

FOSSLight Hub for 뉴비

LG전자 Open Source Task 민경선



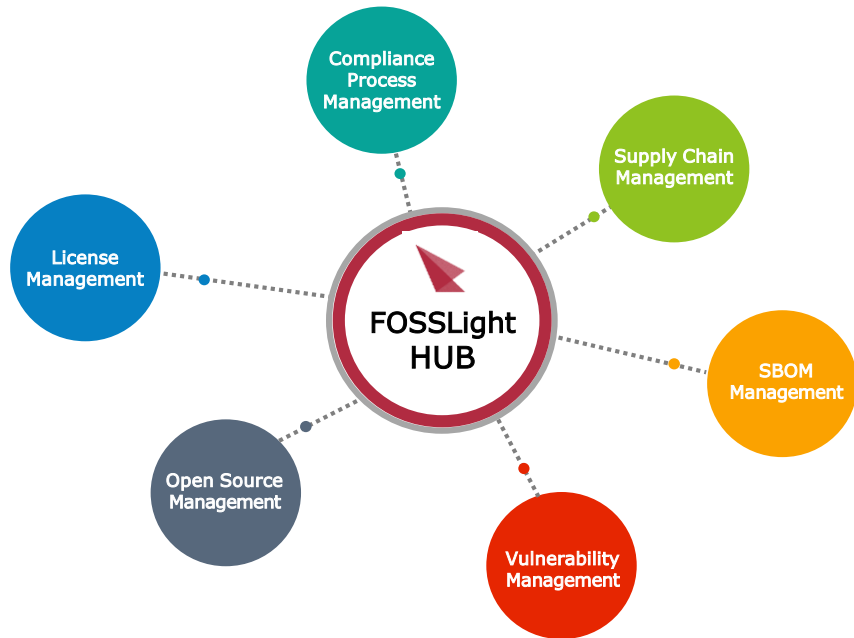
CONTENTS

- FOSSLight Hub 소개
- 설치 및 실행 방법
- Tips
- 시연

FOSSLight Hub

FOSSLight Hub

- 오픈소스 거버넌스를 위한 오픈소스 관리 도구



The screenshot shows the FOSSLight v1.4.5 web interface. The top navigation bar includes links for License List, OSS List, Project List, 3rd Party List, Vulnerability, and Self-Check List. The main content area features a search form with fields for ID, Project Name, Created Date, Division, Distribution Type, Status, Priority, OSS Name, OSS Version, License Name, Additional Information, Comment, and Binary Name. Below the search form is a table with columns for ID, Project Name (Version), Status, Identification, Packaging, Download, Distribution, Vulnerability, Division, Creator, Created Date, Updated Date, Reviewer, and Additional Information. The table contains 13 rows of data, including projects like 'fosslight_source_scanner', 'tuna_project', 'test_1 (ver 1.0.0)', 'mytest', 'Moo (ver 1.0.0)', 'webgoat (ver 8.2.0)', 'test-elle', '3rd party reg (ver 2)', 'copy test (ver 3)', 'mymytest (ver 1.0)', 'testttt (ver 4444)', 'testt (ver 2)', 'my test 211112', 'test download location', and 'PackingTest'.

FOSSLight Hub

오픈소스 및 라이선스 관리



- 오픈소스 정보 통합 관리
- 라이선스 의무사항 및 제약사항 확인
- 오픈소스 일괄 등록

컴플라이언스 프로세스 관리



- 올인원 오픈소스 컴플라이언스 수행
- 고지문 자동 생성 및 공개 소스코드 검증
- 이슈 트래킹

보안취약점 관리



- 보안취약점 조회
- 프로젝트별 보안취약점 모니터링 (자동 메일 알림)

사전점검



- 오픈소스 자동 분석
- 라이선스 자동 검출
- 라이선스 의무사항 및 보안취약점 알림

SBOM 관리



- 오픈소스 및 상용 소프트웨어 목록 관리
- 소프트웨어별 사용 프로젝트 검색
- SPDX 문서 지원 (ISO 표준)

