

# FOSSLight 소개 및 사용 가이드

LG전자 민경선



LG Open Source

# CONTENTS

---

- FOSSLight의 역사
- FOSSLight Scanner
- FOSSLight Hub

# FOSSLight의 역사

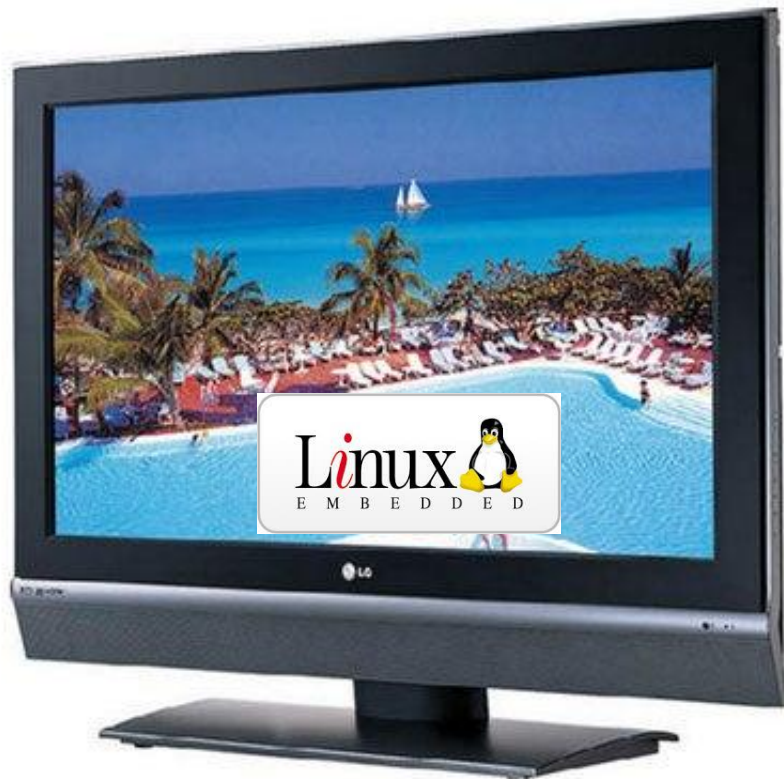
2006



Embedded Linux TV



# 2006 – Embedded Linux



## OPEN SOURCE SOFTWARE NOTICE

The following GPL executables and LGPL/MPL libraries used in this product are subject to the GPL/LGPL/MPL License Agreements:

### GPL EXECUTABLES:

- Linux kernel 2.6.11
- busybox

### LGPL LIBRARIES:

- glibc

### MPL LIBRARIES:

- Nanox

LG Electronics offers to provide source code to you on CD-ROM for a charge covering the cost of performing such distribution, such as the cost of media, shipping and handling upon e-mail request to LG Electronics at: [Opensource@lge.com](mailto:Opensource@lge.com)

This offer is valid for a period of three(3) years from the date of the distribution of this product by LG Electronics.

You can obtain a copy of the GPL, LGPL and MPL licenses on the CD-ROM provided with this product.

- This software is based in part on the work of the Independent JPEG Group.
- This software includes the Zlib compression library, developed by Jean-loup Gailly and Mark Adler. Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

# FOSSLight의 역사

BUSYBOX  
  
BusyBox Lawsuit

2006



Embedded Linux TV



2009



2009

기사 주소: [http://www.dt.co.kr/contents.html?article\\_no=20091217020108607440](http://www.dt.co.kr/contents.html?article_no=20091217020108607440)

## TV · 셋톱박스 저작권 위반 '피소'

박상훈 기자 [nanugi@dt.co.kr](mailto:nanugi@dt.co.kr) | 입력: 2009-12-16 20:34

## SFSLC, 14개업체 제조... 오픈소스 라이선스 관리 시급

삼성전자, 휴맥스 등 국내 대표 가전 업체들이 잇달아 오픈소스 저작권 위반으로 소송에 휘말리고 있어 수출의 걸림돌로 작용할 수 있다는 우려가 나오고 있다.

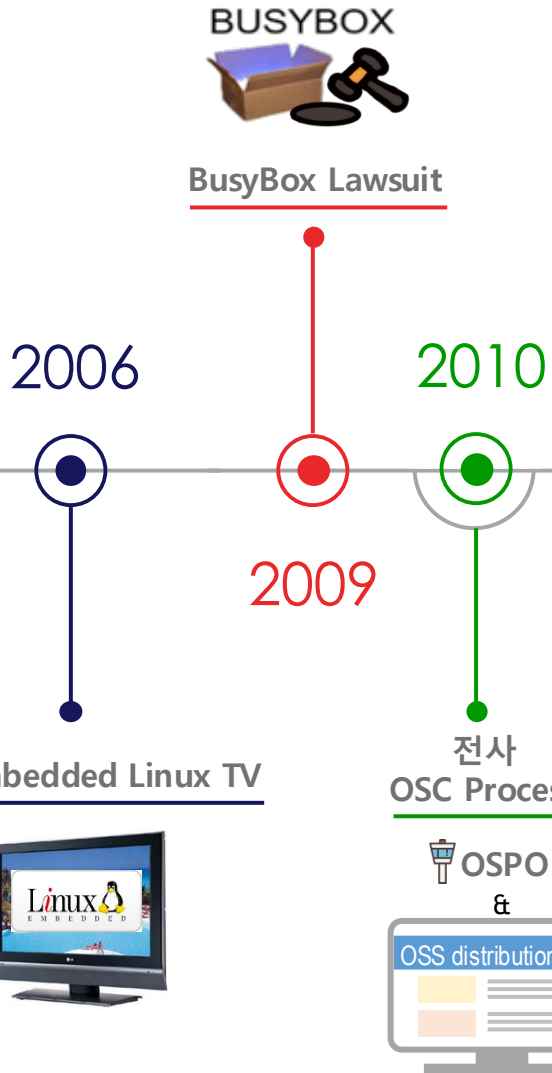
소프트웨어자유법률센터(SFSLC)는 14일(현지시간) 뉴욕 남부 지방법원에 삼성전자를 비롯한 14개 업체를 저작권 위반으로 제소했다. SFSLC는 오픈소스 개발자들을 법률적으로 지원하는 비영리 단체로, 이번 소송은 리눅스 툴 패키지인 '비지박스(BusyBox)'의 개발자를 대신해 법적 대응에 나서는 형태를 취하고 있다.

SFSLC는 소장을 통해 삼성전자, 휴맥스 등이 HDTV, 셋톱박스용 소프트웨어를 개발하면서 '비지박스'를 사용했지만 소스코드를 공개하지 않아 'GPL 버전2' 라이선스를 위반했다고 주장했다. SFSLC는 삼성전자의 LCD HDTV인 LN52A650와 LA26A450, 휴맥스의 HDTV DVR 제품인 'iCord HD' 등을 언급하며 여기에 사용된 소프트웨어(SW)의 소스코드 공개와 함께 이들 제품의 판매금지, 이익배분, 손해배상 등을 요구했다.

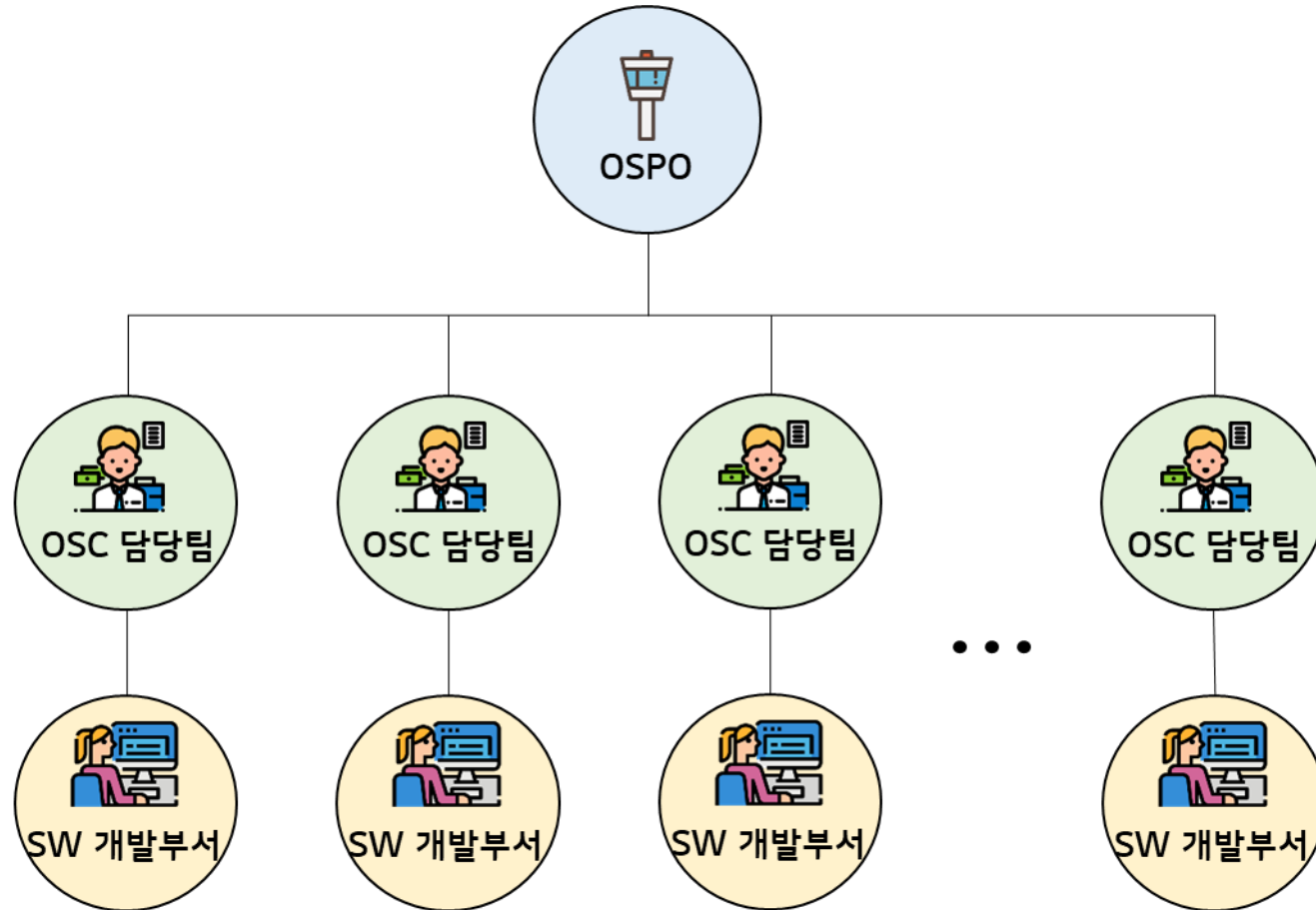
소송 소식이 알려지자 전문가들은 '올 것이 왔다'는 반응이다. 그동안 우리나라는 오픈소스를 폭넓게 활용하는 대표적인 수혜국으로 알려져 왔지만 정작 라이선스 관리에 대해서는 사각지대에 머물러 있었다. 실제로 삼성전자는 지난 8월 셋톱박스 SW 관련 오픈소스 저작권 위반 소송에 휘말린 데 이어 이번에 또 소송을 당했다.

이번에 문제가 된 LN52A650는 '보르도'란 브랜드로 더 널리 알려진 제품으로, 삼성전자가 TV 판매 40년 만에 세계 TV 시장 1위로 올라서는데 결정적인 역할을 했다는 평가를 받고 있다. 'iCord HD' 역시 휴맥스의 유럽 시장 공략의 1등 공신으로 평가받

