

# FOSSLight Scanner 또 Update 되었어요

FOSSLight Community Day 2026

2026.10.28 · LG전자 OSPO 박원재



LG Open Source

# 통합 실행과 개별 스캐너의 역할

Scanner



# 분석에서 SBOM까지, Scanner의 변화

Scanner

## Source

- 1 파일별 결과를 폴더 단위로 요약
- 2 Source 분석 속도 개선
- 3 외부 조회 안정성 개선
- 4 Manifest 에서 라이선스 정보 추출

## Dependency

- 5 uv.lock·NuGet CPM 분석 지원 확대
- 6 Gradle 환경에 맞는 분석 플러그인 선택
- 7 Gradle 의존성 구성 선택

## Binary

- 8 JAR 파일 분석 강화

## SBOM

- 9 SBOM 출력 확장

# 1 파일별 결과를 폴더 단위로 요약

Source

v2.3.3 ~

**요약 조건**    OSS 이름 · 버전 · 라이선스 · 다운로드 위치가 충돌하지 않을 때

파일별 결과 · 8파일

| Path                     | OSS Name | Version | License    |
|--------------------------|----------|---------|------------|
| vendor/alpha/a.c         | alpha    | 1.0     | MIT        |
| vendor/alpha/src/b.c     | alpha    | 1.0     | MIT        |
| vendor/alpha/include/c.h | alpha    | 1.0     | MIT        |
| vendor/beta/x.c          | beta     | 2.0     | Apache-2.0 |
| vendor/beta/y.c          | beta     | 2.0     | Apache-2.0 |
| app/main.c               | alpha    | 1.0     | MIT        |
| app/helper.c             | alpha    | 1.0     | MIT        |
| app/bridge.c             | beta     | 2.0     | Apache-2.0 |

폴더 요약 · 5행

| Path                    | OSS Name | Version | License    |
|-------------------------|----------|---------|------------|
| <b>vendor/alpha (3)</b> | alpha    | 1.0     | MIT        |
| <b>vendor/beta (2)</b>  | beta     | 2.0     | Apache-2.0 |
| app/main.c              | alpha    | 1.0     | MIT        |
| app/helper.c            | alpha    | 1.0     | MIT        |
| app/bridge.c            | beta     | 2.0     | Apache-2.0 |

app/: OSS가 달라 파일별 유지

기본은 폴더 요약 · 파일별 결과 유지: --no\_merge / SBOM 출력 시에는 요약하지 않음

2

## Source 분석 속도 개선

Source

v2.3.13 ~

불필요한 작업은 줄이고, 분석 자원은 더 효율적으로

1

### 불필요한 처리 줄이기

분석에서 제외할 파일을  
더 효율적으로 처리

2

### 병렬 처리 활용

파일 판별 작업을 나누어  
대규모 소스 분석 준비

3

### 분석 엔진 개선

개선된 ScanCode로  
라이선스 분석

개선 효과는 파일 구성과 실행 환경에 따라 달라집니다

## 외부 조회 안정성 개선

수집한 정보와 조회 상태를 함께 남깁니다

### SCANOSS

FingerPrint-OSS 정보 조회

→ 연결·호출 한도 점검  
오류가 나면 해당 조회를 건너뛴다 →

### LGE KB

FingerPrint-OSS 정보 조회

→ 서버 접근 여부 점검  
접속 불가 시 KB 조회를 건너뛴다 →

### Report

수집 정보  
+ 실행 상태

ScanCode·Manifest 결과와 결합하고, Cover 시트에도 조회 상태를 기록

선언된 메타데이터에서 라이선스 단서를 더합니다



입력은 달라도, 프로젝트에 맞는 경로로 분석합니다

## Python · uv.lock v4.1.55 ~

lockfile에 고정된 의존성 정보

uv.lock



패키지·의존 관계 직접 분석



설치·inspect 단계 생략

처리 실패 시 설치 환경 검사로 대체 가능

## .NET · NuGet CPM v4.1.27 ~

패키지 버전을 중앙에서 관리하는 프로젝트

.NET 프로젝트



필요 시 dotnet restore



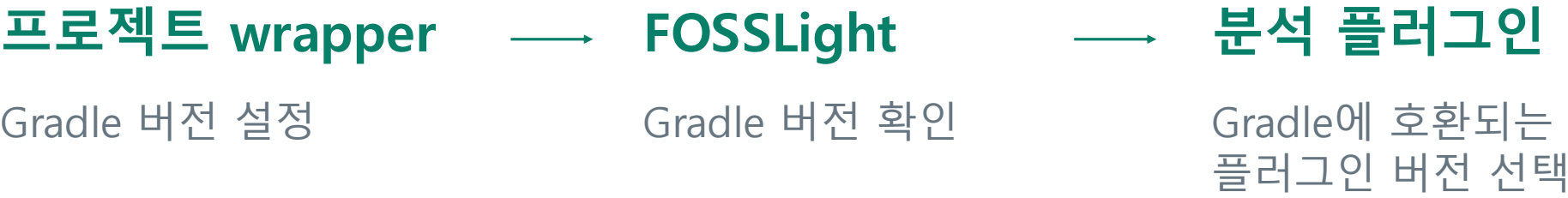
project.assets.json 분석

CPM 선언 파일이 아닌, restore 결과를 분석

## 6 Gradle 환경에 맞는 분석 플러그인 선택

Dependency  
v4.1.54 ~

Android 분석에서도 Gradle 9 환경에 대응합니다



Android 앱 분석 시 플러그인 선택

| 프로젝트의 Gradle 버전 | Android 분석 플러그인 |
|-----------------|-----------------|
| 9 미만            | v1.x            |
| 9 이상            | v2.x            |

일반 Gradle 프로젝트는 별도의 jk1.dependency-license-report 플러그인 사용

## 7 Gradle 의존성 구성 선택

Dependency

v4.1.58 ~

같은 프로젝트도 debug와 release의 의존성은 다릅니다

### Android 의존성 선언 예

| 선언                    | 가상 패키지          |
|-----------------------|-----------------|
| implementation        | core            |
| debugImplementation   | debug-tool      |
| releaseImplementation | release-feature |



### Runtime configuration별 의존성

| 구성 이름                   | 포함 패키지                  |
|-------------------------|-------------------------|
| debugRuntimeClasspath   | core<br>debug-tool      |
| releaseRuntimeClasspath | core<br>release-feature |

```
fossight_dependency -p ./android-project --runtime-config releaseRuntimeClasspath
```

파일 안의 메타데이터와 공개 저장소 정보를 조합합니다



취약점 정보는 **FOSSLight Hub**에서 확인

dependency-check에서 JAR 직접 분석·조회 방식으로 전환

## 출력 환경

Linux



Linux · Windows · macOS

## CycloneDX 1.6

JSON · XML

## SPDX 2.3

JSON · YAML · XML · TAG

SPDX 개선: 반영 예정

## 문서 포함 정보

### 1 식별

이름·버전·PURL·다운로드 위치

### 2 근거

파일·체크섬·라이선스·저작권

### 3 관계

패키지-파일 연결 · 의존 관계



**Questions?**

