Open Chain Korea Working Group

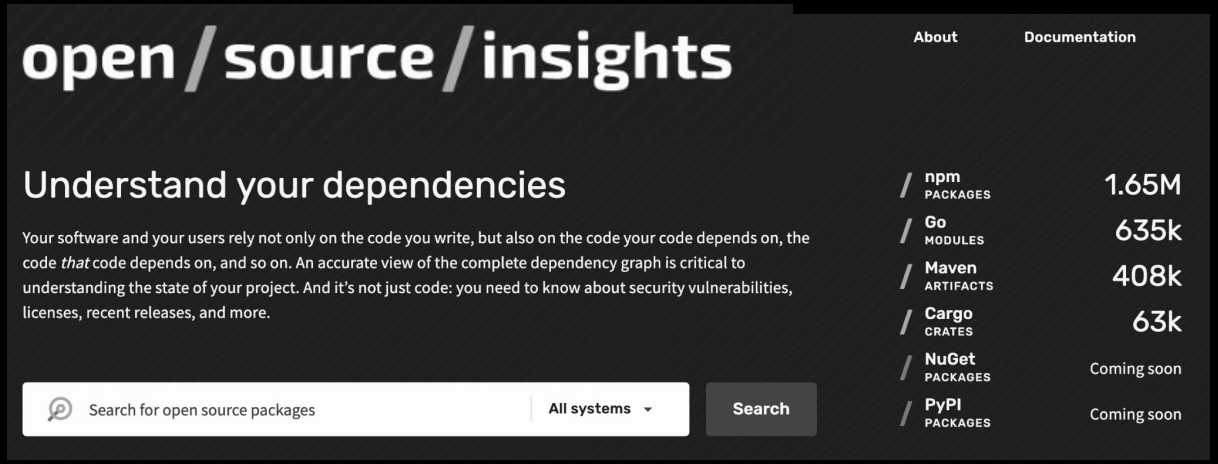
# Google OSV & Open Source Insight

Kakao 오픈소스 기술파트

robin.hwang (황민호)


https://osv.dev

오픈소스 취약성 정보 제공




https://deps.dev

오픈소스 BOM 제공


## Google OSV

- 기존에 CVE 와 Sonatype OSS Index 등을 통해서 취약성 데이터 베이스 확인
- 2021년 02월 05일 구글에서 오픈소스 보안 취약성 데이터 베이스 OSV를 공개
- 구글은 현재 OSS-Fuzz 프로젝트에서 발견한 데이터 세트를 제공
  * OSS-Fuzz : 소프트웨어 프로그래밍 오류를 발견하는 Fuzz Test 프로젝트
- CVE의 경우, 취약성 정보를 특정 패키지 버전에 매핑하기 어려운 경우가 많았음
- 취약성 표준(CPE/Common Platform Enumeration) 의 버전관리 체계가 오픈소스 버전 관리체계와 잘 맞지 않음
- 기존에 보고된 취약점이 있더라도 누락이 되는 문제 발생

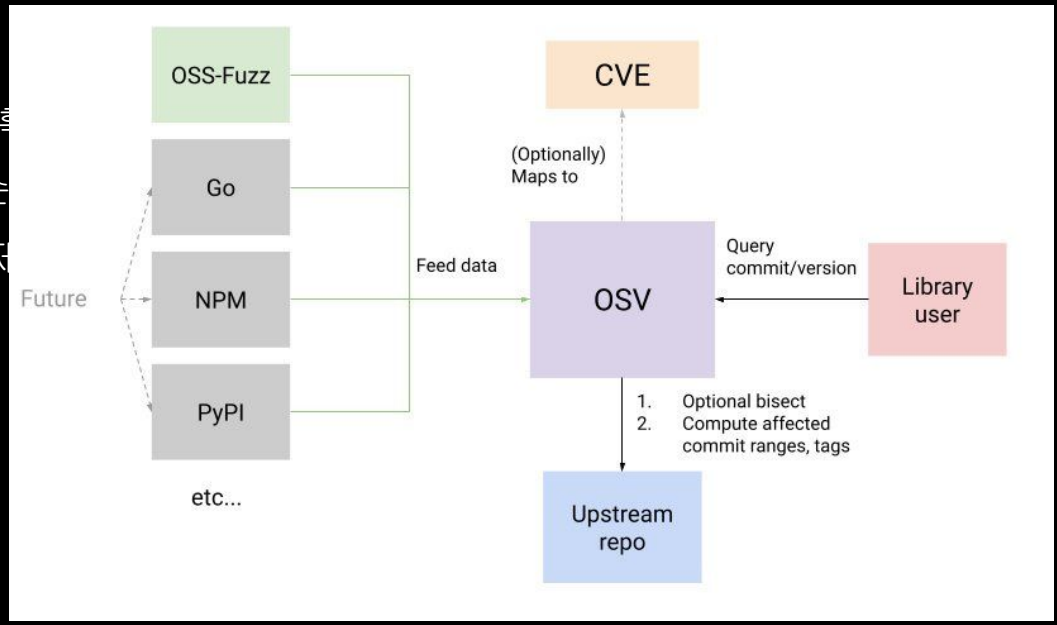

## OSV 목표

1. 관리자가 취약점을 보완하는데 필요한 작업을 줄입니다.
2. 쿼리하기 쉬운 데이터베이스에 정확한 취약성 메타데이터를 제공하여 다운 스트림 소비자에 대한 취약성 쿼리 결과를 정확하게 제공합니다.