# FOSSLight의 역사

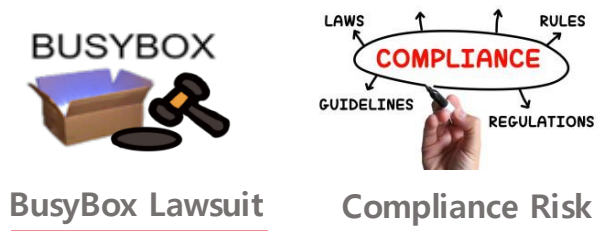


# 2010 – 전사 OSC Process





# FOSSLight의 역사



BusyBox Lawsuit

Compliance Risk

2006

2010

2009

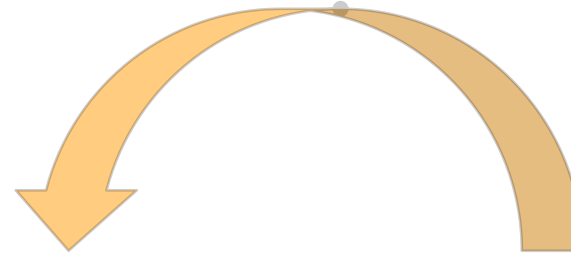
2011

Embedded Linux TV

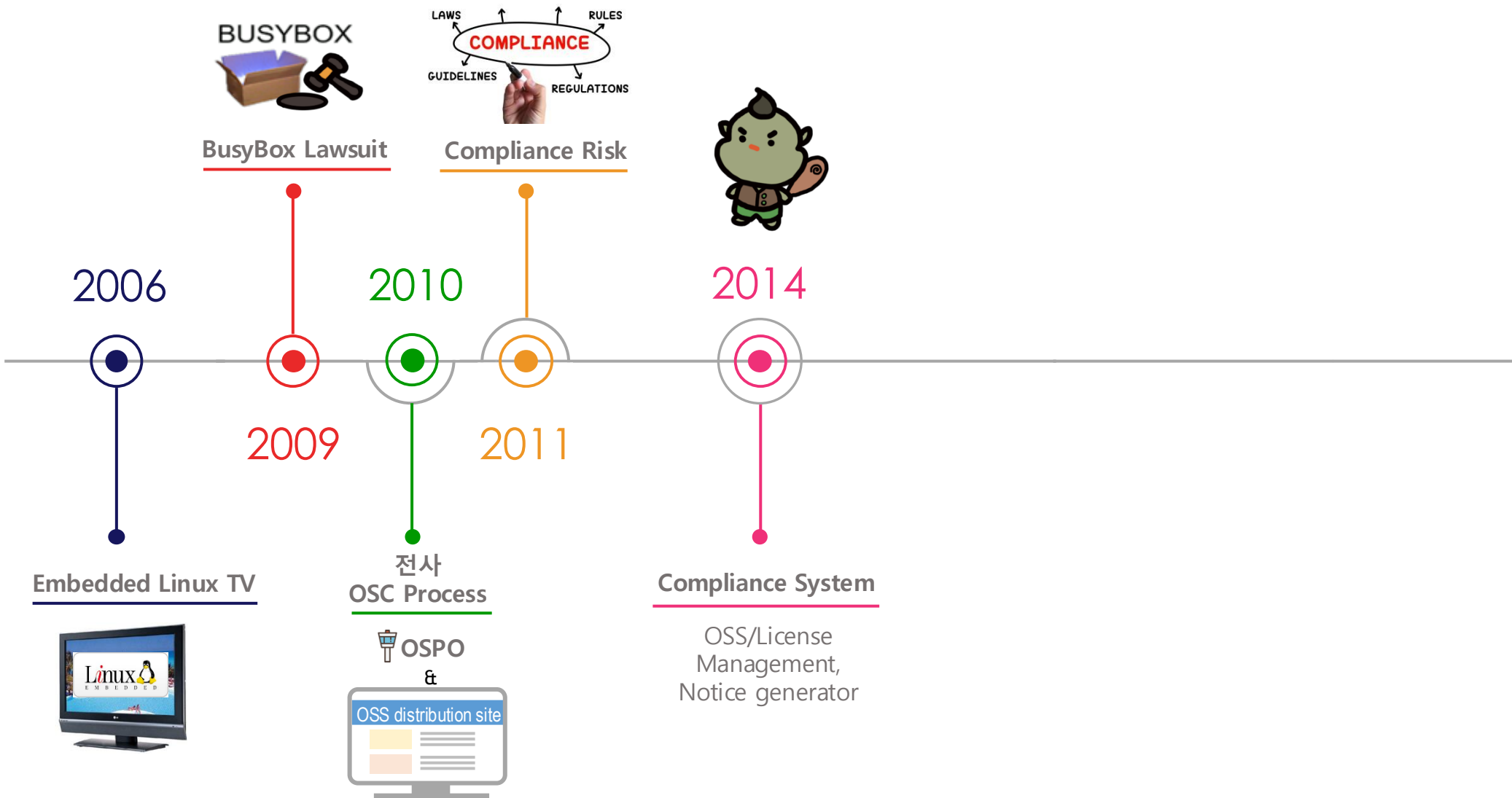
전사  
OSC Process



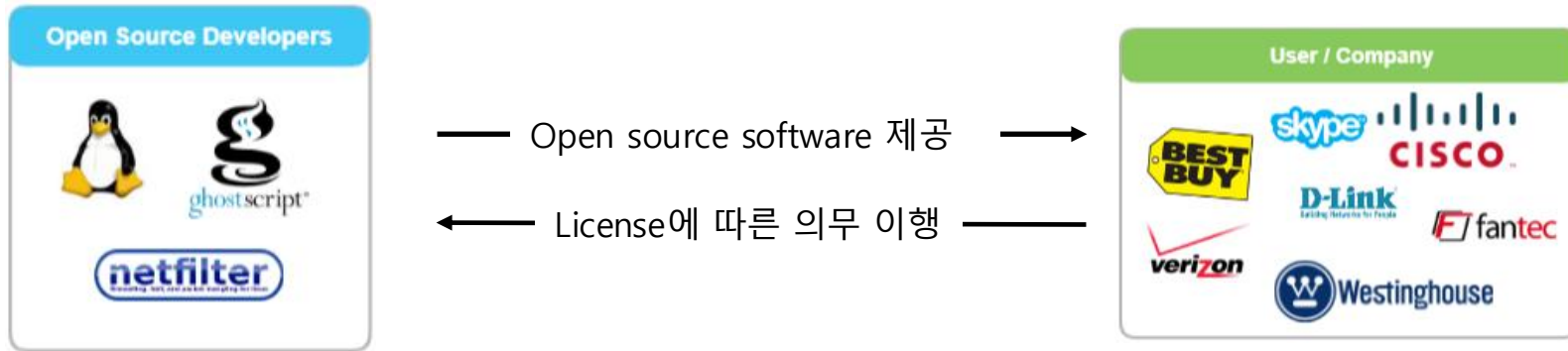
# 2011 – Compliance Risk



# FOSSLight의 역사



# 2014



직접 Legal Claim 제기하는 경우도 발생



# 2014 – Compliance System

SMART OSS NOTICE SYSTEM
General User | Logout

- ★ 1. Open Source Software
  - ★ 1.1 Open Source Software List
  - ★ 1.2 Open Source License List
- ★ 2. OSS Notice 1
  - ★ 2.1 Search
  - ★ 3.1 Search
  - ★ 3.2 Create
- ★ 3. OSS Analysis Report
  - ★ 3.1 Search
  - ★ 3.2 Create
- ★ 4. Package Verification
  - ★ 4.1 Search
  - ★ 4.2 Create
  - ★ 4.3 Package File Export Tool
- ★ 5. Binary Information
  - ★ 5.1 Binary Search
  - ★ 5.2 Build Image Sheet Export

OSS Notice Search

Product/SW Type :  Model/SW Name :  OSS Notice Id :  Creator : ALL

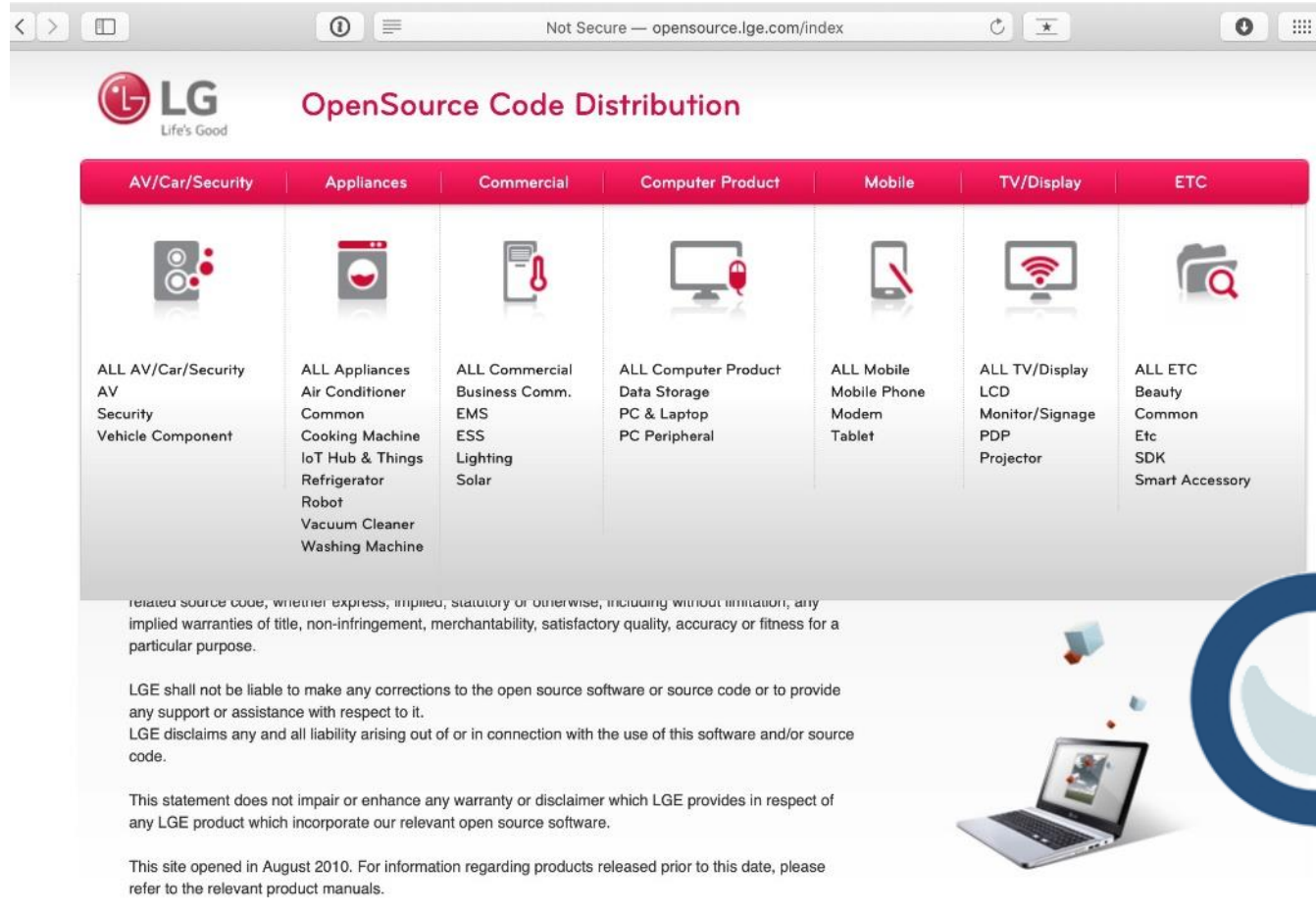
Type : All  Status : All  OSS Name :  Comment :

Req. Department : All  Requestor :   All Create Date : 2015/07/07 ~ : 2015/08/06

ID	Report	Notice	Html	Status	Type	Req. Division	Product / SW Type	Model / SW Name	Requestor	Creator	Update Date	Analysis Ic
2220						CTO / CI Center	Android application	SwingShot for Android	O' 백승주	박원재	15-08-05 17:07	--
2218						MC	Smart Phone	VS820	O' 정지연	황병주	15-08-04 15:09	--
2215						MC	Mobile Phone	LGX150	O' 한일희	황병주	15-08-03 11:05	--
2214						MC	Mobile Phone	LGX155	O' 한일희	최혜성	15-07-31 14:10	--
2211						H&A Aircon	Android Application	LG SIMs2.0(BlackBox) for Android	O' 이혜경	장학성	15-07-31 11:18	--
2210						HE / PC	Application	LG Face-In 2	O'	최혜성	15-07-31 09:48	--
2207						VC / IVI	AV Navigation	LAN5020KKJF	-- 이혜규	황병주	15-07-31 09:18	--
2202						HE / PC	PC Windows application program	olleh tv	O' 조동한	최혜성	15-07-29 14:21	--

14

# 2014 – Compliance System



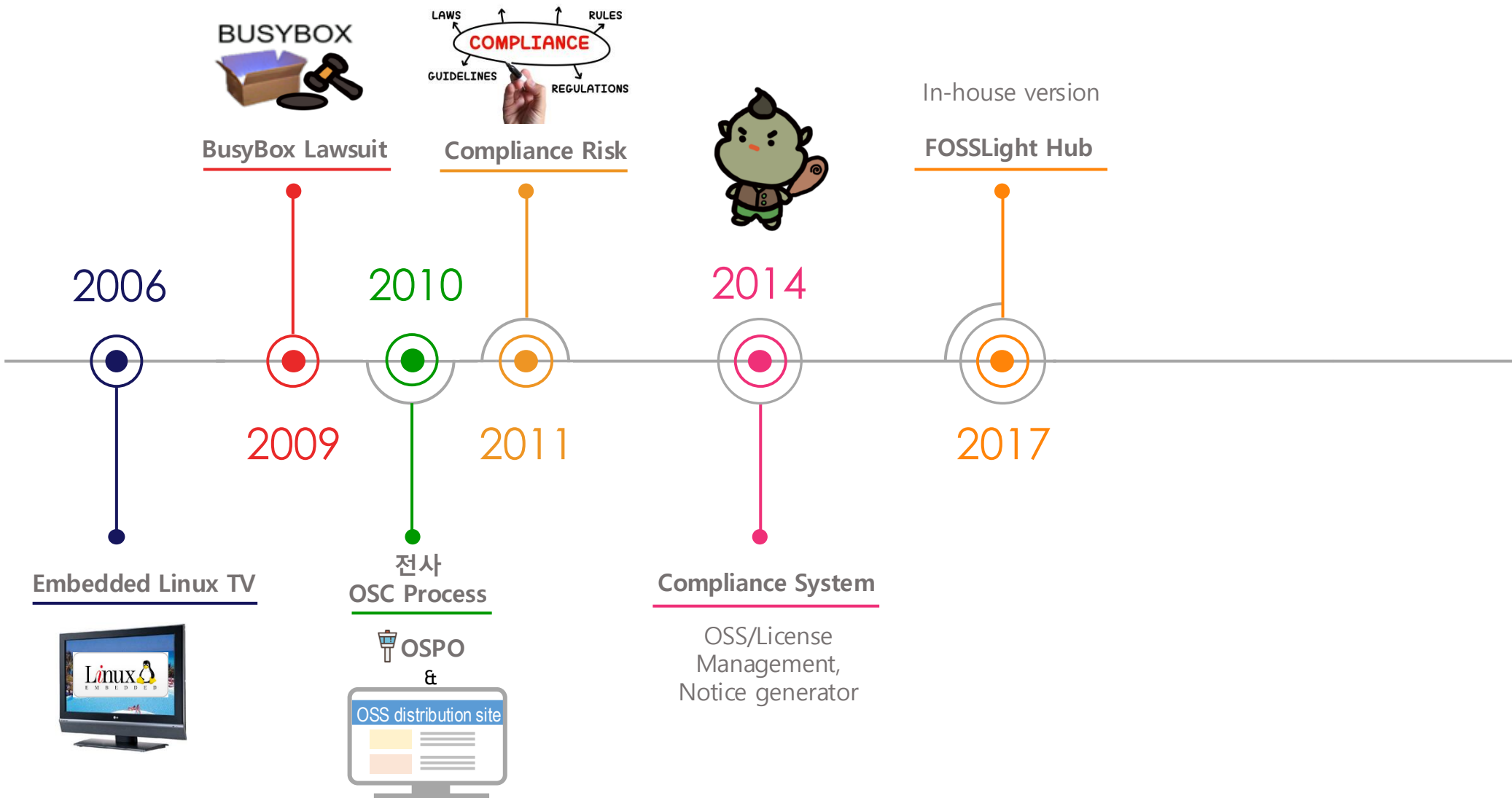
related source code, whether express, implied, statutory or otherwise, including without limitation, any implied warranties of title, non-infringement, merchantability, satisfactory quality, accuracy or fitness for a particular purpose.

LGE shall not be liable to make any corrections to the open source software or source code or to provide any support or assistance with respect to it.  
LGE disclaims any and all liability arising out of or in connection with the use of this software and/or source code.

This statement does not impair or enhance any warranty or disclaimer which LGE provides in respect of any LGE product which incorporate our relevant open source software.

This site opened in August 2010. For information regarding products released prior to this date, please refer to the relevant product manuals.

