KT 공급망 보안을 위한

공급사 SBOM 제출 가이드

V.1.2

2026.06

정보보안실 보안혁신이행담당

목차

1 개요 3

2 제출 프로세스 3

3 표준 SBOM 형식 4

4 SBOM 생성 방법 4

5 SBOM 문서 내 필수 필드 5

6 SBOM 제출 전 체크리스트 8

1 개요

1.1 SBOM(Software Bill of Materials) 정의

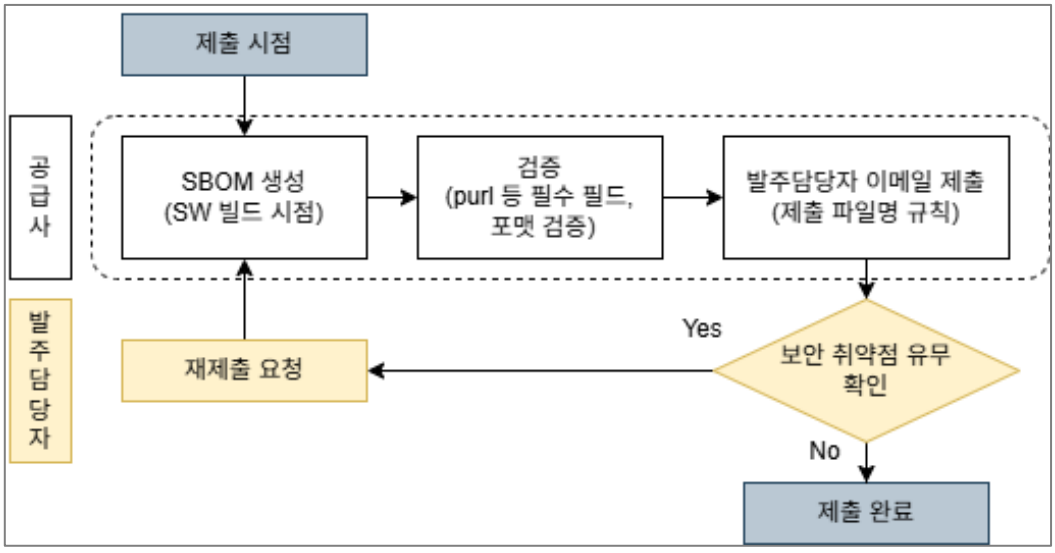
소프트웨어의 구성요소 정보를 나열한 명세서로, 펌웨어, 라이브러리, 오픈소스 등을 포함한 Component 정보(이름, 버전, 의존 관계 등)가 기입된 파일입니다.

1.2 SBOM 제출 목적

공급사 솔루션으로 인해 발생할 수 있는 보안 위험을 체계적으로 식별·관리하기 위해 SBOM 기반의 검증을 통해 KT 서비스 전반의 보안 수준을 향상시키고자 합니다. 이를 위해 공급사에서는 납품 솔루션에서 아래 "5. SBOM 문서 내 필수 항목"이 누락되지 않도록 검토하여 제출해주시기 바랍니다.

2 제출 프로세스

제출 대상으로 지정된 물자의 공급사는 제출 시점 도래 시 SBOM을 생성하여 발주 담당자에게 제출하여야 하고, KT 발주 담당자는 해당 정보를 KT 정보보안실로 제출 및 보안 검토결과(SBOM 보안 취약점 점검)를 공급사에 전달하여 조치 등 후속 관리 진행합니다.



2.1 제출 대상: SW가 포함된 물자(추후 대상 변경 가능)

구분	설명	비고
SW 탑재 장비/물자 (Embedded/Firmware)	HW에 포함되어 공급되는 SW의 SBOM	(예) 방화벽, 라우터, UPS와 같은 전원장치 관리시스템 등 - NIC, Storage는 제외 - 항온/항습기 단품 제외 (단, 온도 중앙조절 장치는 대상)
외부 공급(3rd party) SW	외부 업체가 개발하여 납품/도입하는 SW(완제품 형태)의 SBOM	(예) 백신 프로그램, 패키지 SW, SaaS 솔루션 - 외주 개발 SW가 탑재된 물품 포함 (지니 STB)

2.2 제출 시점

1) SW가 포함된 물자 계약을 위한 장비 평가 시

2) SW가 포함된 물자 계약 시

3) 계약서에 명시된 정기 제출 일정 도래 시

4) 제출한 SBOM을 통해 확인된 보안 취약점 조치 이행 시(신규 취약점 확인 포함)

2.3 제출 전 검증: 아래 *"6 SBOM 제출 전 체크리스트"* 항목 검증

2.4 제출 파일명 규칙: (계약번호/장비평가게시번호)자재코드_SW자재명

- 동일 계약번호로 여러 자재를 구매할 경우 자재별 SBOM 구분을 위함
- 장비평가 대상은 계약번호 대신 장비평가게시번호를 작성합니다.

3 표준 SBOM 형식

KT는 국제적 또는 산업계에서 통용되는 표준 SBOM 형식을 지원하며, 아래 표에 명시된 버전과 파일 포맷으로 제출하여 주시기 바랍니다.