OSV | Open Source Vulnerabilities

## OSV 자동화

- 영향을 받는 버전 및 커밋 목록을 정확하게 획
- 관리자의 보안 취약성 보고 프로세스를 단순
- 버그를 리포팅 하고 수정하는 커밋을 모두 저



OSV | Open Source Vulnerabilities

## OSV Workflow

1. 패키지 소비자는 패키지 버전 또는 커밋 해시를 입력으로 사용하여 OSV에 쿼리를 보냅니다.

```
curl -X POST -d \
'{ "commit" : "6879efc2c1596d11a6a6ad296f80063b558d5e0f" }'\
  'https://api.osv.dev/v1/query?key=$API_KEY'

curl -X POST -d \
'{ "version" : "1.0.0" , "package" : { "name" : "pkg" , "ecosystem" : "pypi" }'\
  ' https://api.osv.dev/v1/query?key=$API_KEY '
```

2. OSV는 특정 버전에 영향을 미치는 일련의 취약점을 조회하고 패키지에 영향을 미치는 취약점 목록을 반환합니다.
   취약성 메타 데이터는 기계가 읽을 수있는 JSON 형식으로 반환 됩니다.

3. 패키지 소비자는이 정보를 사용하여 보안 수정 (정확한 수정 메타 데이터 기반)을 선택하거나 최신 버전으로 업데이트합니다.


## OSV 관련 링크

- OSV UI & Demo : https://osv.dev
- OSV API (v1.0) : https://osv.dev/docs
- OSV GitHub : https://github.com/google/osv

- https://github.com/google/osv
- https://security.googleblog.com/2021/02/launching-osv-better-vulnerability.html
- https://www.dailysecu.com/news/articleView.html?idxno=120553

# open/source/insights

## Open Source Insight

- 2021년 06월 03일 Google 에서 Open Source Insight 서비스 공개
- 기존에 Google은 아마존, MS등과 함께 협업하여 clearlydefined 서비스를 제공
- 직관적인 UI로 서비스 구성
- 보안 취약성 정보를 연결
- 종속성 그래프도 제공
- Open SSF Score 도입

# open / source / insights

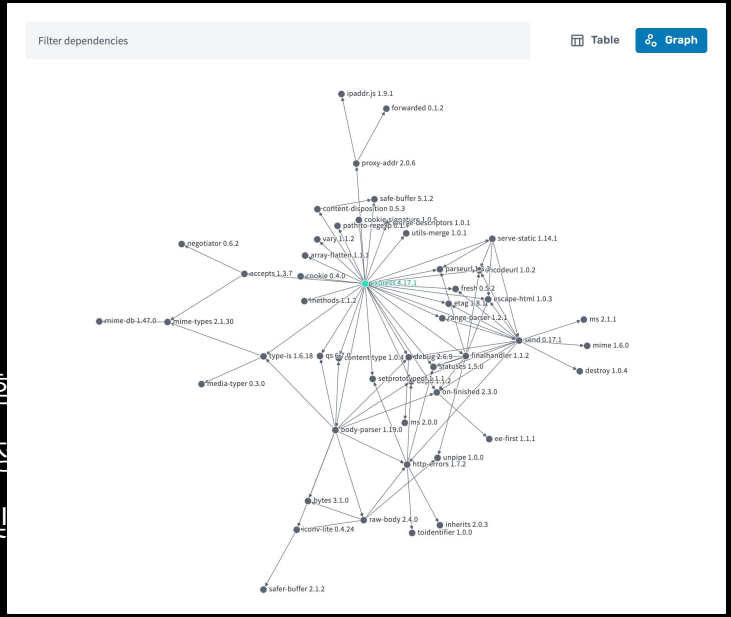
## Open Source Insight 목표 (FAQ)

- 생산적이고 안전하며 신뢰할 수 있는 오픈소스 소프트웨어 환경
- 많은 종속성으로 인해 유지관리가 어려움
- 개발자와 프로젝트 소유자에게 모든 종속성에 대한 정보를 통합
- 오픈소스 소프트웨어 프로젝트에 대한 고품질 정보 및 분석 정보

# open / source / insights

## Open Source Insight 차별점 (FAQ)

- 기존의 npm과 같은 일반적인 도구 세트를 대체하려는 시도는
- 패키징에 정의되어 있는 정보를 토대로 구성
  (lock 파일에 선언된 종속성과 다르거나 완전할 수 있음)
- Insight 가 제공하는 모든 정보를 동일하게 제공하는 서비스는
- 모든 패키징 시스템에 대해 가능한 동일한 분석 및 사용자 경험
- 종속성에 대한 세부 정보 뿐만 아니라 종속된 패키지에 대한 정
- 다양한 메타데이터를 통합하여 라이선스 문제, 보안 취약성 및
  관련 문제를 해결 할 수 있도록 함
- OpenSSF 적용




Open Chain KWG | kakao

open / source / insights

**Open Source Insight 얼마나 정확하고 최신인가? (FAQ)**

- 패키지에 대한 종속성을 계산하는 자체 알고리즘을 구현하였음
- 동일한 입력이 주어졌을때 결과는 99% 이상 신뢰를 가짐
- 다만, 버전 왜곡, 문서화되지 않았거나 모호한 패키징 정보, 사용 불가능한 빌드 시스템 입력 등의 요인에 의해 차이가 발생할 수 있음
- 일반적으로 최신 상태이며, 변경사항이 있을 시 한 시간 정도 이내로 업데이트 됨
- 사용자가 업데이트를 트리거 하는 시스템은 제공하지 않음