스를 웹 플랫폼에 업로드	- 방화벽 + VPN 제품 - C언어, Java, Python으로 구성 - 펌웨어형태로 전용 하드웨어 일체형 장비에 탑재	- 딥러닝 아키텍처가 적용된 의료기기 SW(SaMD) - 기능별로 특화된 오픈소스 모듈 활용하여 개발
SBOM 추출 결과	- 2,681개 파일 중 84개 컴포넌트, 의존성 확인 - 주요 라이브러리 일부는 정확하게 버전까지 일치 - 일부 미탐·오탐현상 발견 (필터링 알고리즘이 원인)	- 9,274개 파일 중 37개 컴포넌트, 의존성 확인 - 일부 미검출에 대해서는 원인확인하여 문제없음 파악 - 성능개선 후 정확성 및 신뢰성 크게 향상	- 1,497개 파일 중 39개 컴포넌트, 의존성 확인 - 직접 의존성 및 하위 종속성 트리 구조로 시각화 확인 - 의료분야에서 많이 활용되는 OSS를 DB에 추가하여 OSS 탐지율 대폭 개선
취약점 분석	- 총 30종류의 101개 취약점 코드클론 발견 - 취약점 CVSS 모두 Medium - UI 개선 및 시각화자료 추가 필요	- 총 89종류의 157개 취약점 코드클론 발견 - 취약점 CVSS 모두 Low - UI 개선 및 시각화자료 추가 필요	- 총 10종류의 20개 취약점 코드클론 발견 - 2개 CVE Low 등급, 그 외 모두 Medium 등급 - 취약점은 위험하지않거나 조치 가능한 것으로 판단
VEX 추출 결과	- 총 101개 취약점 모두 Under-Investigation 상태로 분류	- 총 160개 취약점 모두 Under-Investigation 상태로 분류	- 총 20개 취약점 모두 Under-Investigation 상태로 분류
공급망보안 관리 계획	- 개발·배포되는 모든 SW에 대해 SBOM 생성하여 관리 - VEX Status 활용하여 취약점 위험성 판단, 우선순위 조정 - 협업, 릴리즈 간 SBOM 활용 - 조직내 활용 프로세스 정립	- 취약점 공개 DB 활용하여 자사제품 분석 진행 - VEX Status 활용하여 Exploitable 여부 판단 및 우선순위 조정 - SBOM을 활용한 SW공급망 보안 관리체계 구축	- 의료기기 관련 인허가 시 SBOM 기반 관련 문서 작성, 자료 활용 계획 - SBOM 기반의 기기 구성요소 파악 및 취약점 식별