표준 SBOM 형식	버전	파일 포맷
CycloneDX	1.4, 1.5	JSON
SPDX	2.2, 2.3	JSON

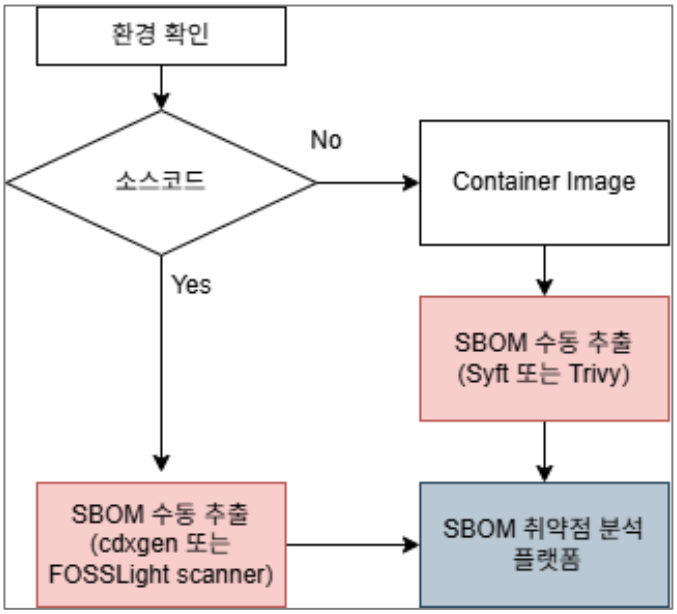
※ SBOM 생성 도구(아래 "*4.2 오픈소스 SBOM 생성도구*")별 지원 형식 선택하여 제출

4 SBOM 생성 방법

오픈소스 SBOM 생성 도구를 활용한 추출 환경별 SBOM 생성 방법을 안내합니다.

4.1 SBOM 생성 도구 선택 가이드

환경별 SBOM 수동 추출 대상을 정의하고, 그에 맞는 SBOM 생성 도구를 제안합니다.



4.2 오픈소스 SBOM 생성 도구

4.2.1 SBOM 생성 도구 선택 시 참고사항

1) 정확한 SBOM 생성을 위해서는 소스코드 레벨, 이미지 레벨의 추출을 권장합니다. (참고) 바이너리를 통해 생성된 SBOM은 취약점 분석에 적합하지 않아 소스코드/이미지에서 SBOM 추출 필요
2) 소스코드만 있는 상태에서는 전이적 의존성이 누락될 수 있으며, 전이적 의존성이 정확하게 포함하기 위해서는 빌드(또는 패키지 설치)가 완료된 상태에서의 SBOM 생성을 권장합니다.

환경	생성도구	지원 대상	지원 SBOM 형식	비고
소스 코드	Cdxgen	Java(Maven/Gradle), Python, Node.js, Go, Ruby, PHP, Rust, .NET, C/C++ 등	Cyclonedx	공식 문서: https://owasp.org/www-project-cdxgen/ GitHub: https://github.com/CycloneDX/cdxgen
	FOSSLight Scanner	상동	SPDX, Cyclonedx, xlsx	공식 문서: https://fosslight.org/fosslight-guide/scanner/ Github: https://github.com/fosslight/fosslight_scanner
이미지	Trivy	컨테이너 이미지, Docker 이미지, OCI 이미지, git 레파지토리	SPDX, Cyclonedx	공식 문서: https://trivy.dev/docs/latest/guide/target/sbom/ GitHub: https://github.com/aquasecurity/trivy
	Syft	컨테이너 이미지, Docker 이미지, OCI 이미지 등	SPDX, Cyclonedx	공식 문서: https://oss.anchore.com/docs/guides/sbom/getting-started/ Github: https://github.com/anchore/syft

5 SBOM 문서 내 필수 항목

SBOM 문서에 아래 정의된 필수 항목이 있어야 취약점 분석이 가능하므로 반드시 공급사는 필수 항목의 존재 여부 확인 후 제출해야 하며, 필수 항목 부족 시 반려될 수 있습니다.

5.1 SBOM 형식별 필수 항목 정보

SBOM에 포함되어야 할 필수 항목 목록을 전달하고, 각 항목에 대한 설명은 *"5.2 SBOM 형식별 항목 설명"*을 참고합니다.

Data Type	SPDX	Cyclonedx
기본 정보	SPDXID, CreationInfo, DataLicense, DocumentNamespace	bomFormat, specVersion, version, serialNumber, tools("name", "version"), component
SW 정보	[Packages] 하위 SPDXID, CopyrightText, DownloadLocation, externalRef("referenceCategory", "referenceLocator", "referenceType"), filesAnalyzed,licenseConcluded, licenseDeclared, name, versionInfo	[Components] 하위 type, name, version, purl, bom-ref, licenses
의존성	[relationships] 하위 spdxElementId, relatedSpdxElement, relationshipType	[dependencies] 하위 ref, dependsOn