공급망 관리

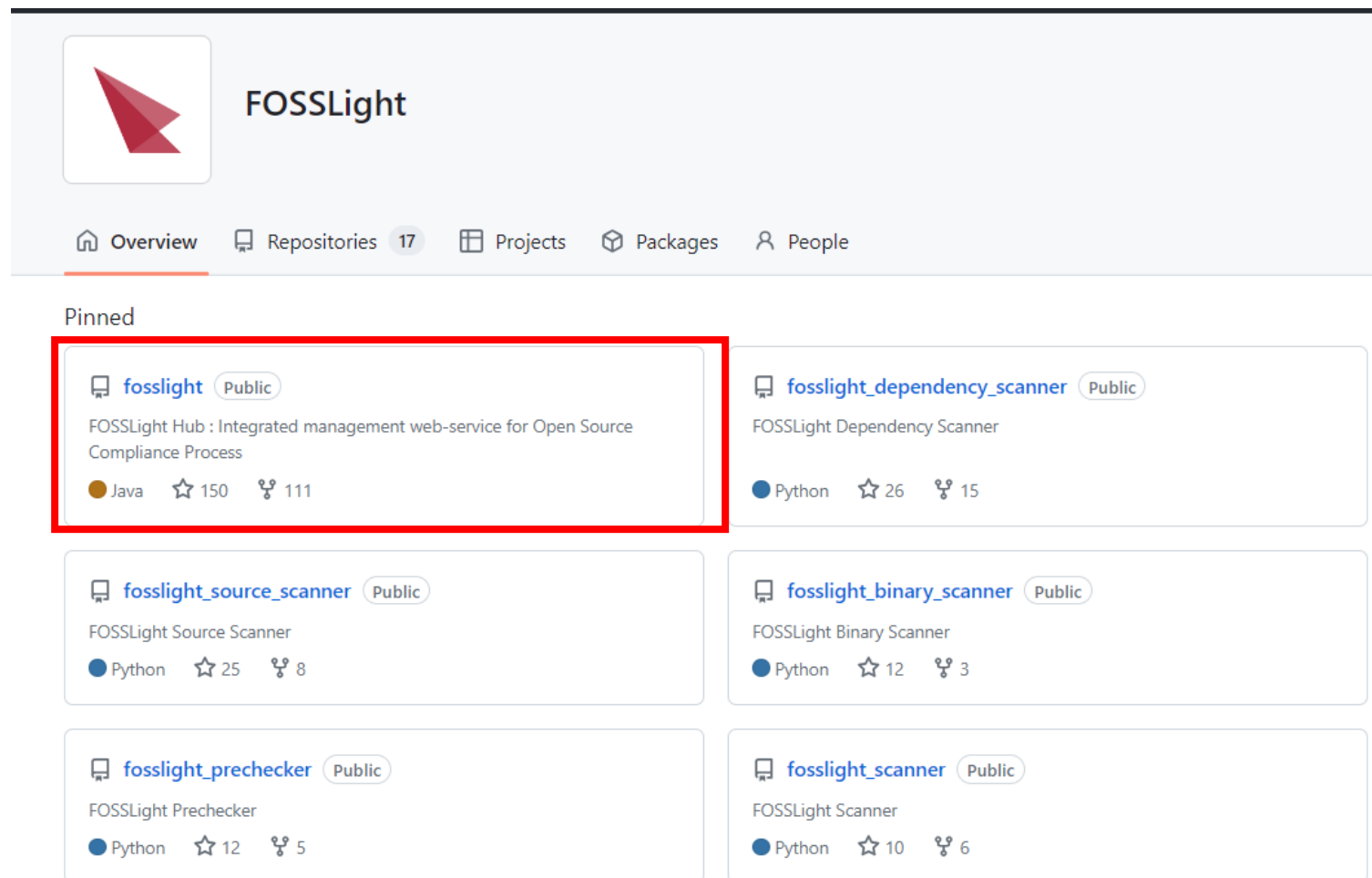


- 공급받은 타사 소프트웨어 관리
- 오픈 소스 확약서 관리
- 프로젝트 자동 연계

설치 및 실행 방법

설치 및 실행 방법

- FOSSLight Hub 소스 다운로드



The screenshot displays the GitHub profile page for FOSSLight. The profile header includes the FOSSLight logo and navigation tabs for Overview, Repositories (17), Projects, Packages, and People. Under the 'Pinned' section, several repositories are listed. The repository 'fosslight' is highlighted with a red border. It is a public repository for Java, with 150 stars and 111 forks. Other pinned repositories include 'fosslight_dependency_scanner' (Python, 26 stars, 15 forks), 'fosslight_source_scanner' (Python, 25 stars, 8 forks), 'fosslight_binary_scanner' (Python, 12 stars, 3 forks), 'fosslight_prechecker' (Python, 12 stars, 5 forks), and 'fosslight_scanner' (Python, 10 stars, 6 forks).