[표 17] 실증 결과에 대한 평가

구 분	실증결과에 대한 평가
총평 및 시사점	- 실증을 통해 SBOM과 VEX가 단순 산출문서가 아니라 SW 공급망보안 핵심 자산이자 지속가능한 관리 체계로 확장될 수 있는 기반임이 확인, **세 기업 모두 SBOM과 VEX 문서를 통한 SW 공급망 보안 관리체계 운영의 가능성 및 효과성을 확인** - 사전 OSS 리스트와 비교하였을 때 대부분의 OSS 리스트와 취약점이 이상 없이 검출됨을 확인, 3차년도 실증과 비교하여 **도구 개선 작업을 통한 유의미한 정확도 향상을 확인** - VEX 문서 활용을 통해 **'취약점 존재 여부'가 아닌 '제품에 영향을 미치는지(Exploitable 여부)'에 기반한 우선순위 결정 체계의 가능성을 확인,** 효율적 취약점 관리 기대
Lesson Learned	- 막연한 규제 대응 불안감에서 벗어나 OSS 구성요소를 투명하게 관리할 수 있는 체계의 중요성 인식, SBOM/VEX 기반의 체계적 공급망보안 관리 방안 수립 계획을 세우는 계기가 됨 - 스스로 사용중인 OSS의 취약점을 파악·관리하지 않으면 글로벌 규제 대응 및 고객사 요구에 대응하기 어렵다는 점을 체감, 체계적인 관리의 필요성 인식 - CVE는 모두 조치해야할 사항이 아니라 실질적으로 SW에 영향을 미치는 Exploitable한 취약점을 조치해야 한다는 인식 제고, 이 과정에서 VEX 문서를 활용할 예정 - SBOM 도구 적용 결과, 기존 OSS 리스트 수작업 정리 대비 식별되지 않은 요소, 종속성, Exploitable 여부 등을 확인, 수동 관리가 가진 누락·오판 가능성의 개선과 시간·비용 절감 측면에서 자동화 기반 SBOM/VEX 생성 도구의 필요성을 명확히 인지 - 실증사업 참여를 통해 자체적으로 사용중인 OSS를 목록화하고 업데이트를 수행하는 계기가 됨 - OSS 기별-버전관리-취약점검토-배포관리로 이어지는 내부 관리 절차의 정립과 책임부서 지정의 필요성을 절감하였으며 SW 공급망보안에 대한 조직적 인식 수준이 크게 향상
도구 개선 사항	- Low, Medium, High로 표시되던 CVSS Level을 점수로 표시할 수 있도록 개선 - 취약점 설명 단계에서 버튼 클릭을 통해 패치 정보를 확인할 수 있도록 개선 - CNEPS 도구의 Gateway Time-out 및 파일 제한 조건을 제거하고 Batch 기반 병렬 알고리즘을 적용하여 성능 개선 후, 컴포넌트 탐지 정확도가 상승
실증 사업 간 애로사항, 개선사항	- VEX 기반 Exploit 여부 판단 과정에서 단순 CVSS 레벨 및 Exploitable 여부 외 추가적인 기술정보, 해석, 시각화 그래프를 추가함으로서 자세한 설명 및 실무 활용도 제고 필요 - 파일 크기 제한, 비표준 빌드 환경 파일 처리 문제, 해시 후 파일 구조 변경 등 업로드 제약, 오류발생 시 참고할 수 있는 가이드 제공 및 UI 개선 등 플랫폼 사용 편의성 개선 필요 - API/CLI 기반 자동 업로드 및 실시간 업데이트 등 연동 기능 제공이 있으면 좋을 듯 함
정책적 제도적 제언	- 산업전반으로 SBOM 제출 의무 범위를 확대하고 표준 형식, 제출 주기 등 기준을 표준화 - 취약점 개수가 아닌 VEX Status 기반의 실효성 중심 취약점 평가 체계 구축 - 국가적 SBOM 중앙 저장소 및 취약점 패치, SBOM 검증을 진행하는 공공주도의 체계 마련 - 중소기업을 위한 SBOM 생성도구 제공, 컨설팅, 교육 프로그램 등 지원 프로그램 확대 - 산업별 가이드라인 마련 및 오픈소스 라이선스 및 출처 정보 관리 관련 법적·제도적 근거 명확화

V

참고

국·내외 SW공급망보안 현황 및
SBOM 도구 실증
결과보고서

V 참고

1) Checkmarx 칼럼, “XZ 유틸즈 백도어 악성코드 발견.. 현재까지 알려진 가장 진보된 공급망 공격”

2) 로그프레소 위협분석, “북한 라자루스(Lazarus) 그룹이 배포한 악성 npm 패키지 감염 사례”

3) https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

4) NHS England, “business continuity management toolkit case study: WannaCry attack”

5) The White House, “Executive Order on Improving the Nation’s Cybersecurity”

6) Federal Register, “Strengthening and Promoting Innovation in the Nation’s Cybersecurity” / The White House, ”Sustaining Select Efforts to Strengthen the Nation’s Cybersecurity and Amending Executive Order 13694 and Executive Order 14144

7) US Army, “Assistant Secretary of the Army(Acquisition, Logistics and Technology) – Sofrware Bill of Materials Policy

8) U,S. Department of War, “Software Fast Track Initiative”

9) European Parliament(2022.9.), “Regulation of the European Parliament and of the council : on horizontal cybersecurity requirements for products with digital elements and amending Regulation(EU) 2019/1020”

10) European Commission, “Radio Equipment Directive”

11) European Insurance and Ocuupational Pensions Authority, “Digital Operational Resilience Act(DORA)”

12) 국가정보원, 과학기술정보통신부, 디지털플랫폼정부위원회, “SW 공급망 보안 가이드라인 v1.0”

13) 고용노동부 보도자료, “산업변화에 발맞춰 변화하는 2024년 국가직무능력표준(NCS)”

14) https://www.etnews.com/20250103000035?

15) https://www.lawtimes.co.kr/LawFirm-NewsLetter/205209

16) GOV.UK, “Software Security Code of Practice”

17) METI, “Revised Guide Formulated on Specific Methods for Managing Software Vulnerability Utilizing ‘Software Bill of Materials (SBOM),’“

18) 정보통신산업진흥원, “국가별 ICT 시장동향, 일본”

19) Australian Signals Directorate, “New guidance on integrating a Software Bill of Materials (SBOM)”

20) Joint guidance on a shared vision of software bill of materials for cyber security - Canadian Centre for Cyber Security

21) FD&C Act, Section 524B, 2022

22) FDA, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, Final Guidance, 2023; FD&C Act §524B, 2022

23) 스마트의료보안포럼 발표자료, “의료기기 SBOM 동향, 방지호 박사, 2024.05”

24) 법률 제20331호, “디지털의료제품법”