5.2 SBOM 형식별 항목 설명

5.2.1 SPDX

Data Type	항목명	설명	예시
Metadata	SPDXID	문서 고유 식별자	SPDXRef-DOCUMENT
	CreationInfo.	SBOM 생성 정보	"creators":[Tool: Syft], "
	DataLicense	SBOM 자체의 라이선스	CC0-1.0
	DocumentNamespace	글로벌 유일 식별자 (중복 방지)	http://example.com/spdx/example-server/1.0
Packages	SPDXID	패키지 고유 ID	SPDXRef-package-515…
	CopyrightText	권리 귀속 확인	Copyright (c) OpenSSL
	DownloadLocation	출처 추적	https://www.openssl.org/source/openssl-1.1.1k.tar.gz
	externalRef. "referenceCategory"	외부 참조 용도/범주 (패키지 식별, 보안 등)	"package-manager"
	externalRef. "referenceLocator"	실제 외부 참조 식별자 (Identifier String)	"pkg:generic/openssl@1.1.1k"
	externalRef.	외부 참조 식별자 표준	"purl"

	“referenceType”	(specification)	
	filesAnalyzed	파일 단위 분석 여부	True / false
	licenseConcluded	분석 후 확정 라이선스	OpenSSL
	licenseDeclared	공급자가 선언한 라이선스	OpenSSL
	name	소프트웨어 이름	openssl
	versionInfo	소프트웨어 버전	1.1.1k
relationships(의존성)	spdxElementId	관계의 주체 고유 식별자	SPDXRef-Package-MyApp
	relatedSpdxElement	관계의 대상 고유 식별자	SPDXRef-Package-75cdc…
	relationshipType	관계의 성격 (SPDX 요소 간 관계 종류)	DEPENDS_ON: 요소가 다른 요소에 의존

5.2.2 Cyclonedx

Data Type	항목명	설명	예시
Metadata	bomFormat	SBOM 형식	CycloneDX
	specVersion	SBOM 형식 버전	스펙 버전
	version	문서 버전	1
	serialNumber	문서 고유 식별자	urn:uuid:123e4567- …
	tools.	SBOM 생성 정보	“name”: “Syft”, “version”: “0.90.0”, …
	component	루트 애플리케이션 정보	“name”: “abc”, “version”:1.0”, “bom-ref”: “88bbee27-bc8…”
Components	type	구성요소 유형	library / application
	name	소프트웨어 이름	openssl
	version	소프트웨어 버전	1.1.1k
	purl	실제 외부 참조 식별자 (Identifier String)	pkg:generic/openssl@1.1.1k
	bom-ref	외부 참조 식별자	“baeca056-827…"
	licenses	라이선스	OpenSSL
Dependencies(의존성)	ref	관계의 주체 고유 식별자 (bom-ref)	“88bbee27-bc8…”
	dependsOn	관계의 대상 고유 식별자 (bom-ref)	“baeca056-827…"

5.2.3 SBOM 대분류 Data Type에 대한 설명

5.2.3.1 기본 정보(Metadata): SBOM 문서 자체와 생성 도구에 대한 정보

5.2.3.2 SW 정보(Packages/Components): SW를 구성하는 라이브러리 정보

5.2.3.3 Package URL(PURL): 소프트웨어 패키지 고유 식별자

※ PURL 정보에 "pkg:" 없이 "cpe:" 항목만 존재할 경우 SBOM 재제출 필요

5.2.3.4 의존성 정보(relationships/dependencies): 라이브러리가 사용하는 다른 소프트웨어에 대한 정보

※ 의존성이 포함되지 않을 경우 숨겨진 취약점을 놓칠 수 있어 SBOM 재체출 필요

5.2.3.4.1 의존성 종류

의존성 종류	설명	SBOM 필수 여부
직접 의존성	프로젝트가 직접 선언한 라이브러리	필수
전이적 의존성	직접 의존성이 다시 의존하는 라이브러리	필수

(예시) 전이적 의존성

```
MyApp
└── library-A v1.0 (직접 의존성)  ← 프로젝트가 직접 명시적으로 선언 √
      └── library-B v2.3 (전이적 의존성) √
```

6 SBOM 제출 전 체크리스트

6.1 포맷 오류 검증(SBOM Validation Checker)

SBOM 파일의 포맷이 맞는지 아래의 링크로 확인 가능하며, 포맷 오류 확인 시 재추출이 필요합니다.

- https://sbomgenerator.com/tools/validator(업로드형)
- https://sbom.observer/free/sbom-analyzer(업로드형)
- https://github.com/microsoft/sbom-tool(설치형)

6.2 유의미한 SBOM 데이터 점검

6.2.1 파일 점검

1) 파일의 크기가 1KB 이상이며, 파일 내용이 비어 있지는 않는지

6.2.2 필수 필드 점검

1) Metadata가 최상위 컴포넌트(납품 프로젝트)의 이름과 버전과 동일한지
2) 모든 SW(Packages/Components) 객체 안에 PURL 필드가 존재하는지
3) PURL 필드의 데이터가 "pkg:…"로 되어 있는지

6.2.3 의존성 점검

1) 직접 의존성 및 전이적 의존성이 포함되어 있는지

별첨1. 참고 사이트

1. CycloneDX Specification
2. SPDX Specification
3. Package URL Specification