Repository Name	Language	Stars	Forks
fosslight	Java	150	111
fosslight_dependency_scanner	Python	26	15
fosslight_source_scanner	Python	25	8
fosslight_binary_scanner	Python	12	3
fosslight_prechecker	Python	12	5
fosslight_scanner	Python	10	6

설치 및 실행 방법 (Docker)

- Docker를 이용하여 빌드 및 실행 가능
- 개발 환경
 - Docker (<https://docs.docker.com/engine/install/>)
 - Docker Compose (<https://docs.docker.com/compose/install/>)
- 빌드 및 실행
 - `docker-compose up --build`

설치 및 실행 방법

- **요구사항**
 - JAVA 11 이상
 - MariaDB 10.0 이상 또는 MySql 5.6 이상
 - Memory 8GB+
- **개발 환경**
 - Framework : Spring Boot 2.1.x
 - Build Tool : Gradle 6.x
 - IDE : Spring Tool Suite
 - lombok 설치 필요 (<https://projectlombok.org/setup/eclipse>)
 - Project Character Set : UTF-8

설치 및 실행 방법

• 다운로드 & 설치

- JAVA를 설치 : <https://openjdk.java.net>
- DDL : [fosslight create.sql](#)
- MariaDB 또는 Mysql 설치 : <https://mariadb.org/download>
- Database 생성 및 초기 Data 등록
 - `mysql -u root -p < fosslight_create.sql`
 - 만약 Database가 이미 존재하거나 Database 이름을 변경하려면 상단의 create database 문과 USE 'fosslight' 문을 변경
 - `mysql -u root -p <DATABASE_NAME> < fosslight_create.sql`

-- fosslight 데이터베이스 구조 내보내기

```
CREATE DATABASE IF NOT EXISTS `fosslight` DEFAULT CHARACTER SET utf8mb4;
```

```
USE `fosslight`;
```

- 접속 계정이 이미 존재하거나, 다른 계정을 사용하는 경우 CREATE USER 및 GRANT 부분을 삭제(또는 변경)

```
CREATE USER IF NOT EXISTS 'fosslight'@'%' IDENTIFIED BY 'fosslight';
```

```
CREATE USER IF NOT EXISTS 'fosslight'@'localhost' IDENTIFIED BY 'fosslight';
```

```
GRANT ALL PRIVILEGES ON fosslight.* TO 'fosslight'@'%';
```

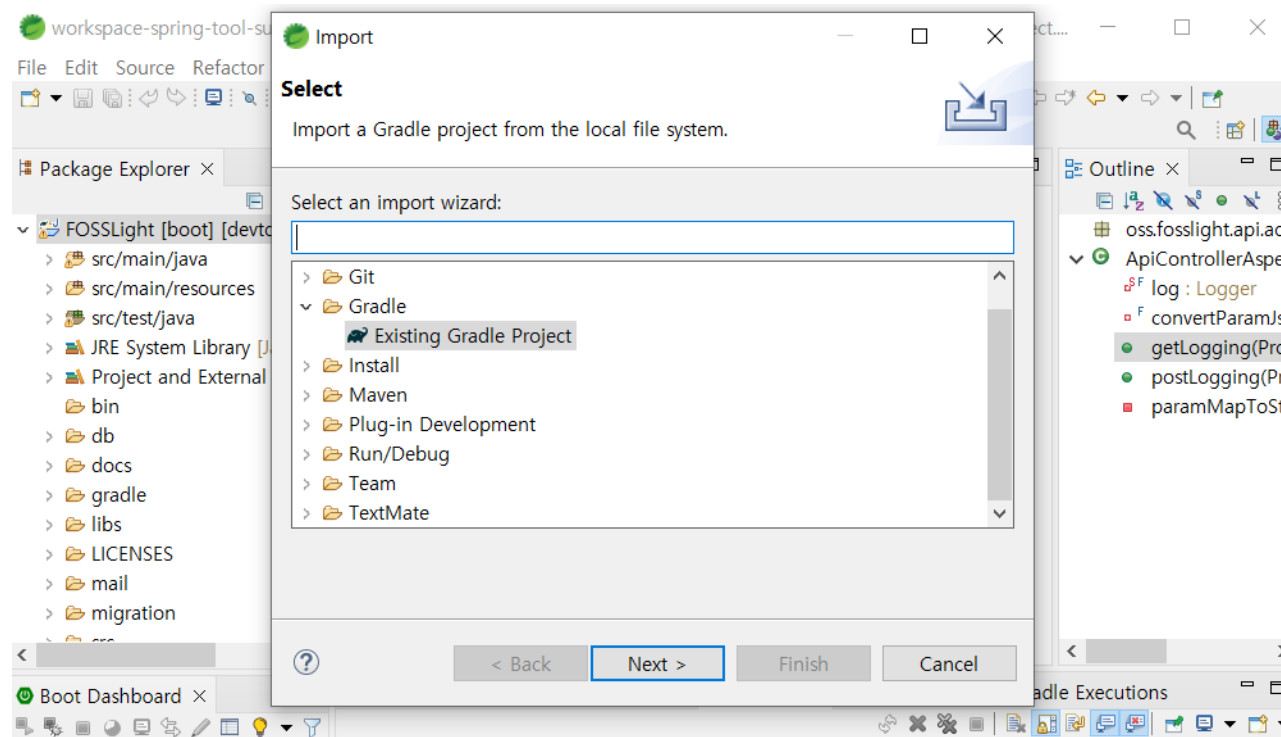
```
GRANT ALL PRIVILEGES ON fosslight.* TO 'fosslight'@'localhost';
```

```
FLUSH PRIVILEGES;
```