# FOSSLight의 역사



2006

Embedded Linux TV



BusyBox Lawsuit

2009

2010

전사 OSC Process



Compliance Risk

2011



2014

Compliance System

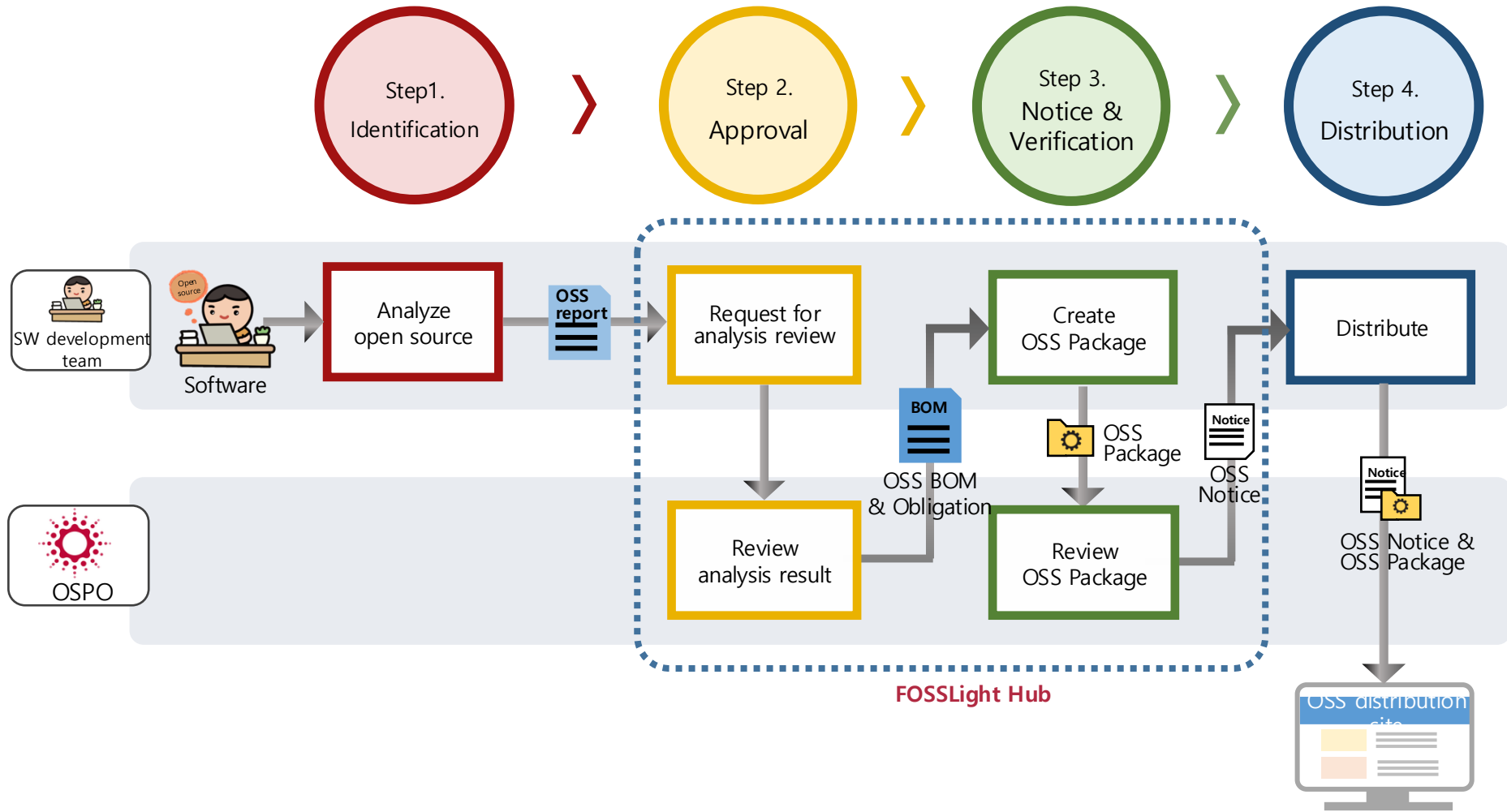
OSS/License Management, Notice generator

In-house version

FOSSLight Hub

2017

# 2017 – FOSSLight Hub



# 2017 – FOSSLight Hub

osc.lge.com/index

**FOSSLIGHT**

일반석지영 | Logout

Dashboard > License List > OSS List > **Project List** > 3rd Party List > BAT List > Binary DB > Vulnerability > Self-Check List > Compliance Status > Model(S/W) OSC Status > 3rd Party Status > External Link >

Project List

ID:  Project Name:  Created Date:  ~  **Search**

Division:  Creator:  Reviewer:

Distribution Type:  Network Service:  Model Name:

Status:  Progress  Request  Review  Complete  Drop

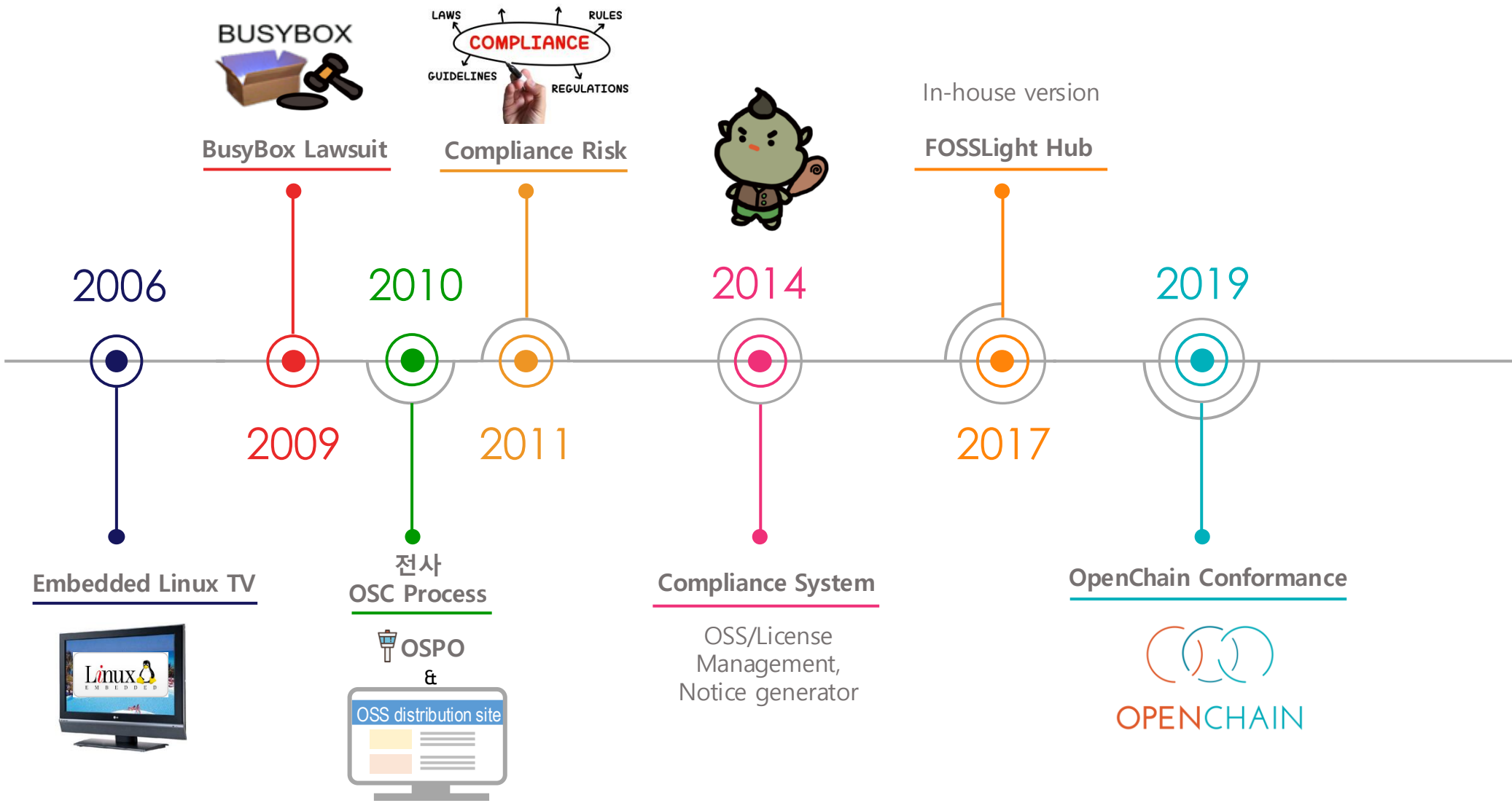
Priority:  View My Projects Only:

Expand

Copy Change Status BOM Compare Excel download Add

ID	Project Name (Version)	Status	Identification	Packaging	Distribution	Download	Distribution Type	Vulnerability	Division	Creator	Created Date	Updated Date	Reviewer	Additional Information
3785		R	Request 3rd SRC BIN BOM				General Model	Warning			2021-08-24	2021-08-24		특미 ThinQAp
3784		P	Progress 3rd SRC BIN BOM				General Model	Warning			2021-08-23	2021-08-23		
3783		P	Progress 3rd SRC BIN BOM				General Model	Warning			2021-08-23	2021-08-23		ThinQ.AI Clou
3782		P	Progress 3rd SRC BIN BOM				Preceding Software				2021-08-19	2021-08-23		ThinQ.AI User
3781		P	Progress 3rd SRC BIN BOM				Preceding Software	Warning			2021-08-19	2021-08-24	방재권	ThinQ.AI Serv
3780		P	Progress 3rd SRC BIN BOM				General Model				2021-08-19	2021-08-19		Copy From (2)
3779		P	Progress 3rd SRC BIN BOM				General Model				2021-08-19	2021-08-19		Copy From (2)
3778		P	Progress 3rd SRC BIN BOM				Transfer in-house	Warning			2021-08-19	2021-08-19		Copy From (2)
3777		P	Progress 3rd SRC BIN BOM				Transfer in-house	Warning			2021-08-19	2021-08-19		Copy From (2)
3774		P	Confirm 3rd SRC BIN BOM	Start			General Model	Warning			2021-08-19	2021-08-20	석지영	LG ThinQ App
3773		C	Confirm Android	Confirm Done			General Model	Warning			2021-08-18	2021-08-20	김소임	
3772		C	Confirm 3rd SRC BIN BOM	Confirm Done			General Model	Warning			2021-08-18	2021-08-24	석지영	Copy From (3)
3770		C	Confirm 3rd SRC BIN BOM	N/A	N/A		Preceding Software	Warning			2021-08-18	2021-08-20	박원재	
3767		R	Review 3rd SRC BIN BOM				General Model				2021-08-17	2021-08-23	박원재	
3766		R	Review 3rd SRC BIN BOM				Preceding Software	Warning			2021-08-17	2021-08-23	박원재	

# FOSSLight의 역사



# 2019 – OpenChain Conformance

THE LINUX FOUNDATION PROJECTS

OPENCHAIN

Adopt Resources FAQ Community

## LG Announces Conformance To OpenChain 2.1 (ISO/IEC 5230)

By Shane Coughlan | February 8, 2021 | Featured, News



**LG**  
Life's Good

Today the OpenChain Project announced LG Electronic's conformance to OpenChain 2.1 (ISO/IEC 5230), the International Standard for open source license compliance. This standard defines the

### OpenChain Spec.

#### 1. Program Foundation

- 1.1. Policy
- 1.2. Competence
- 1.3. Awareness
- 1.4. Program scope
- 1.5. License Obligations

#### 2. Relevant tasks defined and supported

- 2.1. Access
- 2.2. Effectively resourced

#### 3. Open source content review and approval

- 3.1. Bill of materials
- 3.2. License compliance

#### 4. Compliance artifact creation and delivery

- 4.1. Compliance artifacts

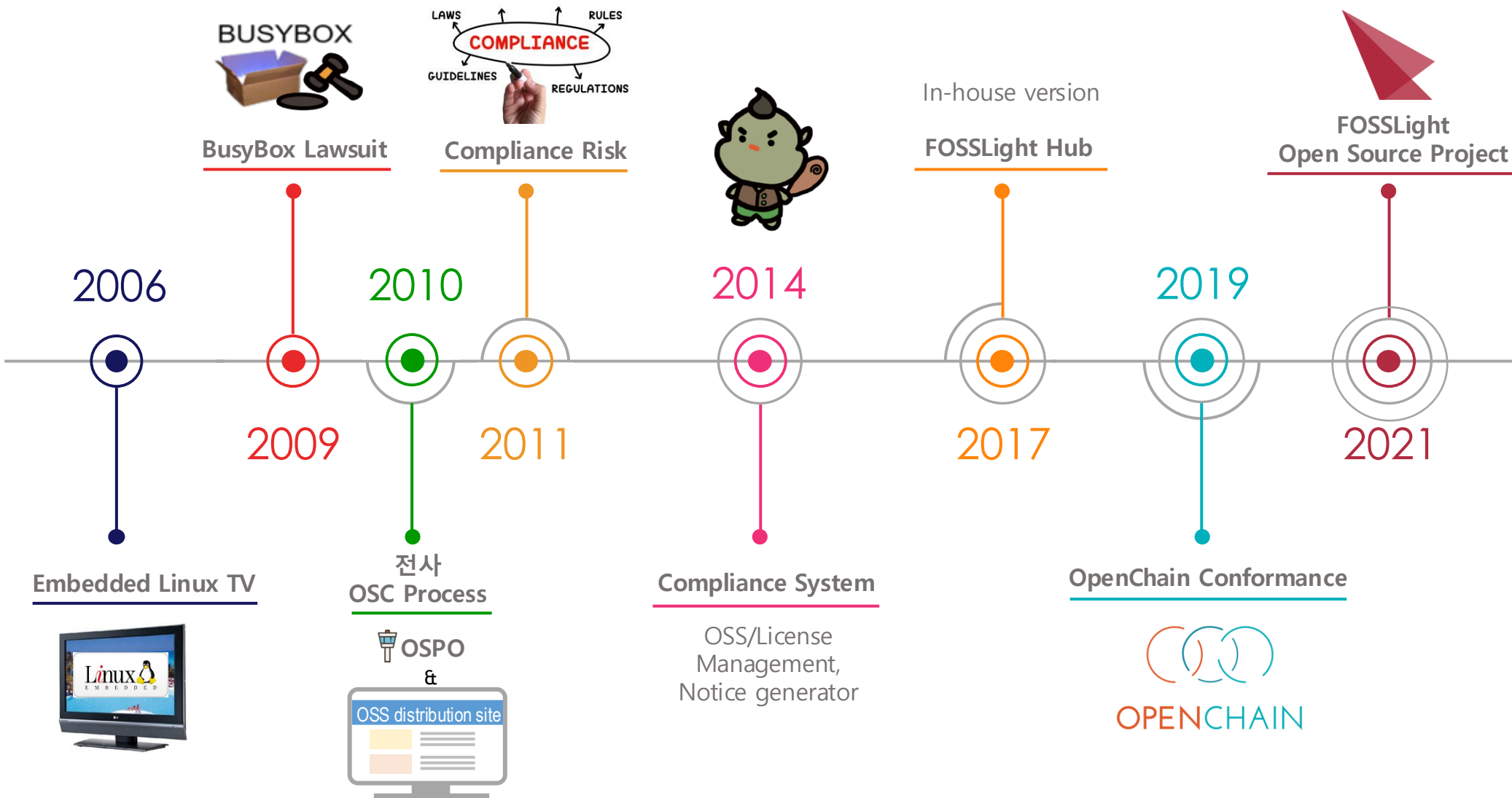
#### 5. Understanding open source community engagements

- 5.1. Contributions

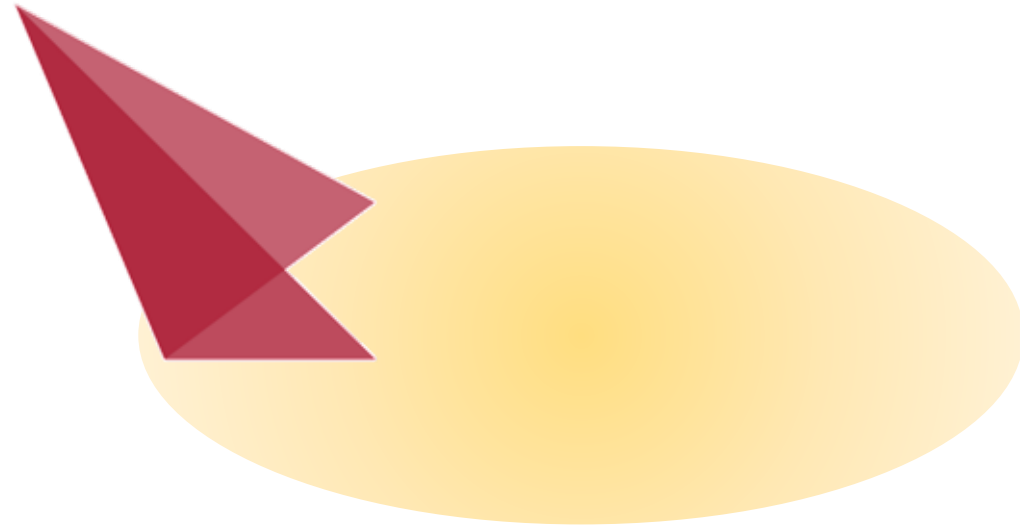
#### 6. Adherence to the specification requirements