25) 식품의약품안전처, “디지털의료기기 전자적 침해행위 보안지침”

26) CISA, “Software Supply Chain Security Update, 2025”

27) NTIA, “Survey of Existing SBOM Formats and Standards, 2021”,

28) The Linux Foundation Projects “About SPDX”

29) OWASP “CycloneDX One Pager”

30) NTIA, Department of Commerce “The Minimum Elements For a Software Bill of Materials” (2021.07)

31) CISA, “2025 Minimum Elements for a Software Bill of Materials (SBOM)”

VI

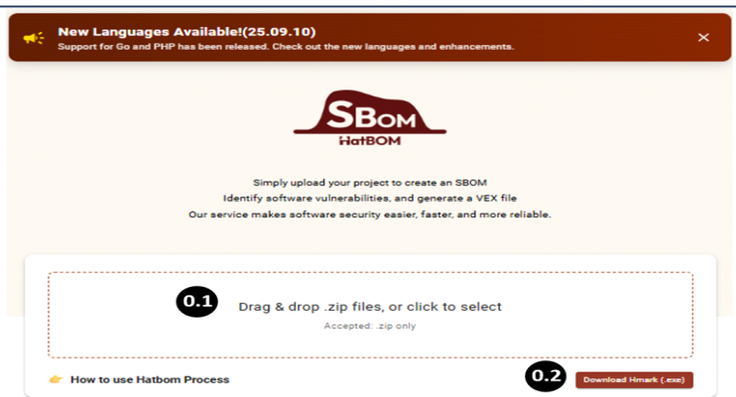
부록

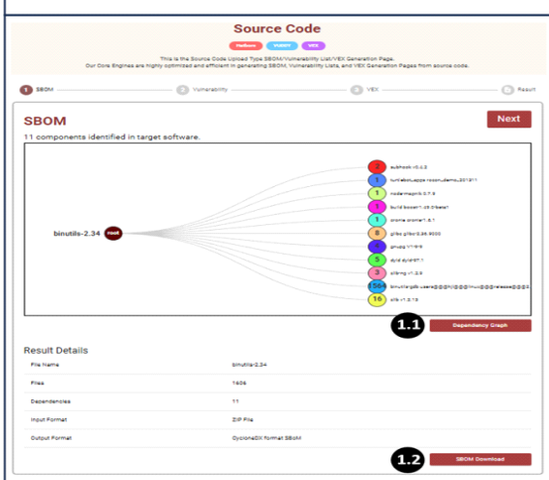
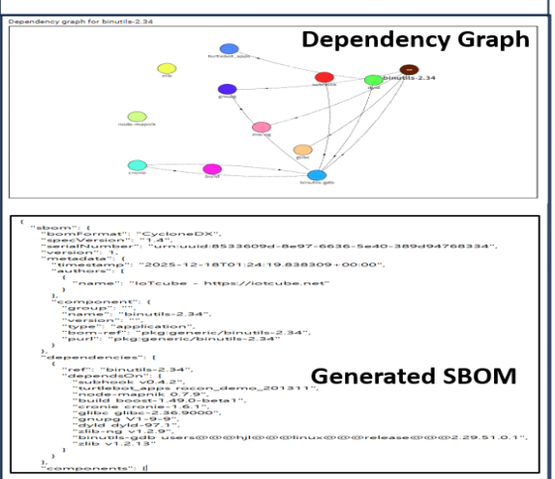
국·내외 SW공급망보안 현황 및
SBOM 도구 실증
결과보고서

Ⅵ 부록

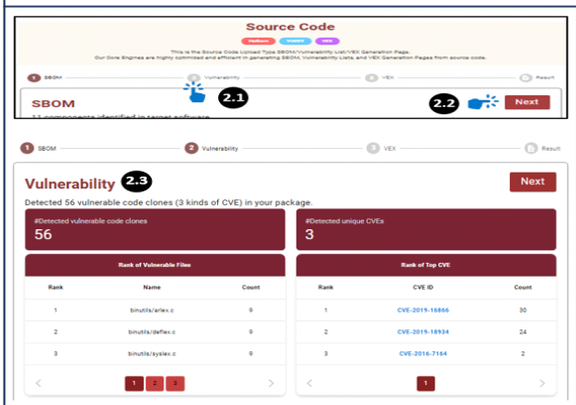
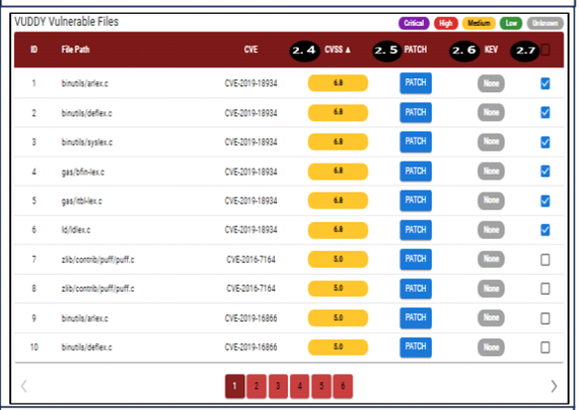
SBOM 도구를 사용하여 실증 참여기업 따라해보기