설치 및 실행 방법

• IDE Configuration

- [Spring Tool Suite](#)를 다운로드
※ STS (Spring Tool suite) 4.x 기준
- lombok 설치: <https://projectlombok.org/setup/eclipse>
- File > Import > Gradle > Existing Gradle Project
- [Git Source Directory](#)를 설정하고 Import
- Project > Properties > Resource > Text file encoding에서 UTF-8로 설정



설치 및 실행 방법

• 실행 옵션 세팅

application.properties 파일

```

5  spring.profiles.active=local
6  server.port=8180
7
8  # View Configuration
9  spring.mvc.view.prefix=/WEB-INF/
10 spring.mvc.view.suffix=.jsp
11 spring.servlet.multipart.max-file-size=4
12 spring.servlet.multipart.max-request-size=4
13 server.servlet.session.timeout=10800s
14
15 spring.main.allow-bean-definition-overriding=true
16 spring.main.allow-circular-references=true
17
18 server.tomcat.max-http-form-post-size=-1
19 server.tomcat.max-swallow-size=-1
20
21 spring.cache.jcache.config=classpath:ehcache.xml
22
23 server.servlet.encoding.charset=UTF-8
24
25 spring.datasource.driver-class-name=org.mariadb.jdbc.Driver
26 spring.datasource.url=127.0.0.1:3306/fosslight
27 spring.datasource.username=fosslight
28 spring.datasource.password=fosslight
29

```

- **server.port** : 웹 서버 포트 (8180으로 설정한 경우 <http://localhost:8180>)
- **spring.datasource.url** : FOSSLight Hub Database가 설치되어있는 서버의 IP, Port, Database Name 설정
- **spring.datasource.username** : Database 접속자명 설정
- **spring.datasource.password** : Database 접속자 패스워드 설정

설치 및 실행 방법

• 실행 옵션 세팅

application.properties 파일

```

43 logging.level.root=info
44 logging.level.org.apache.*=error
45 logging.level.sun.rmi.*=error
46 logging.level.org.quartz.*=error
47 logging.level.oss.fosslight.*=info
48 logging.path=./logs
49 logging.file=fosslight
50
51 spring.banner.location=classpath:ba
52
53 secret.key=\$2a\$10\$nSPm7WPvj6GsrJ
54 token.secret.key=\$2a\$10\$3fTAdBgolJwCkDlHcIQyNe/9LMqlI81u.q52n5z9TxS8v0Kaa.6Uu
55
56 checkFlag=
57 nvd.nist.gov.api.key=0dc1b6f1-8d0c-454f-b4f8-be97c2327b3e
58 nvd.scheduled.cron.value=0 0 18 * * ?
59
60 root.dir=./service
61 upload.path=\${root.dir}/upload
62 packaging.path=\${upload.path}/packaging
63 export.template.path=\${root.dir}/template
64 notice.path=\${root.dir}/notice
65 reviewReport.path=\${root.dir}/reviewReport
66 internal.url.dir.path=/docx/license