- 6.1. Conformance
- 6.2. Duration

# FOSSLight의 역사



# 2021 – FOSSLight Open Source Project

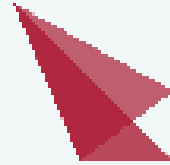


## FOSSLight

FOSS (Free and Open Source Software) + Light

# FOSSLight Scanner

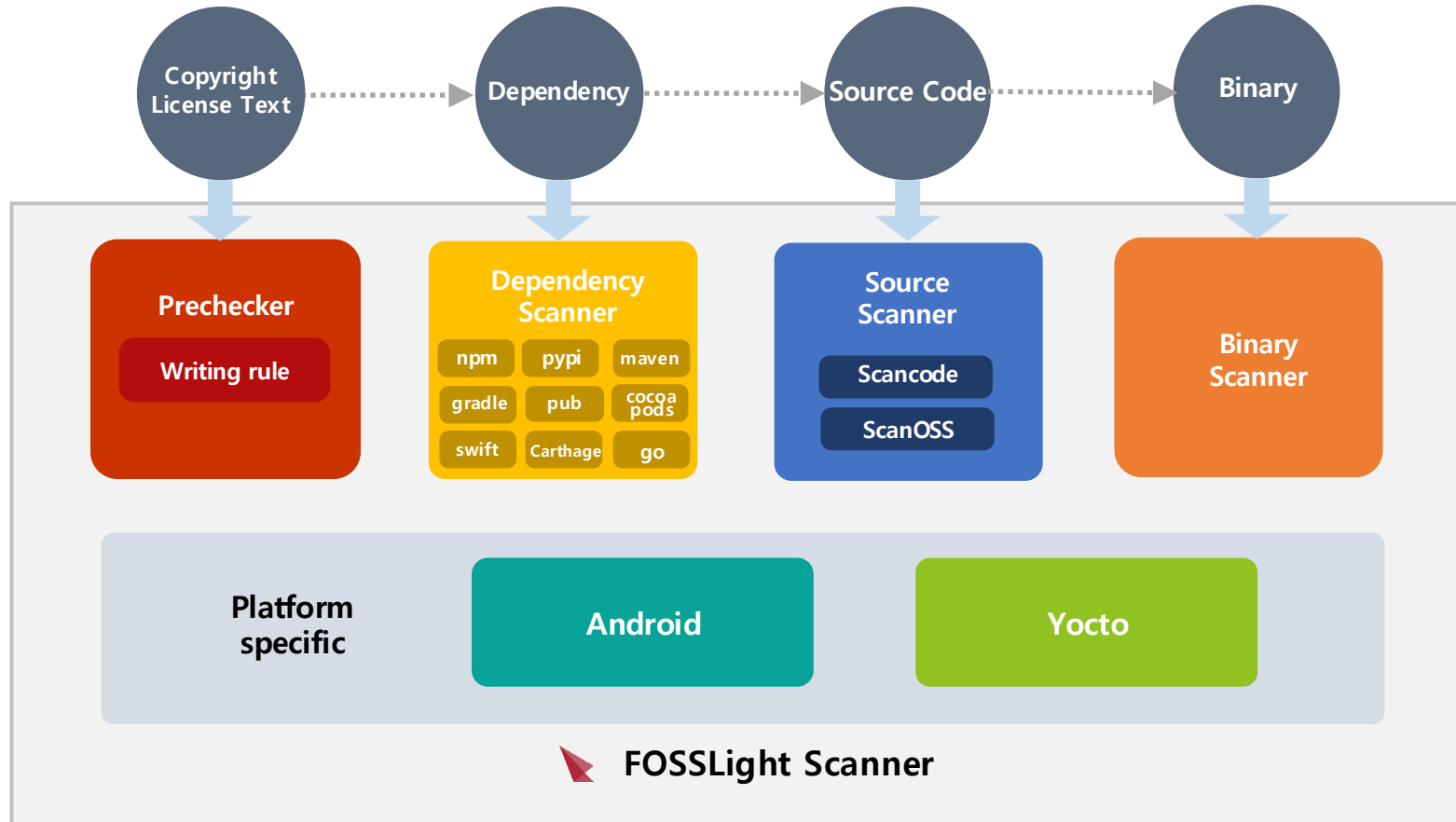
---



# About FOSSLight Scanner

- **오픈 소스 분석을 한번에 수행 가능한 툴**
- **소스 코드, 바이너리, 디펜던시에 대한 오픈 소스 분석 가능**
- **LG전자가 오픈 소스로 공개한 오픈 소스 분석 툴**
- **오픈 소스 정보를 포함한 보고서(Report) 생성**
  - cydone, spdx, csv, excel, json, yaml 포맷 지원

# FOSSLight Scanner



# FOSSLight Scanner – Dependency

- Transitive Dependency까지 확인하여 오픈소스 이름 및 버전, 라이선스를 검출함
- 지원 패키지 매니저 : Gradle, Maven, NPM, PIP, Pub, Cocoapods, Swift, Carthage, Go 등

Dependency 분석을 위해서는 미리 수행에 필요한 전제 조건 수행 필요함



ID	Source Name or OSS Name	OSS Version	License	Download Location	Homepage	
-	[Name of the Sc	[Name of the OSS used in	[Version Number	[License of the C	[Download URL or a specific location within a VCS for the OSS]	[Web site that serves as the OSS's home page]
1	pubspec.yaml pub:ansicolor	1.0.5	Apache-2.0	https://pub.dev/packages/pub:ansicolor/versions/1.0.5	https://github.com/google/ansicolor-dart	
2	pubspec.yaml pub:async	2.5.0-nullsafety.1	BSD-3-Clause	https://pub.dev/packages/pub:async/versions/2.5.0-nullsafety.1	https://www.github.com/dart-lang/async	
3	pubspec.yaml pub:cached_network_image	2.3.2+1	MIT	https://pub.dev/packages/pub:cached_network_image/versions/2.3.2+1	https://github.com/Baseflow/flutter_cached_network_image	
4	pubspec.yaml pub:characters	1.1.0-nullsafety.3	BSD-3-Clause	https://pub.dev/packages/pub:characters/versions/1.1.0-nullsafety.3	https://www.github.com/dart-lang/characters	
5	pubspec.yaml pub:charcode	1.2.0-nullsafety.1	BSD-3-Clause	https://pub.dev/packages/pub:charcode/versions/1.2.0-nullsafety.1	https://github.com/dart-lang/charcode	
6	pubspec.yaml pub:clock	1.1.0-nullsafety.1	Apache-2.0	https://pub.dev/packages/pub:clock/versions/1.1.0-nullsafety.1	https://github.com/dart-lang/clock	
7	pubspec.yaml pub:collection	1.15.0-nullsafety.3	BSD-3-Clause	https://pub.dev/packages/pub:collection/versions/1.15.0-nullsafety.3	https://www.github.com/dart-lang/collection	
8	pubspec.yaml pub:console_log_handler	1.1.6	Apache-2.0	https://pub.dev/packages/pub:console_log_handler/versions/1.1.6	https://github.com/MikeMitterer/dart-console_log_handler	
9	pubspec.yaml pub:convert	2.1.1	BSD-3-Clause	https://pub.dev/packages/pub:convert/versions/2.1.1	https://github.com/dart-lang/convert	
10	pubspec.yaml pub:crypto	2.1.5	BSD-3-Clause	https://pub.dev/packages/pub:crypto/versions/2.1.5	https://www.github.com/dart-lang/crypto	
11	pubspec.yaml pub:ffi	0.1.3	BSD-3-Clause	https://pub.dev/packages/pub:ffi/versions/0.1.3	https://github.com/dart-lang/ffi	
12	pubspec.yaml pub:file	5.2.1	BSD-3-Clause	https://pub.dev/packages/pub:file/versions/5.2.1	https://github.com/google/file.dart	
13	pubspec.yaml pub:flutter	1.22.0	BSD-3-Clause	https://pub.dev/packages/pub:flutter/versions/1.22.0	http://flutter.dev	
14	pubspec.yaml pub:flutter_blurhash	0.5.0	MIT	https://pub.dev/packages/pub:flutter_blurhash/versions/0.5.0	https://github.com/fluttercommunity/flutter_blurhash	
15	pubspec.yaml pub:flutter_cache_manager	1.4.2	MIT	https://pub.dev/packages/pub:flutter_cache_manager/versions/1.4.2	https://github.com/Baseflow/flutter_cache_manager	



# FOSSLight Scanner - Binary

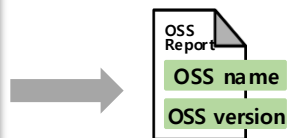
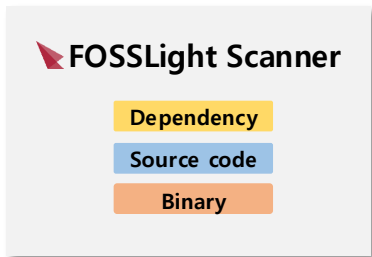
- 바이너리 목록 추출하여 Database에서 오픈소스 정보 확인
- Jar 파일에 대하여 보안 취약점 확인도 가능



	A	B	C	D	E	F	G	H	I	J	K
1	ID	Source Name	OSS Name	OSS Version	License	Download Location	Homepage	Copyright Text	Exclude	Comment	Vulnerability Link
2	22	lib/aho-cch	hanks:ah	1.2.3	Apache License Version 2.0	hanks/AhoCorasickDoubleArrayTrie				OWASP Result.	
3	23	lib/androi	vaadin.ext	0.0.201311	Apache License 2.0	<a href="http://developer.android.com/sdk">http://developer.android.com/sdk</a>				OWASP Result.	
4	24	lib/annota	jetbrains.a	22.0.0	The Apache Software License	JetBrains/java-annotations				OWASP Result.	
5	25	lib/ant-	1.1	apache.an	1.10.12	<a href="https://ant.apache.org/">https://ant.apache.org/</a>				OWASP Result.	<a href="https://nvd.nist.gov/vuln/search/results?form_type=Ad">https://nvd.nist.gov/vuln/search/results?form_type=Ad</a>
6	26	lib/checke	checkerfra	3.12.0	The MIT License	<a href="https://checkerframework.org">https://checkerframework.org</a>				OWASP Result.	
7	27	lib/comm	commons	1.9.4	<a href="https://www.apache.org/licenses">https://www.apache.org/licenses</a>	<a href="https://commons.apache.org/proper/commons-beanutils/">https://commons.apache.org/proper/commons-beanutils/</a>				OWASP Result.	<a href="https://nvd.nist.gov/vuln/search/results?form_type=Ad">https://nvd.nist.gov/vuln/search/results?form_type=Ad</a>
8	28	lib/comm	commons	1.5.0	<a href="https://www.apache.org/licenses">https://www.apache.org/licenses</a>	<a href="https://commons.apache.org/proper/commons-cli/">https://commons.apache.org/proper/commons-cli/</a>				OWASP Result.	
9	29	lib/comm	commons	1.15	<a href="https://www.apache.org/licenses">https://www.apache.org/licenses</a>	<a href="https://commons.apache.org/proper/commons-codec/">https://commons.apache.org/proper/commons-codec/</a>				OWASP Result.	
10	30	lib/comm	commons	3.2.2	<a href="http://www.apache.org/licenses">http://www.apache.org/licenses</a>	<a href="http://commons.apache.org/collections/">http://commons.apache.org/collections/</a>				OWASP Result.	<a href="https://nvd.nist.gov/vuln/search/results?form_type=Ad">https://nvd.nist.gov/vuln/search/results?form_type=Ad</a>
11	31	lib/comm	commons	1.21	<a href="https://www.apache.org/licenses">https://www.apache.org/licenses</a>	<a href="https://commons.apache.org/proper/commons-compress/">https://commons.apache.org/proper/commons-compress/</a>				OWASP Result.	<a href="https://nvd.nist.gov/vuln/search/results?form_type=Ad">https://nvd.nist.gov/vuln/search/results?form_type=Ad</a>
12	32	lib/comm	commons	2.9.0	<a href="https://www.apache.org/licenses">https://www.apache.org/licenses</a>	<a href="https://commons.apache.org/dbcp/">https://commons.apache.org/dbcp/</a>				OWASP Result.	
13	33	lib/comm	commons	2.1	<a href="http://www.apache.org/licenses">http://www.apache.org/licenses</a>	<a href="http://commons.apache.org/digester/">http://commons.apache.org/digester/</a>				OWASP Result.	
14	34	lib/comm	commons	2.11.0	<a href="https://www.apache.org/licenses">https://www.apache.org/licenses</a>	<a href="https://commons.apache.org/proper/commons-io/">https://commons.apache.org/proper/commons-io/</a>				OWASP Result.	<a href="https://nvd.nist.gov/vuln/search/results?form_type=Ad">https://nvd.nist.gov/vuln/search/results?form_type=Ad</a>
15	35	lib/comm	commons	2.2.1	<a href="https://www.apache.org/licenses">https://www.apache.org/licenses</a>	<a href="https://commons.apache.org/licenses/LICENSE-2.0.txt">LICENSE-2.0.txt</a>				OWASP Result.	
16	36	lib/comm	commons	3.12.0	<a href="https://www.apache.org/licenses">https://www.apache.org/licenses</a>	<a href="https://commons.apache.org/proper/commons-lang/">https://commons.apache.org/proper/commons-lang/</a>				OWASP Result.	
17	37	lib/comm	commons	1.2	<a href="http://www.apache.org/licenses">http://www.apache.org/licenses</a>	<a href="http://commons.apache.org/proper/commons-logging/">http://commons.apache.org/proper/commons-logging/</a>			Exclude	OWASP Result. Excluded due to Binary DB.	
18	38	lib/comm	commons	1.2	Apache-2.0					Binary DB Result	