SBOM Generation

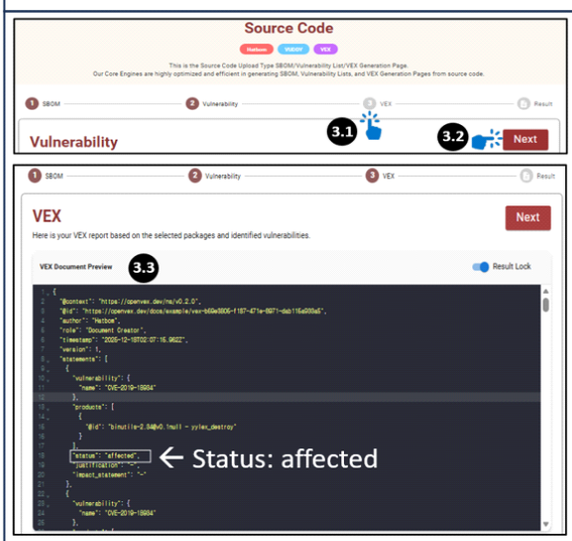
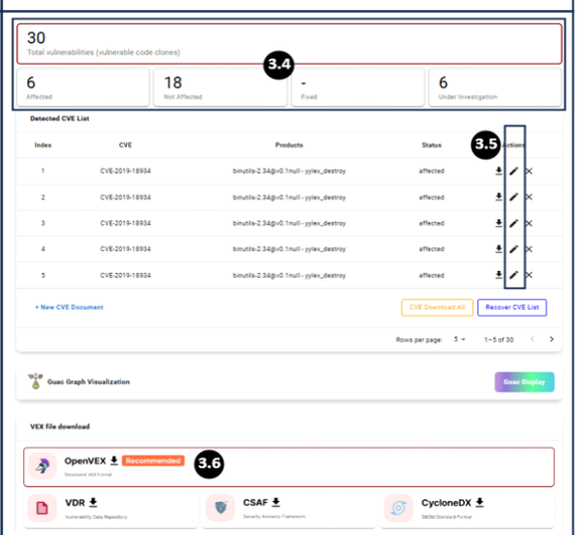
⓪ 메인화면(https://iotcube.net)

0-1. 분석하고자 하는 프로젝트 소스 디렉토리를 .zip 파일로 만들어 선택 0-2. 소스파일 프러이버시를 원한다면 Hmark도구를 다운받아 해시파일로 만든 .zip파일을 선택

① SBOM 자동 생성	① SBOM 자동 생성
	
1-1. 오픈소스 컴포넌트들간의 의존성을 확인하고자 하는 경우 클릭 1-2. SBOM 문서를 다운받기를 원한다면 클릭	위) 오픈소스 컴포넌트들간의 의존성 관계를 보여줌 아래) 자동생성된 SBOM 문서(CycloneDX형식의 json)

Vulnerability Detection

② Vulnerability Detection	② Vulnerability Detection
	
2-1. 네비게이션의 Vulnerability를 클릭하거나 2-2. Next 버튼을 클릭 2-3. [결과화면 1] 총 56개의 취약한 코드클론이 탐지되었고, 3종의 CVE가 존재	[결과화면 2] 2.4 CVSS(심각도 수준)값 표시 2.5 패치 정보 제공 2.6 KEV 표시로 패치 적용 우선순위 제공 2.7 VEX문서 생성을 위한 예제로 CVSS가 6.8인 6개를 선택

VEX Document

③ VEX문서 생성	③ VEX문서 생성
	
3-1. 네비게이션의 VEX를 클릭하거나 3-2. Next 버튼을 클릭 [결과화면 1] 3-3. CVSS가 6.8인 취약점들에 대한 악용가능성 (Exploitability)을 판단	[결과화면 2] 3.4 총 30개의 탐지된 취약점들에 대한 분석결과 Affected(6), Not Affected(18), Fixed(0), Under Investigation(6) 3.5 내부 검토회의를 거쳐 각각의 취약점 상태를 조정할 수 있다. 3.6 최종적으로 결정된 VEX문서를 OpenVEX형식으로 저장한다.

※ 보다 상세한 사용자 가이드는 아래 사이트에서 제공하고 있으니 참조바랍니다.
(User Guide 및 동영상 제공)