```

- **logging.path** : 로그파일 출력 경로 설정
(Default "./logs"는 application 실행 위치를 의미)
- **logging.file** : 로그를 출력할 로그 파일명
- **root.dir** : 파일 업로드, 다운로드 최상위 경로를 의미

설치 및 실행 방법

- **Build & Run**

- Build (war 파일 생성)
 - ./gradlew build
- Run
 - ./gradlew bootRun
- Build & run
 - ./gradlew clean build && java -jar build/libs/FOSSLight-[version].war

- **동작 확인**

- 웹브라우저에서 <http://localhost:8180>으로 접속
- 초기 로그인 계정은 id : admin, password: admin

Tips

DB 버전 업그레이드 Tip

- [MyBatis Migrations](#)를 이용하여 DB 버전을 업그레이드
 - v1.5.0부터 migration하는 script를 제공
- migration/migration/environments/development.properties 파일에 DB 접속 정보를 수정

```
$ cd migration/migration
$ cat environments/development.properties
## Base time zone to ensure times are consistent across machines
time_zone=GMT+0:00

## The character set that scripts are encoded with
# script_char_set=UTF-8

## JDBC connection properties.
driver=org.mariadb.jdbc.Driver
url=jdbc:mysql://localhost:3306/fosslight
username=fosslight
password=fosslight
```


DB 버전 업그레이드 Tip

- fosslight/migration/mybatis-migrations-3.3.11 폴더를 MIGRATIONS_HOME로 export

```
$ cd fosslight
$ pwd
$ /home/test/fosslight
$ export MIGRATIONS_HOME=/home/test/fosslight/migration/mybatis-migrations-3.3.11
$ export MIGRATIONS=$MIGRATIONS_HOME/bin
$ export PATH=$MIGRATIONS:$PATH
```

DB 버전 업그레이드 Tip

- migrate status를 확인 후 업그레이드

```
$ cd /home/test/fosslight/migration/migration
```

```
$ migrate status
```

```
-----  
-- MyBatis Migrations - status  
-----
```

ID	Applied At	Description
20230322085317	...pending...	create changelog
20230322091138	...pending...	update v1.4.9
20230322092534	...pending...	update v1.5.0

```
-----  
-- MyBatis Migrations SUCCESS  
-- Total time: 0s  
-- Finished at: Wed Mar 22 20:12:07 KST 2023  
-- Final Memory: 7M/500M
```

```
$ migrate up
```

DB 버전 업그레이드 Tip

- 버전 업그레이드 진행 되었는지 확인

```
$ migrate status
-----
-- MyBatis Migrations - status
-----
ID                Applied At        Description
=====
20230322085317    2023-03-22 20:12:35 create changelog
20230322091138    2023-03-22 20:12:35 update v1.4.9
20230322092534    2023-03-22 20:12:36 update v1.5.0
-----

-- MyBatis Migrations SUCCESS
-- Total time: 0s
-- Finished at: Wed Mar 22 20:12:39 KST 2023
-- Final Memory: 7M/500M
-----
```

NVD Data 세팅 Tip

- NVD(National Vulnerability Database)에서 제공되는 [NVD Data Feeds](#)
- FOSSLight Hub 내 Vulnerability List에서 Open Source의 보안 취약점 존재 여부 및 관련 정보 (CVE ID, CVSS Score) 확인

Vulnerability List

Vulnerability

OSS Name Exact Match OSS Version CVE ID

	OSS Name	Nickname	OSS Version	Max CVSS Score
	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	>= <input type="text"/> x
1	tomcat		9.0.9	▲
2	tomcat		9.0.8	▲
3	tomcat		9.0.7	▲
4	tomcat		9.0.6	▲
5	tomcat		9.0.5	▲
6	tomcat		9.0.41	▲
7	tomcat		9.0.40	▲
8	tomcat		9.0.4	▲
9	tomcat		9.0.39	▲
10	tomcat		9.0.38	▲
11	tomcat		9.0.37	▲
12	tomcat		9.0.36	▲
13	tomcat		9.0.35-3.57.3	▲
14	tomcat		9.0.35-3.39.1	▲
15	tomcat		9.0.35	▲

Page 1 of 15 View 1 - 15 of 214

NVD Data 세팅 Tip

- 일 1회 [NVD Data Feeds](#)를 다운로드하여 Database에 저장
 - 최근 한달 전 변경된 데이터를 취득하여 반영
- 2002년 Data부터 NVD Data를 다운로드 받을 경우 아래와 같이 세팅
 - 최초 1회만 세팅하면 이후 Data는 누적되므로 추가 세팅이 필요 없음