# FOSSLight Scanner를 통한 SBOM 생성

- FOSSLight Scanner 실행하여 오픈소스 분석 보고서 생성



	Source Name or Path	OSS Name	OSS Version	License	Download Location	Homepage	Copyright Text	Exclude	Comment	Dependency	
1	package.json	npm:lge-example	1.0.0	Apache-2.0	<a href="https://github.com/LGE-OSS/example">https://github.com/LGE-OSS/example</a>	<a href="https://www.npmjs.com/package/lge-example">https://www.npmjs.com/package/lge-example</a>			root pack	npm:copy-	
2	package.json	npm:copy-anything	2.0.6	MIT	<a href="https://github.com/mesqueeb/copy-anything">https://github.com/mesqueeb/copy-anything</a>	<a href="https://www.npmjs.com/package/copy-anything">https://www.npmjs.com/package/copy-anything</a>			direct	npm:is-wha	
3	package.json	npm:is-what	3.14.1	MIT	<a href="https://github.com/mesqueeb/is-what">https://github.com/mesqueeb/is-what</a>	<a href="https://www.npmjs.com/package/is-what">https://www.npmjs.com/package/is-what</a>				transitive	
4	requirements.txt	pypi:CacheControl	0.12.11	Apache Software License	<a href="https://pypi.org/project/CacheControl/0.12.11">https://pypi.org/project/CacheControl/0.12.11</a>	<a href="https://github.com/ionrock/cachecontrol">https://github.com/ionrock/cachecontrol</a>				transitive	pypi:msgpa
5	requirements.txt	pypi:Deprecated	1.2.14	MIT License	<a href="https://pypi.org/project/Deprecated/1.2.14">https://pypi.org/project/Deprecated/1.2.14</a>	<a href="https://github.com/tantale/deprecated">https://github.com/tantale/deprecated</a>				transitive	pypi:wrapt
6	requirements.txt	pypi:jinja2	3.1.2	BSD License	<a href="https://pypi.org/project/jinja2/3.1.2">https://pypi.org/project/jinja2/3.1.2</a>	<a href="https://palletsprojects.com/p/jinja/">https://palletsprojects.com/p/jinja/</a>				transitive	pypi:Marku
7	requirements.txt	pypi:MarkupSafe	2.1.3	BSD License	<a href="https://pypi.org/project/MarkupSafe/2.1.3">https://pypi.org/project/MarkupSafe/2.1.3</a>	<a href="https://palletsprojects.com/p/markupsafe/">https://palletsprojects.com/p/markupsafe/</a>				transitive	
8	requirements.txt	pypi:PyGithub	2.1.1	GNU Library or Lesser Gen	<a href="https://pypi.org/project/PyGithub/2.1.1">https://pypi.org/project/PyGithub/2.1.1</a>	<a href="https://github.com/pygithub/pygithub">https://github.com/pygithub/pygithub</a>				transitive	pypi:Depre
9	requirements.txt	pypi:PyJWT	2.8.0	MIT License	<a href="https://pypi.org/project/PyJWT/2.8.0">https://pypi.org/project/PyJWT/2.8.0</a>	<a href="https://github.com/jpadilla/pyjwt">https://github.com/jpadilla/pyjwt</a>				transitive	
10	requirements.txt	pypi:PyNaCl	1.5.0	Apache License 2.0	<a href="https://pypi.org/project/PyNaCl/1.5.0">https://pypi.org/project/PyNaCl/1.5.0</a>	<a href="https://github.com/pyca/pynacl/">https://github.com/pyca/pynacl/</a>				transitive	pypi:cffi(1.
11	requirements.txt	pypi:PyYAML	6.0.1	MIT License	<a href="https://pypi.org/project/PyYAML/6.0.1">https://pypi.org/project/PyYAML/6.0.1</a>	<a href="https://pyyaml.org/">https://pyyaml.org/</a>				transitive	
12	requirements.txt	pypi:XlsxWriter	3.1.8	BSD License	<a href="https://pypi.org/project/XlsxWriter/3.1.8">https://pypi.org/project/XlsxWriter/3.1.8</a>	<a href="https://github.com/imcmamara/XlsxWriter">https://github.com/imcmamara/XlsxWriter</a>				transitive	
13	requirements.txt	pypi:appdirs	1.4.4	MIT License	<a href="https://pypi.org/project/appdirs/1.4.4">https://pypi.org/project/appdirs/1.4.4</a>	<a href="https://github.com/ActiveState/appdirs">https://github.com/ActiveState/appdirs</a>				transitive	
14	requirements.txt	pypi:attrs	23.1.0	MIT License	<a href="https://pypi.org/project/attrs/23.1.0">https://pypi.org/project/attrs/23.1.0</a>	<a href="https://www.attrs.org/en/stable/changelog.html">https://www.attrs.org/en/stable/changelog.html</a>				transitive	
15	requirements.txt	pypi:beautifulsoup4	4.12.2	MIT License	<a href="https://pypi.org/project/beautifulsoup4/4.12.2">https://pypi.org/project/beautifulsoup4/4.12.2</a>	<a href="https://www.crummy.com/software/BeautifulSoup/bs4/">https://www.crummy.com/software/BeautifulSoup/bs4/</a>				transitive	pypi:soups
16	requirements.txt	pypi:binaryornot	0.4.4	BSD License	<a href="https://pypi.org/project/binaryornot/0.4.4">https://pypi.org/project/binaryornot/0.4.4</a>	<a href="https://github.com/audreyt/binaryornot">https://github.com/audreyt/binaryornot</a>				transitive	pypi:charde
17	requirements.txt	pypi:boolean.py	4.0	BSD-2-Clause	<a href="https://pypi.org/project/boolean.py/4.0">https://pypi.org/project/boolean.py/4.0</a>	<a href="https://github.com/bastikr/boolean.py">https://github.com/bastikr/boolean.py</a>				transitive	
18	requirements.txt	pypi:certifi	2023.7.22	Mozilla Public License 2.0	<a href="https://pypi.org/project/certifi/2023.7.22">https://pypi.org/project/certifi/2023.7.22</a>	<a href="https://github.com/certifi/python-certifi">https://github.com/certifi/python-certifi</a>				transitive	
19	requirements.txt	pypi:cffi	1.16.0	MIT License	<a href="https://pypi.org/project/cffi/1.16.0">https://pypi.org/project/cffi/1.16.0</a>	<a href="http://cffi.readthedocs.org">http://cffi.readthedocs.org</a>				transitive	pypi:pycpar
20	requirements.txt	pypi:chardet	5.2.0	GNU Lesser General Public	<a href="https://pypi.org/project/chardet/5.2.0">https://pypi.org/project/chardet/5.2.0</a>	<a href="https://github.com/chardet/chardet">https://github.com/chardet/chardet</a>				transitive	

# FOSSLight Scanner 설치 및 실행

---

# FOSSLight Scanner OS별 지원 형식

	Ubuntu	Windows	MacOS
실행 파일 (.exe)	FOSSLight Binary Scanner	FOSSLight Binary Scanner, FOSSLight Dependency Scanner	FOSSLight Binary Scanner
PyPI 패키지	전체 Scanner 지원		

- 실행 파일
  - FOSSLight Dependency Scanner (Windows만 가능)
    - [https://github.com/fosslight/fosslight\\_dependency\\_scanner/releases](https://github.com/fosslight/fosslight_dependency_scanner/releases)
  - FOSSLight Binary Scanner (Ubuntu, MacOS, Windows 가능)
    - [https://github.com/fosslight/fosslight\\_binary\\_scanner/releases](https://github.com/fosslight/fosslight_binary_scanner/releases)

# FOSSLight Scanner PyPI 패키지

10 프로젝트 "fosslight"의 경우

정렬 순서: **관련성**

Project Name	Description	Release Date
<b>fosslight-scanner</b>	FOSSLight Scanner	2025년 11월 14일
<b>fosslight-yocto</b>	FOSSLight Yocto	2025년 7월 16일
<b>fosslight-prechecker</b>	FOSSLight Prechecker	2025년 7월 21일
<b>fosslight-source</b>	FOSSLight Source Scanner	2025년 12월 12일
<b>fosslight-binary</b>	FOSSLight Binary Scanner	2025년 12월 12일
<b>fosslight-android</b>	FOSSLight Android Scanner	2025년 12월 12일

**YES, THIS ASK DON**

**DON**

# Pypi 통해 설치 방법

- Python Package로 설치

```
$ pip install fosslight_scanner
```

- FOSSLight Scanner 한 번에 설치 가능

- FOSSLight Dependency Scanner
- FOSSLight Source Scanner
- FOSSLight Binary Scanner

- ❖ 하기 Scanner는 별도로 설치해야 함

- FOSSLight Android Scanner (\$ pip install fosslight\_android)
- FOSSLight Yocto Scanner (\$ pip install fosslight\_yocto)
- FOSSLight Prechecker (\$ pip install fosslight\_prechecker)

# FOSSLight Scanner 실행 방법

- 여러 FOSSLight Scanner의 통합 버전

```
$ fosslight [Mode] [option1] <arg1> [option2] <arg2>
```

- Mode:

all	모든 Scanner 실행
source	FOSSLight Source Scanner 실행
dependency	FOSSLight Dependency Scanner 실행
binary	FOSSLight Binary Scanner 실행
compare	FOSSLight reports 를 비교

- Options:

-h	Help message 출력
-p <input path>	분석할 경로 (default: 현재 위치 path)
-w <link>	다운받아 분석할 링크
-f <format>	결과 파일 포맷 (default: excel, 여러 개 지정 가능)
-e <exclude path>	분석 결과에서 exclude 처리하고자하는 경로
-o <output path>	결과 파일 저장 경로(파일명 지정 가능) (default: fosslight_report_{date})
-c <number>	분석 수행할 프로세스 수 (default: 시스템의 cpu 수 -1)
-r	Raw data 보존
-t	Progress Bar 숨기기
-v	FOSSLight Scanner 버전 출력

- Options for only 'all' or 'dependency' mode

-d <dependency_arg>	Dependency 분석을 위한 추가 arguments
---------------------	--------------------------------

## FOSSLight Scanner 실행 방법

```
fosslight -p path_to_analyze
```

# FOSSLight Hub

---

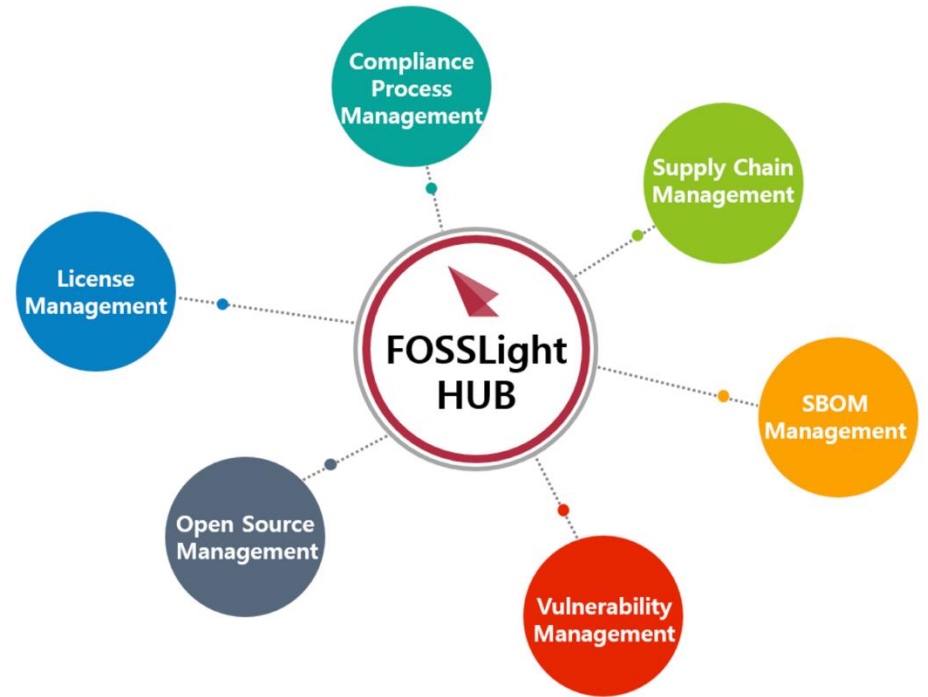
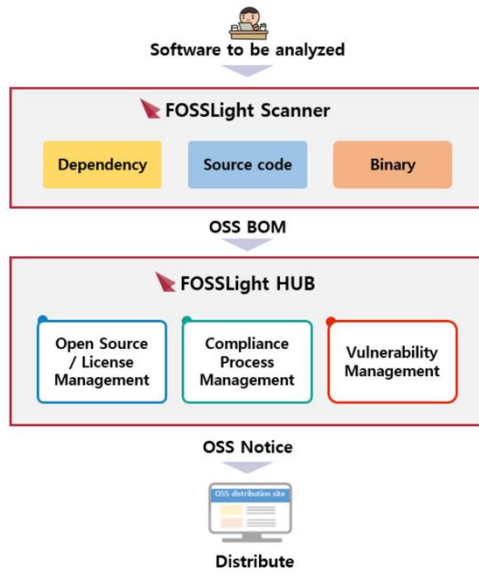
# FOSSLight Hub

## 오픈 소스 거버넌스를 위한 오픈 소스 관리 도구



# FOSSLight

오픈 소스를 사용하여 소프트웨어를 개발하고 배포할 때,  
오픈 소스 거버넌스를 위해 FOSSLight를 활용하실 수 있습니다.



# 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
- 프로젝트 별 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, CycloneDX 문서 지원 (ISO 표준)



## SW 공급망 관리

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

# 오픈소스 관리

- 오픈소스 버전별로 라이선스 및 의무 사항 관리

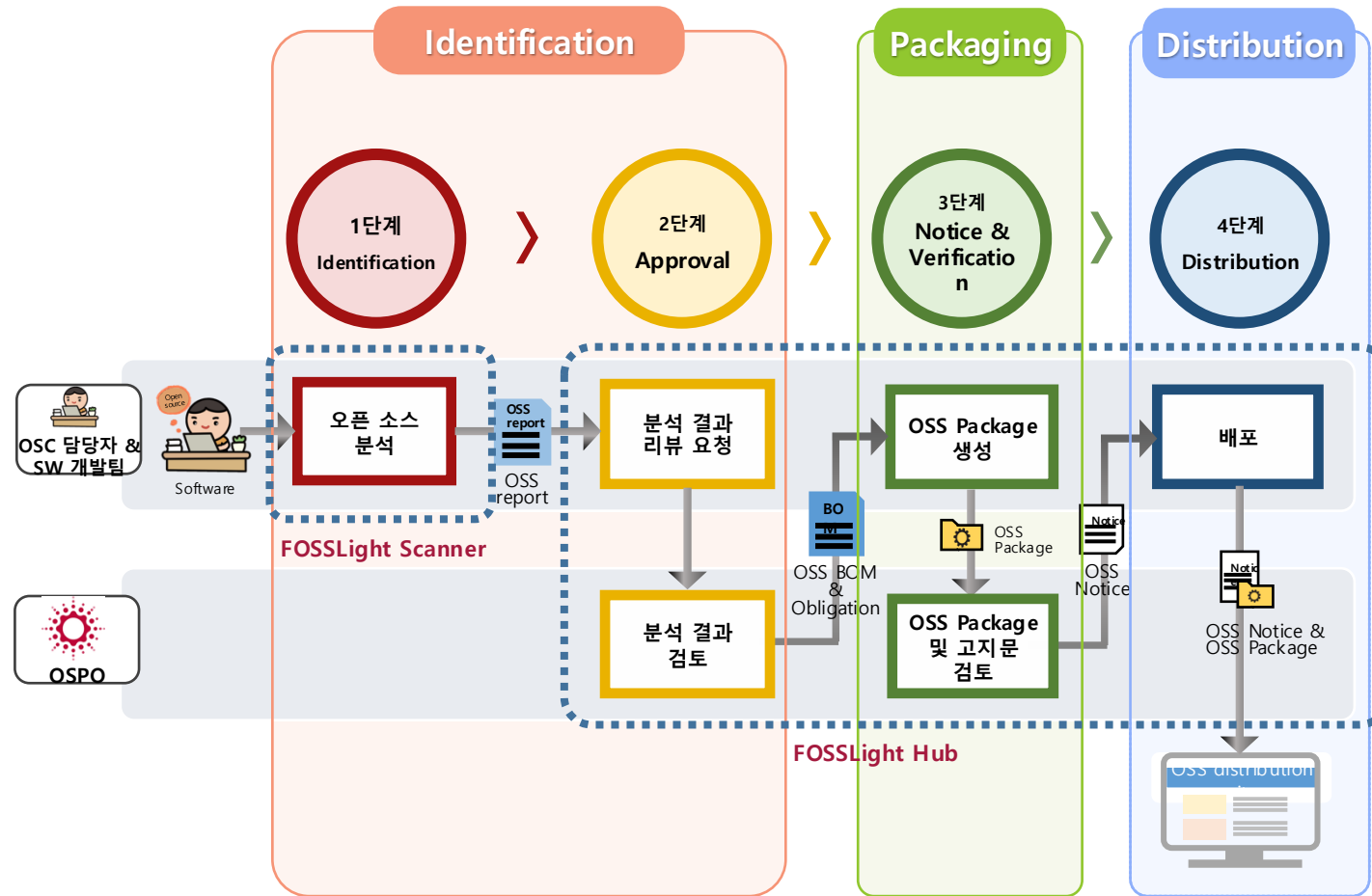
ID	OSS Name	OSS Version	License Name	Obligation
93432	[Nick] <a href="#">bjorklund</a>	1.0.1	MIT	
93429	[Nick] <a href="#">ashpy</a>	0.4.0	Apache-2.0	
93428	[Nick] <a href="#">async-array-methods</a>	2.1.0	MIT	
93427	<a href="#">zhanzhzhen-ban</a>	gitlock-001-sha256-1	MIT	
93426	[Nick] <a href="#">antlr-verilog-lsp-parser</a>	1.0.4	MIT	
93425	[Nick] <a href="#">browser-date-formatter</a>	3.0.2	MIT	
93424	[Nick] <a href="#">bitbucket-url-to-object</a>	0.3.0	MIT	
93423	<a href="#">zeehio-aves</a>	3.0.1	MIT	
93422	[Nick] <a href="#">cbar</a>	0.1.2	MIT	
93421	[Nick] <a href="#">check-pipfile-lock</a>	0.0.5	MIT	

# 라이선스 관리

- 라이선스별로 의무사항, 제약사항, 준수사항 관리

ID	License Name	Identifier	License Type	Restriction	Obligation	Website	User Guide
748	<a href="#">FlyCapture SDK End User License</a>		Proprietary Free	R		<a href="#">URL</a>	
747	<a href="#">TAU License</a>		Permissive	R	📄	<a href="#">URL</a>	- 실험 또는 비상업 목적으로 저작물의 전체 사
746	<a href="#">AWISC License</a>		Permissive		📄	<a href="#">URL</a>	
745	<a href="#">Standard "No Charge" GreenSock License</a>		Permissive	R	📄	<a href="#">URL</a>	- You may use the code at no charge in commerc
744	<a href="#">BSD-like License (castor)</a>		Permissive		📄	<a href="#">URL</a>	
743	<a href="#">REALNETWORKS COMMUNITY SOURCE LICENSE v1.2</a>		Weak Copyleft	R	📄🔗		상업적으로 사용할 수 없고 연구 목적으로만 s
742	<a href="#">Riverbank SIP License</a>		Permissive		📄	<a href="#">URL</a>	
741	<a href="#">Hazelcast Community License 1.0</a>		Permissive	R	📄	<a href="#">URL</a>	Hazelcast hereby grants to Licensee a non-exclu
740	<a href="#">Business Source License 1.1</a>	BUSL-1.1	Permissive	R	📄	<a href="#">URL</a>	The Licensor hereby grants you the right to copy
739	<a href="#">European Union Public License 1.2</a>	EUPL-1.2	Copyleft	R	📄🔗	<a href="#">URL</a>	Use, reproduce, modify, make derivative works,
738	<a href="#">GOOGLE TERMS OF SERVICE</a>		Proprietary Free	R		<a href="#">URL</a>	Software in Google services > "You may not copy
737	<a href="#">Google Developers Site Terms of Service</a>		Proprietary Free			<a href="#">URL</a>	Google Developers Site Terms of Service is used
736	<a href="#">GNU General Public License v3.0 w/lemcu.org GPL exception 1.0</a>		Copyleft		📄🔗	<a href="#">URL</a>	
735	<a href="#">BSD-like License (JTidy)</a>		Permissive		📄	<a href="#">URL</a>	
733	<a href="#">GNU General Public License v2.0 w/Ada Linking Exception</a>		Copyleft		📄🔗	<a href="#">URL</a>	

# 참고) LG전자 오픈소스 컴플라이언스 프로세스



# 컴플라이언스 프로세스 관리

- 단계별 프로세스 진행 및 이력 조회
- 프로젝트 검색, 부서별 검색, 오픈소스별 검색

ID	Project Name	Status	OSC Process	Download	Distribution Type	Security	Division	Creator	Reviewer
5219	hi_test_fosslight_util(ver.1.0)	Final Review	Identification > Packaging > Distribution	[Download]	Transfer in-house	Need to resolve(9.8)	CTO ICT기술센	일반이혜인	이혜인/선임연
5218	test(ver.444566)	Progress	Identification > Packaging > Distribution	[Download]	General	Need to resolve(9.8)	BS BS연구소	soim	
5217	version	Progress	Identification > Packaging > Distribution	[Download]	General	Need to resolve(9.8)	CTO SW센터	김경애/Task Le	김경애/Task Le
5214	test_3rd(ver.1.0)	Progress	Identification > Packaging > Distribution	[Download]	General	Need to resolve(7.8)	BS ID	민경선/책임연	민경선/책임연
5213	user hi test project	Progress	Identification > Packaging > Distribution	[Download]	General	Discovered(N/A)	BS ID	일반이혜인	
5212	test soijm(ver.1234)	Progress	Identification > Packaging > Distribution	[Download]	General	Discovered(N/A)	CTO SW센터	김소임/책임연	
5211	api_create_project test	Review	Identification > Packaging > Distribution	[Download]	General	Discovered(N/A)	CTO SW센터	시스템관리자	시스템관리자
5210	test soijm(ver.123)	Request	Identification > Packaging > Distribution	[Download]	General	Need to resolve(9.8)	CTO SW센터	김소임/책임연	민경선/책임연
5209	hi packaging test	Drop	Identification > Packaging > Distribution	[Download]	General	Need to resolve(7.8)	CTO SW센터	이혜인/선임연	이혜인/선임연
5208	ssssaaa(ver.2)	Drop	Identification > Packaging > Distribution	[Download]	General	Discovered(N/A)	CTO SW센터	민경선/책임연	
5207	noticehtml test	Progress	Identification > Packaging > Distribution	[Download]	General	Need to resolve(10)	CTO SW센터	민경선/책임연	민경선/책임연
5206	test_csg(ver.test)	Review	Identification > Packaging > Distribution	[Download]	General	Need to resolve(10)	CTO SW센터	석지영/책임연	석지영/책임연
5205	verify test	Progress	Identification > Packaging > Distribution	[Download]	General	Need to resolve(7.8)	CTO SW센터	시스템관리자	시스템관리자

# OSS 고지문 발급

- 사용된 Open Source 및 저작권, License를 고지하기 위한 OSS 고지문 발급
- 공개할 소스코드 취합한 OSS Package 리뷰
- 지원 포맷 : HTML, TEXT, SPDX, CycloneDX

Open Source Software Notice		OSSN
<p>This product from LG Electronics, Inc. contains the open source software detailed below (including the source code included following this notice) for the terms and conditions of their use.</p>		
Open Source	License	
junit 4.12	EPL-1.0	
<p>The source code for the above may be obtained free of charge from LG Electronics, Inc. (including the source code also provide open source code to you on CD-ROM for a charge covering the cost of shipping, and handling) upon email request to opensource@lge.com. This offer is valid for 90 days from the date of this notice or 90 days after our last shipment of this product.</p>		

**EPL-1.0**  
Eclipse Public License - v 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS ECLIPSE PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

# 사전 점검

- 프로젝트에서 사용할 오픈소스와 라이선스 리스트를 업로드하여 각각의 의무 사항 및 보안취약점 정보를 확인할 수 있음

The screenshot displays the FOSSlight self-check interface. On the left, a 'Self-Check' window shows a 'FOSSlight Report' for '1341\_selfCheck' dated 2024-03-29 17:23:37. Below it is a table with columns for ID, Binary Name or Source Path, OSS Name, OSS Version, and License. Two rows are highlighted in red, indicating required fields are missing.

ID	Binary Name or Source Path	OSS Name	OSS Version	License
48	example-1.0.1/package.json	This field is required.		Apache-2.0
39	example-1.0.1/LICENSE	This field is required.		Apache-2.0
63	example-1.0.1/third_party/httptools	httptools	0.0.4 Unconfirmed versio	MIT
64	example-1.0.1/third_party/httptools	httptools	0.0.7 Unconfirmed versio	MIT

On the right, a browser window shows the 'License text' for Apache License 2.0, including the title 'TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION' and the start of the '1. Definitions' section.

# 사전 점검 (Pre-Review)

- 오픈소스를 다운로드한 URL만 알아도 오픈소스와 라이선스 정보를 확인할 수 있음

Pre-Review ▾

+ 🗑️ ✎️ ⚙️

<input type="checkbox"/>	ID	Source Name o	OSS Name	OSS Version	License	Download Location	Homepage
		~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x
<input type="checkbox"/>	2		This field is required.	2.0.0	MIT	<a href="https://mvnrepository.com/artifact/org.slf4j/slf4j-api">https://mvnrepository.com/artifact/org.slf4j/slf4j-api</a>	<a href="http://www.slf4j.org">http://www.slf4j.org</a>
<input type="checkbox"/>	1		Test Spring Framework Unconfirmed open source	6.1.2	Apache-2.0	<a href="https://github.com/spring-projects/spring-framework">https://github.com/spring-projects/spring-framework</a>	<a href="https://github.com/spring-projects/spring-framewo">https://github.com/spring-projects/spring-framewo</a>
<input type="checkbox"/>	3		mybatis	3.5.9	EPL-2.0 Declared : Apache-2.0	<a href="https://mvnrepository.com/artifact/org.mybatis/mybatis">https://mvnrepository.com/artifact/org.mybatis/mybatis</a>	<a href="https://mybatis.org/mybatis-3">https://mybatis.org/mybatis-3</a>

# 사전 점검 (Pre-Review)


- 오픈소스를 다운로드한 URL만 알아도 라이선스 정보를 확인할 수 있음

Pre-Review ▾

+ □ ✎ ⬇

<input type="checkbox"/>	ID	Source Name o	OSS Name	OSS Version	License	Download Location	Homepage
		~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x
<input type="checkbox"/>	2		This field is required.	2.0.0	MIT	<a href="https://mvnrepository.com/artifact/org.slf4j/slf4j-api">https://mvnrepository.com/artifact/org.slf4j/slf4j-api</a>	<a href="http://www.slf4j.org">http://www.slf4j.org</a>
<input type="checkbox"/>	1		Test Spring Framework Unconfirmed open source	6.1.2	Apache-2.0	<a href="https://github.com/spring-projects/spring-framework">https://github.com/spring-projects/spring-framework</a>	<a href="https://github.com/spring-projects/spring-framewo">https://github.com/spring-projects/spring-framewo</a>
<input type="checkbox"/>	3		mybatis	3.5.9	EPL-2.0 Declared : Apache-2.0	<a href="https://mvnrepository.com/artifact/org.mybatis/mybatis">https://mvnrepository.com/artifact/org.mybatis/mybatis</a>	<a href="https://mybatis.org/mybatis-3">https://mybatis.org/mybatis-3</a>

License detected based on OSS Name, Version, and Download location. To change the license, click the "Change License" button.

<input type="checkbox"/>	Result	Download location	OSS name	OSS version	License (current)	License (to be changed)	Evidence
<input type="checkbox"/>		<a href="https://mvnrepository.com/artifact/org.mybatis/mybatis">https://mvnrepository.com/artifact/org.mybatis/mybatis</a>	mybatis	3.5.9	EPL-2.0 Declared : Apache-2.0	Apache-2.0	 DB

Change License

# 사전 점검 (Pre-Review)

- 오픈소스를 다운로드한 URL만 알아도 오픈소스 정보를 확인할 수 있음

Pre-Review ▾

+ ✖ ✎ ⚙

<input type="checkbox"/>	ID	Source Name o	OSS Name	OSS Version	License	Download Location	Homepage
		~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x
<input type="checkbox"/>	2		This field is required.	2.0.0	MIT	<a href="https://mvnrepository.com/artifact/org.slf4j/slf4j-api">https://mvnrepository.com/artifact/org.slf4j/slf4j-api</a>	<a href="http://www.slf4j.org">http://www.slf4j.org</a>
<input type="checkbox"/>	1		Test Spring Framework Unconfirmed open source	6.1.2	Apache-2.0	<a href="https://github.com/spring-projects/spring-framework">https://github.com/spring-projects/spring-framework</a>	<a href="https://github.com/spring-projects/spring-framewo">https://github.com/spring-projects/spring-framewo</a>
<input type="checkbox"/>	3		mybatis	3.5.9	EPL-2.0 Declared : Apache-2.0	<a href="https://mvnrepository.com/artifact/org.mybatis/mybatis">https://mvnrepository.com/artifact/org.mybatis/mybatis</a>	<a href="https://mybatis.org/mybatis-3">https://mybatis.org/mybatis-3</a>

There exists another OSS which has same download location. Please click "Change OSS Name" if you want to change to the registered OSS Name.

<input type="checkbox"/>	Result	Download location	OSS name (now)	Registered OSS name (to be changed)
<input type="checkbox"/>		<a href="https://mvnrepository.com/artifact/org.slf4j/slf4j-api">https://mvnrepository.com/artifact/org.slf4j/slf4j-api</a>	This field is required.	<a href="#">slf4J</a>
<input type="checkbox"/>		<a href="https://github.com/spring-projects/spring-framework">https://github.com/spring-projects/spring-framework</a>	Test Spring Framework Unconfirmed open source	<a href="#">Spring Framework</a>

Change OSS Name

# 사전 점검 (Pre-Review)

- 오픈소스 라이선스 의무 사항 확인 가능함

The screenshot displays the FOSSlight self-check interface. On the left, a 'Pre-Review' table lists items for review. On the right, a license popup for Apache-2.0 is shown, including the license name, identifier, and full license text.