- **DB에서 설정값 변경**

```
UPDATE T2_CODE_DTL SET CD_DTL_NM = 'Y' WHERE CD_NO = '990' AND CD_DTL_NO = '100';
```

- NVD Data Feed initialize flag Code의 Default 값은 "N" 으로 설정
- "Y"로 변경시 다음 NVD 스케줄 동작 시 모든 NVD Data를 Clean하고 2002년 Data 파일 부터 순차적으로 등록 처리
- 해당 값은 NVD Data 초기화 수행 시 에러 여부와 상관 없이 Default 값 ("N") 으로 변경

Simple NVD Data 세팅 Tip

- 전체 NVD Data 세팅 시간이 부담인 경우
- 개발용으로 NVD Data 일부만 빠르게 필요한 경우

Simple NVD Data 세팅 Tip

- 개발용으로 Data 일부만 Sync하여 사용
 - 하루 전 변경된 데이터를 취득하여 반영

src/main/java/oss/fosslight/scheduler/SchedulerWorkerTask.java

```

74 // 새벽 12시 스케줄 - CPE Dictionary, CVE Update Data Sync
75 @Scheduled(cron="${nvd.scheduled.cron.value}")
76 // @Scheduled(fixedDelay=1000)
77 public void nvdDataIfJob() {
78     String resCd = "";
79     try {
80         resCd = nvdService.executeNvdDataSync();
81
82         if (resCd == "00") {
83             vulnerabilityService.doSyncOSSNvdInfo();
84             log.info("nvdDataIfJob end");
85         } else {
86             log.error("executeNvdDataSync - resCd : " + resCd);
87         }
88     } catch (IOException ioe) {
89         log.error(ioe.getMessage() + " (resCd : " + resCd + ")", ioe);
90     }
91 }

```

application.properties 파일

```

56 checkFlag=
57 nvd.nist.gov.api.key=0dc1b6f1-8d0c-454f-b4f8-be97c2327b3e
58 nvd.scheduled.cron.value=0 0 18 * * ?
59

```

Scheduler 동작 시간 설정

Simple NVD Data 세팅 Tip

src/main/java/oss/fosslight/service/NvdDataService.java

```

144         if (!initializeFlag) {
145             Date today = new Date();
146             SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss.SSS");
147             sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
148
149             Calendar cal = Calendar.getInstance();
150             cal.setTime(today);
151             cal.add(Calendar.HOUR, -1);
152
153             String endTime = sdf.format(cal.getTime());
154
155             Calendar mon = Calendar.getInstance();
156             mon.add(Calendar.MONTH, -1);
157             String startTime = sdf.format(mon.getTime());
158
159             lastModStartDate = startTime + "%2B01:00";
160             lastModEndDate = endTime + "%2B01:00";
161         }
162

```

mon.add(Calendar.DATE, -1)

하루 전 data 를 가지고 오는 것으로 변경
* sync 기간은 설정 할 수 있음

Mail 서버 세팅 Tip

application.properties 파일

```
80     spdx.default.url=  
81  
82     external.service.useflag=N  
83     external.service.github.token=  
84  
85     mail.smtp.useflag=N  
86     mail.smtp.host=  
87     mail.smtp.port=587  
88     mail.smtp.email=  
89     mail.smtp.username=  
90     mail.smtp.password=  
91     mail.smtp.encoding=UTF-8  
92  
93     smtp.default.bcc=  
94     smtp.default.admin=  
95     smtp.default.bat=  
96     smtp.default.security=  
97
```

폐쇄망 사용시 제약사항 Tip

- **Vulnerability 정보**

- NVD Data Rest Api (<https://services.nvd.nist.gov/rest/json/cpematch/2.0>, <https://services.nvd.nist.gov/rest/json/cves/2.0>) 를 통해 response 된 "JSON Data" 를 취합하여 변경 사항을 저장
- 폐쇄망에서는 NVD Data Feeds를 가지고 올 수 없음

- **Check License Name**

- 위치 : Project, 3rd party, Self-check
- 기능 : Download location, OSS name, OSS version을 기반으로 검출된 License를 확인 가능
 - 1순위 : FOSSLight Hub DB 검색
 - 2순위 : ClearlyDefined와 Github에서 License 검색
- 폐쇄망에서는 2순위 검색이 되지 않음

시연



Thank You!