ID	Binary Name or Source Path	OSS Name	OSS Version	License
48	example-1.0.1/package.json	This field is required.		Apache-2.0
39	example-1.0.1/LICENSE	This field is required.		Apache-2.0
63	example-1.0.1/third_party/httptools	httptools	0.0.4 Unconfirmed version	MIT
64	example-1.0.1/third_party/httptools	httptools	0.0.7 Unconfirmed version	MIT

License Name	Identifier	License Obligat	Restrict	Website	Nick Name
Apache License 2.0	Apache-2.0	Permis:		<a href="#">URL</a>	#Apache 2, #Apache 2.0, #Apache

**License text**

Apache License  
Version 2.0, January 2004  
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

# 사전 점검 (오픈소스 분석)

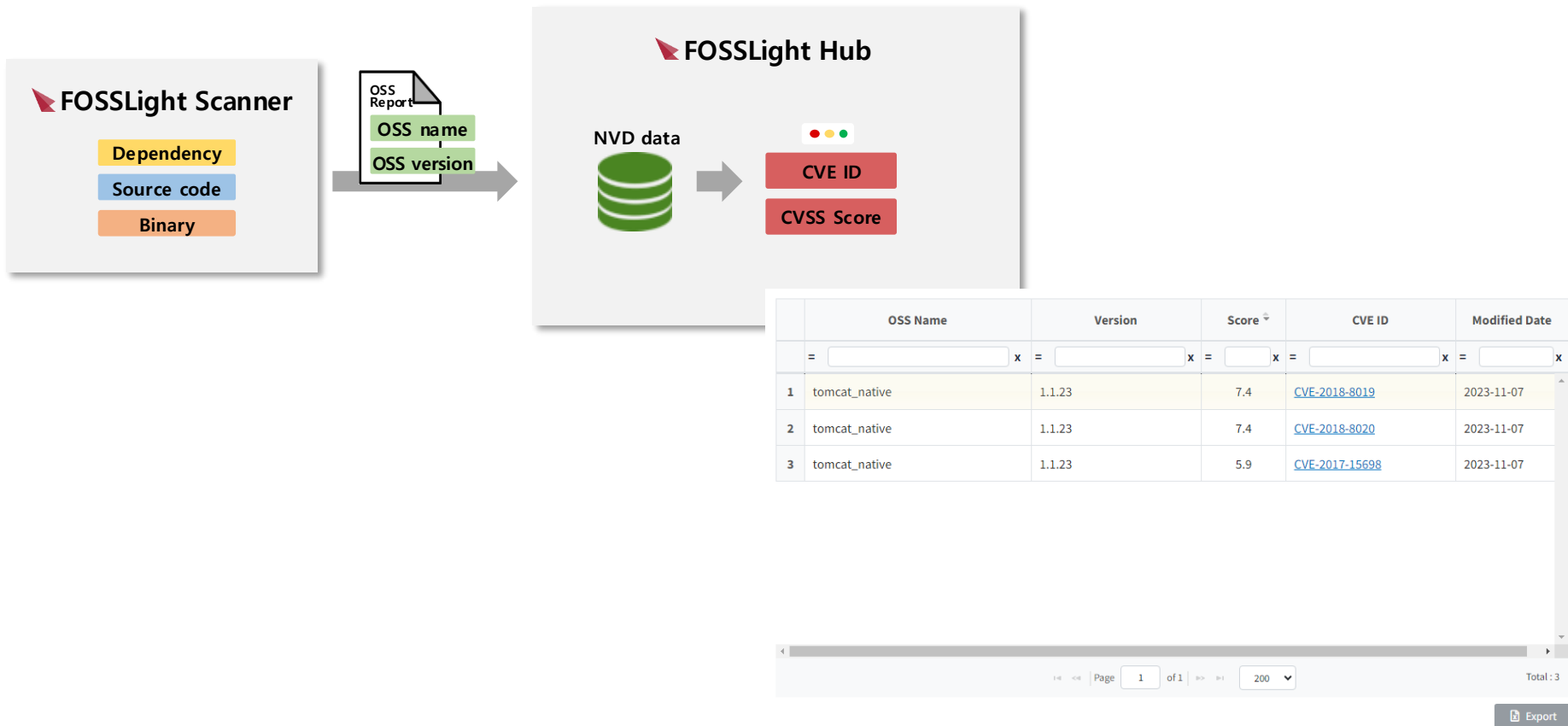
- Self-Check에 스캐닝 도구를 연동하여 소스 레파지토리 주소를 입력으로 오픈소스 라이선스 의무 사항 확인 가능

The screenshot shows a web interface for 'Self-Check' with a 'Notice' tab. It features two radio buttons: 'Upload Analysis Result' (unselected) and 'URL' (selected). Below the radio buttons is a text input field containing 'http://github.com/LGE-OSS/example' and a blue 'send' button. Underneath is a 'Pre-Review' dropdown menu and a table with columns for ID, Binary Name or So, OSS Name, OSS Ver:, License, Download, Homepage, Copyright Text, OSS | Licen, User Vuln, Oblig Resti, and a checkbox. The table has one row with placeholder text and 'x' marks.

ID	Binary Name or So	OSS Name	OSS Ver:	License	Download	Homepage	Copyright Text	OSS   Licen	User Vuln	Oblig Resti	Guid	bility	<input type="checkbox"/>
~	[ ] x	~	[ ] x	~	[ ] x	~	[ ] x	~	[ ] x	~	[ ] x	>=	[ ]

# 보안 취약점 관리

- 오픈소스 분석한 결과를 FOSSLight Hub 업로드하여 보안취약점 조회 및 관리 가능



1. **CVE ID** : CVE-2018-8019  
 2. **Description** : When using an OCSP responder Apache Tomcat Native 1.2.0 to 1.2.16 and 1.1.23 to 1.1.34 did not correctly handle invalid responses. This allowed for revoked client certificates to be incorrectly identified. It was therefore possible for users to authenticate with revoked certificates when using mutual TLS. Users not using OCSP checks are not affected by this vulnerability. Al emplear un respondedor OCSP, Apache Tomcat Native desde la versión 1.2.0 hasta la 1.2.16 y desde la versión 1.1.23 hasta la 1.1.34 no gestionó correctamente las respuestas inválidas. Esto permitió que los certificados de cliente revocados se identificasen erróneamente. Por lo tanto, era posible que los usuarios se autenticasen con certificados revocados al emplear TLS mutuo. Los usuarios que no emplean comprobaciones OCSP no se han visto afectados por esta vulnerabilidad.

# 제품 보안 취약점 확인

- 개발 제품별 프로젝트 등록하여 프로젝트별 보안 취약점 확인 가능

<input type="checkbox"/>	ID	Project Name	Status	OSC Process	Download	Security
<input type="checkbox"/>	697	<a href="#">3rd party create test 1</a>	Complete	Identification > Packaging		Discovered(N/A)
<input type="checkbox"/>	532	<a href="#">Sample_pro</a>	Complete	Identification > Packaging		Discovered(N/A)
<input type="checkbox"/>	506	<a href="#">AnotherTest Project (0.1)</a>	Complete	Identification > Packaging		Need to resolve(7.8)
<input type="checkbox"/>	480	<a href="#">MoonSangWoong_TRAINING PROJECT (1.0)</a>	Complete	Identification > Packaging		Need to resolve(9.8)
<input type="checkbox"/>	475	<a href="#">mj.prj.(0.1)</a>	Complete	Identification > Packaging		Need to resolve(9.8)
<input type="checkbox"/>	469	<a href="#">jkh test.(1.0.0)</a>	Complete	Identification > Packaging		Need to resolve(9.8)
<input type="checkbox"/>	467	<a href="#">DY Training Project (1.0)</a>	Complete	Identification > Packaging		Need to resolve(10.0)

# 보안취약점 조회

- 오픈소스 버전에 따른 보안 취약점 점수 및 내용 확인 가능

The screenshot shows the FOSSLIGHT-LGE interface. On the left is a navigation menu with 'Vulnerability' selected. The main area displays search results for 'tomcat'. A table lists three vulnerabilities for 'tomcat\_native' version '1.1.23'. Below the table, a detailed view for CVE-2018-8019 is shown.

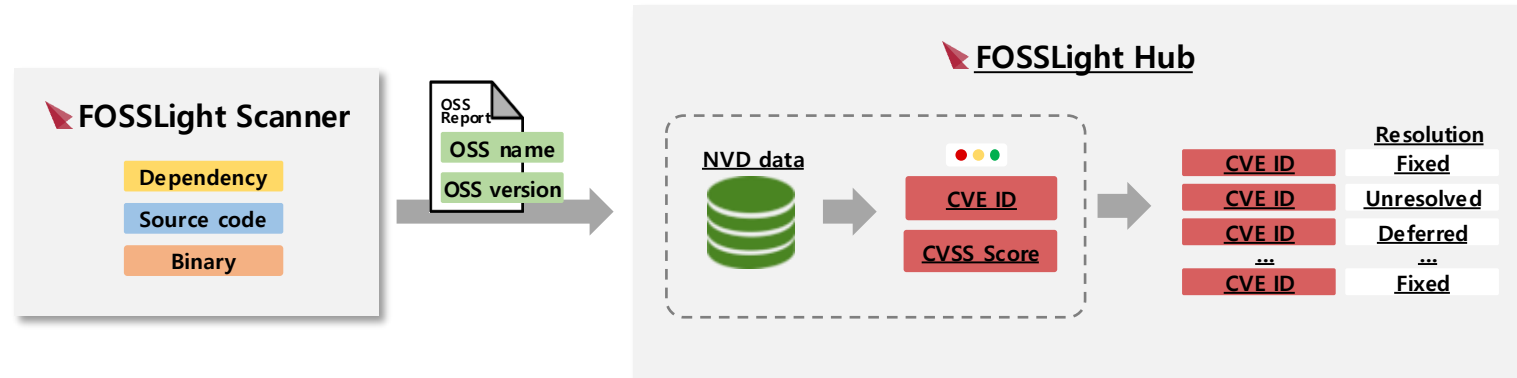
	OSS Name	Version	Score	CVE ID	Modified Date
1	tomcat_native	1.1.23	7.4	<a href="#">CVE-2018-8019</a>	2023-11-07
2	tomcat_native	1.1.23	7.4	<a href="#">CVE-2018-8020</a>	2023-11-07
3	tomcat_native	1.1.23	5.9	<a href="#">CVE-2017-15698</a>	2023-11-07

Below the table, the detailed view for CVE-2018-8019 is shown:

- CVE ID** : CVE-2018-8019
- Description** : When using an OCSP responder Apache Tomcat Native 1.2.0 to 1.2.16 and 1.1.23 to 1.1.34 did not correctly handle invalid responses. This allowed for revoked client certificates to be incorrectly identified. It was therefore possible for users to authenticate with revoked certificates when using mutual TLS. Users not using OCSP checks are not affected by this vulnerability. Al emplear un respondedor OCSP, Apache Tomcat Native desde la versión 1.2.0 hasta la 1.2.16 y desde la versión 1.1.23 hasta la 1.1.34 no gestionó correctamente las respuestas inválidas. Esto permitió que los certificados de cliente revocados se identificasen erróneamente. Por lo tanto, era posible que los usuarios se autenticasen con certificados revocados al emplear TLS mutuo. Los usuarios que no emplean comprobaciones OCSP no se han visto afectados por esta vulnerabilidad.

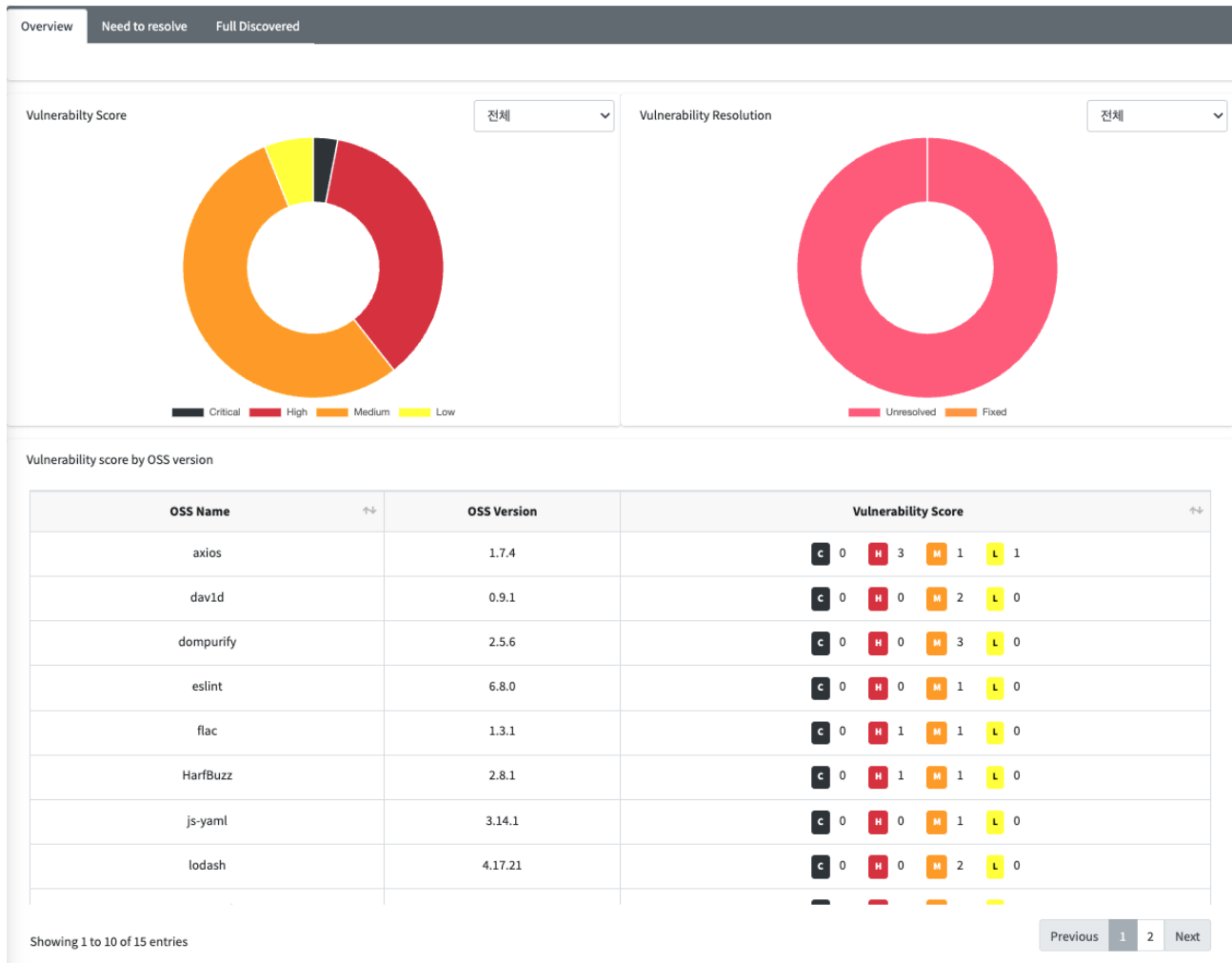
# 보안 프로세스 관리

- 프로젝트별로 발견된 보안취약점을 확인하고 해결 여부를 관리할 수 있음



# 보안 프로세스 관리

- 프로젝트별로 발견된 보안취약점을 확인하고 해결 여부를 관리할 수 있음



# 보안 프로세스 관리

- 프로젝트별로 발견된 보안취약점을 확인하고 해결 여부를 관리할 수 있음

<input type="checkbox"/>	OSS Name	OSS Versior	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerability Link	Affected SW Version Range	Security Comments
	~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>
<input type="checkbox"/>	axios	1.7.4	CVE-2025-27...	7.7	2025-03-07	Unresolved	<a href="https://nvd.nist.gov/vuln/deta">https://nvd.nist.gov/vuln/deta</a>		
<input type="checkbox"/>	axios	1.7.4	CVE-2025-58...	7.5	2025-09-12	Unresolved	<a href="https://nvd.nist.gov/vuln/deta">https://nvd.nist.gov/vuln/deta</a>		
<input type="checkbox"/>	axios	1.7.4	CVE-2025-62...	6.3	2026-04-09	Unresolved	<a href="https://nvd.nist.gov/vuln/deta">https://nvd.nist.gov/vuln/deta</a>		
<input type="checkbox"/>	axios	1.7.4	CVE-2026-25...	7.5	2026-02-09	Unresolved	<a href="https://nvd.nist.gov/vuln/deta">https://nvd.nist.gov/vuln/deta</a>		
<input type="checkbox"/>	dav1d	0.9.1	CVE-2023-32...	5.9	2023-05-10	Unresolved	<a href="https://nvd.nist.gov/vuln/deta">https://nvd.nist.gov/vuln/deta</a>		
<input type="checkbox"/>	dav1d	0.9.1	CVE-2024-1580	5.9	2024-02-19	Unresolved	<a href="https://nvd.nist.gov/vuln/deta">https://nvd.nist.gov/vuln/deta</a>		
<input type="checkbox"/>	dompurify	2.5.6	CVE-2025-15...	5.1	2026-03-03	Unresolved	<a href="https://nvd.nist.gov/vuln/deta">https://nvd.nist.gov/vuln/deta</a>		
<input type="checkbox"/>	dompurify	2.5.6	CVE-2026-0540	5.3	2026-03-03	Unresolved	<a href="https://nvd.nist.gov/vuln/deta">https://nvd.nist.gov/vuln/deta</a>		
<input type="checkbox"/>	eslint	6.8.0	CVE-2025-50...	5.5	2026-01-26	Unresolved	<a href="https://nvd.nist.gov/vuln/deta">https://nvd.nist.gov/vuln/deta</a>		
<input type="checkbox"/>	flac	1.3.1	CVE-2017-6888	5.5	2018-04-25	Unresolved	<a href="https://nvd.nist.gov/vuln/deta">https://nvd.nist.gov/vuln/deta</a>		
<input type="checkbox"/>	flac	1.3.1	CVE-2020-22...	7.8	2023-08-22	Unresolved	<a href="https://nvd.nist.gov/vuln/deta">https://nvd.nist.gov/vuln/deta</a>		

Page 1 of 1 | 200 | Count: 28

# 보안취약점 실시간 알림

- 보안 취약점 변경 사항에 대해 관리자 및 프로젝트 담당자에게 메일 알림

## FOSSLight Hub Notification

### [OSC] Vulnerability Discovered

#### « Vulnerability Information »

OSS ID	OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
22869	json-smart-v2	2.2.1	<a href="#">CVE-2021-27568</a>	9.1	An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as demonstrated by NumberFormatException. When it is not caught, it may cause programs using the library to crash or expose sensitive information.	2021-02-23	2022-05-12
15690	json-smart-v2	2.3	<a href="#">CVE-2021-27568</a>	9.1	An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as demonstrated by NumberFormatException. When it is not caught, it may cause programs using the library to crash or expose sensitive information.	2021-02-23	2022-05-12

\* This mail was sent by [osc.lge.com](mailto:osc.lge.com)

# SBOM 관리

- 특정 오픈소스 버전을 사용하는 프로젝트 조회 가능

The screenshot displays the SBOM management interface. At the top, there are tabs for 'Project', 'Self-Check', '315\_selfCheck', and '324\_selfCheck'. Below the tabs is a search bar with a magnifying glass icon highlighted by a red box. The search bar contains the text 'Project ID or Name' and a checkbox for 'My Project'. To the right of the search bar is a '+ Advanced Search' button with the text 'option selected' below it. Below the search bar are several filter fields: Status, Created Date, Division, Creator, Reviewer, Watcher, Network Service, Priority, Binary Name, Model Name, Distribution Type, OSS Notice, License Name, and 3rd Party Name. A red box highlights the 'openssl' project name and its version '1.0.0'. Below the filters are 'save conditions' and 'reset' buttons. At the bottom, there are 'Copy', 'Change', and 'BOM Compare' buttons. Below these buttons is a table with the following data:

ID	Project Name	Status	OSC Process	Download	Creator	Created Date
632	<a href="#">sbom test</a>	Progress	Identification > Packaging		ab	2023-12-06

# SBOM 변경 추적

+ Add new\_project\_from\_api  My Project  + Advanced Search

Copy

Status	OSS_Before	License_Before	OSS_After	License_After
add			npm:copy-anything (2.0.6)	MIT
add			soon	MIT
delete	mesqueeb-copy-anything (2.0.6)	MIT		
delete	mobis_psh	MIT		

Page 1 of 1 15 Count : 4

# 공급망 관리

- 타사에서 전달받은 Software 별 SBOM 관리 가능

**Mobile application (1.2) | Progress**

3rd party 🔗 🗑️ ↺ 📄 +

Pre-Review OSS bulk registration Save (Binary DB)

+ 🗑️ ✎️ ⬇️

<input type="checkbox"/>	ID	Binary Name	OSS Name	OSS Version	License	Download	Homepage	Copyright	Tr	Vulnerability
		~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="checkbox"/> x	~ <input type="checkbox"/> x	~ <input type="text"/> x	>=	<input type="checkbox"/>
<input type="checkbox"/>	1	sample.jar	android-logging-log4j	1.0.3	Apache-2.0	https://c	<a href="https://c">https://c</a>			
<input type="checkbox"/>	2	multi.jar	angularjs-dropdown-multiselect	1.11.8	MIT	https://r	<a href="http://d">http://d</a>	Copyright (c		
<input type="checkbox"/>	3	dbus.so	dbus-java	2.7	AFL-2.1	https://c	<a href="https://v">https://v</a>	Copyright (c		

# FOSSLight 설치 및 관리

---

# 개발 환경 설정

- [https://fosslight.org/hub-guide/advanced/1\\_developer.html](https://fosslight.org/hub-guide/advanced/1_developer.html)

The screenshot displays the FOSSLight Guide website. The left sidebar contains a search bar and a navigation menu with categories like 'FOSSLIGHT HUB', 'FOSSLIGHT HUB BASIC TUTORIALS', and 'FOSSLIGHT HUB ADVANCED'. The main content area is titled 'Developer Documentation' and includes a 'Note' section stating that source code can be downloaded and executed. Below this, there are sections for 'FOSSLight Hub 소스 다운로드' (FOSSLight Hub source code download) and '설치 및 실행 방법 - 1' (Installation and execution method - 1), which mentions using Docker. A code block shows the command 'docker-compose up --build'. Further down, there is a '요구사항' (Requirements) section listing Java 11, MariaDB 10.0, and MySQL 5.6, and another '개발 환경' (Development environment) section listing Spring Boot 2.1.x, Gradle 6.x, Git, Spring Tool Suite, and UTF-8 encoding.

# 개발 환경 설정

## • 소스 코드 빌드 & 실행

- Java, MariaDB 설치 필요

1. JAVA를 설치합니다.: <https://openjdk.java.net>
2. DDL : [fossilight\\_create.sql](#)
3. MariaDB 또는 Mysql 설치합니다. : <https://mariadb.org/download>
4. Database 생성 및 초기 Data 등록

```
mysql -u root -p < fossilight_create.sql
```

plaintext

## • Docker로 빌드 & 실행

- 자동으로 DB, Java 세팅하여 쉽게 실행 가능

### 개발 환경

- [Docker](#)
- [Docker Compose](#)

### 빌드 및 실행

```
docker-compose up --build
```

plaintext

초기 NVD Data Setting 필요

# DB 백업 및 복구

2. License

3. Open Source

4. Project

5. 3rd Party

6. Binary DB

7. Vulnerability

8. Self-Check

9. System

## FOSSLIGHT HUB BASIC TUTORIALS

Project

Self-Check

## FOSSLIGHT HUB TIPS

- ☒ Tips: Common

- ☒ Tips: Project

- ☒ Tips: Use Case

- ☒ Tips: Vulnerability

## FOSSLIGHT HUB ADVANCED

Developer Documentation

REST API

## ☒ Maintenance

- ☒ DB 백업 및 복구하기

- DB 버전 업그레이드하기

- NVD Data를 2002년 Data부터 다운로드 받

- 🏠 FOSSLight Homepage

## Maintenance

### Note

FOSSLight Hub를 운영하는 데 유용한 가이드입니다.

## DB 백업 및 복구하기

### 1. 백업

선택1. 전체 백업

```
mysqldump -u[아이디] -p[패스워드] [데이터베이스명] > [백업파일명].sql
```

```
$ mysqldump -ufossilight -pfossilight fossilight > fossilight_backup.sql
```

plaintext

선택2. FOSSLight 최신 버전으로 업데이트를 위한 DB 백업 (Data만 추출)

```
mysqldump -u[아이디] -p[패스워드] [데이터베이스명] --no-create-info > [백업파일명].sql
```

```
$ mysqldump -ufossilight -pfossilight fossilight --no-create-info > fossilight_backup.sql
```

plaintext

### 2. 복구

1. 버전에 따른 Table 구조를 반영하기 위해 빈 DB를 새로 만들고 기본 값을 설정합니다. [Developer Documentation - 다운로드 & 설치 - 4. Database 생성 및 Data 초기 등록](#)

2. 백업한 파일로 복구합니다. `mysql -u[아이디] -p[패스워드] [데이터베이스명] < [백업파일명].sql`

```
$ mysql -ufossilight -pfossilight fossilight < fossilight_backup.sql
```

DB migration Script 제공

# FOSSLight Hub 호환성

- 다른 시스템과 연동할 수 있도록 REST API 제공
- TOKEN은 User Settings에서 발행 가능

Swagger  
Supported by SMARTBEAR

Select a definition v2

## FOSSLight Hub Open API <sup>1</sup>

[ Base URL: demo.fossilight.org/ ]  
<https://demo.fossilight.org/v2/api-docs?group=v2>

Authorize

**1. OSS & License** Api Oss V 2 Controller

- GET /api/v2/licenses Search License Info
- GET /api/v2/oss Search OSS List
- POST /api/v2/oss Register New OSS

**2. 3rd Party** Api Partner V 2 Controller

**3. Project** Api Project V 2 Controller

**4. Vulnerability** Api Vulnerability V 2 Controller

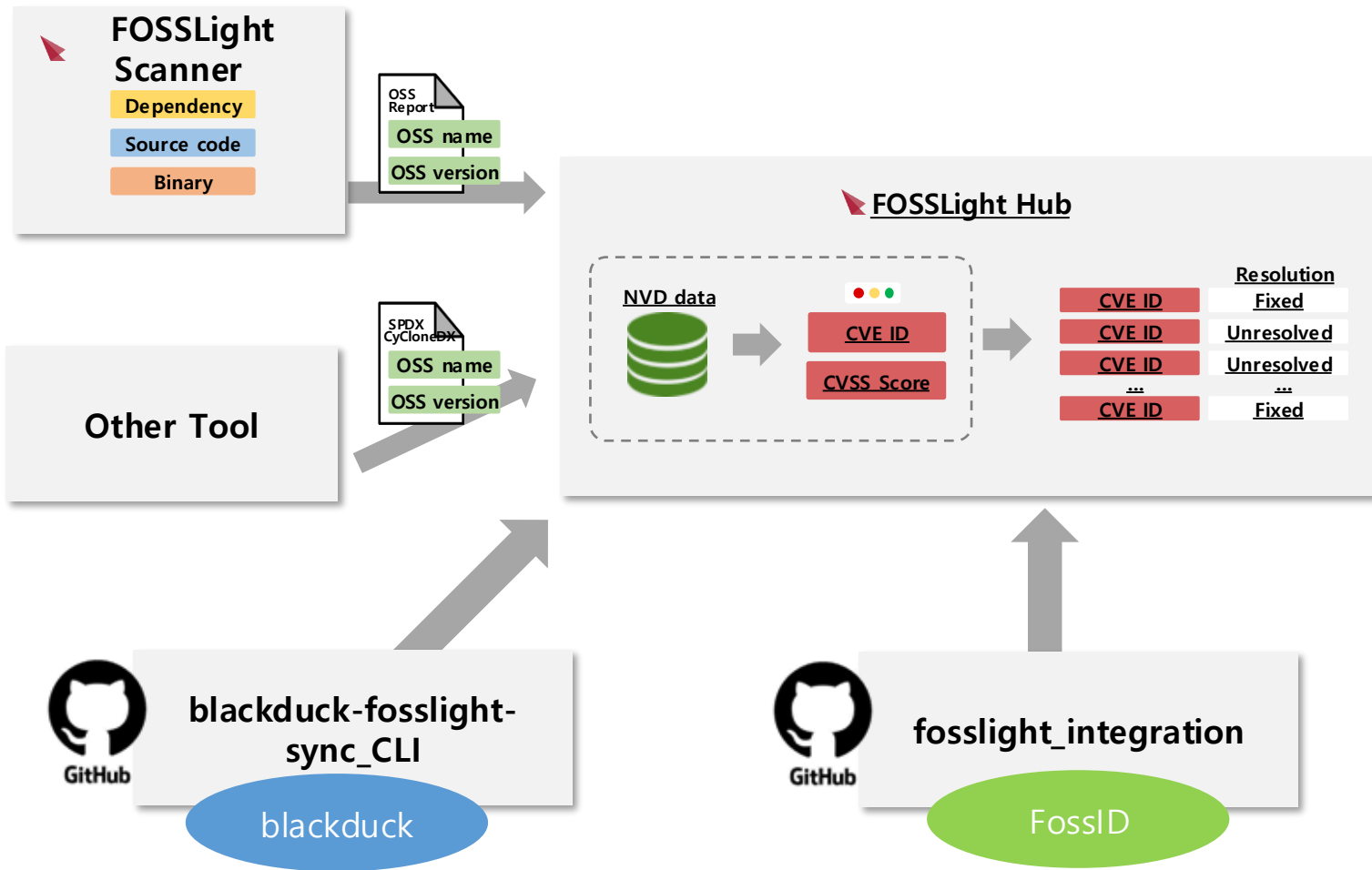
**5. SelfCheck** Api Self Check V 2 Controller

**6. Code v2** Api Code V 2 Controller

**7. Binary** Api Bat V 2 Controller

# FOSSLight Hub 호환성

- FOSSLight Scanner 외 다른 툴의 SBOM 업로드 가능



# FOSSLight Scanner 사용시 주요 장점

- Transitive Dependency 구조를 tree 형태로 시각화하여 제공
- FOSSLight Binary Scanner DB의 자동 축적

```

=== [PRJ-5081] Project Dependency Tree Export ===
Generated at: Wed Apr 22 11:15:06 KST 2026

pkg:npm/%40fontawesome/react-fontawesome
├─ pkg:npm/%40fontawesome/fontawesome-svg-core
├─ pkg:npm/react
├─ pkg:npm/prop-types
│   └─ pkg:npm/react-is
│       └─ pkg:npm/object-assign
│           └─ pkg:npm/loose-envify
│               └─ pkg:npm/js-tokens
pkg:npm/amazon-kinesis-video-streams-webrtc
├─ pkg:npm/json-schema
├─ pkg:npm/xml2js
│   └─ pkg:npm/xmlbuilder
│       └─ pkg:npm/sax
├─ pkg:npm/tslib
├─ pkg:npm/ua-parser-js
├─ pkg:npm/isomorphic-webcrypto
│   └─ pkg:npm/react-native-secure-random
│       └─ pkg:npm/react-native
│           └─ pkg:npm/base64-js
├─ pkg:npm/str2buf
├─ pkg:npm/%40unimodules/core
│   └─ pkg:npm/compare-versions
├─ pkg:npm/expo-random
│   └─ pkg:npm/expo
│       └─ pkg:npm/react
│           └─ pkg:npm/%40expo/config
│               └─ pkg:npm/slugify
└─ pkg:npm/require-from-string
  
```



**THANK YOU !**

