

입문자를 위한 FOSSLight 소개

FOSSLight Hub

LG전자 최혜성



LG Open Source

FOSSLight Hub

오픈소스 관리

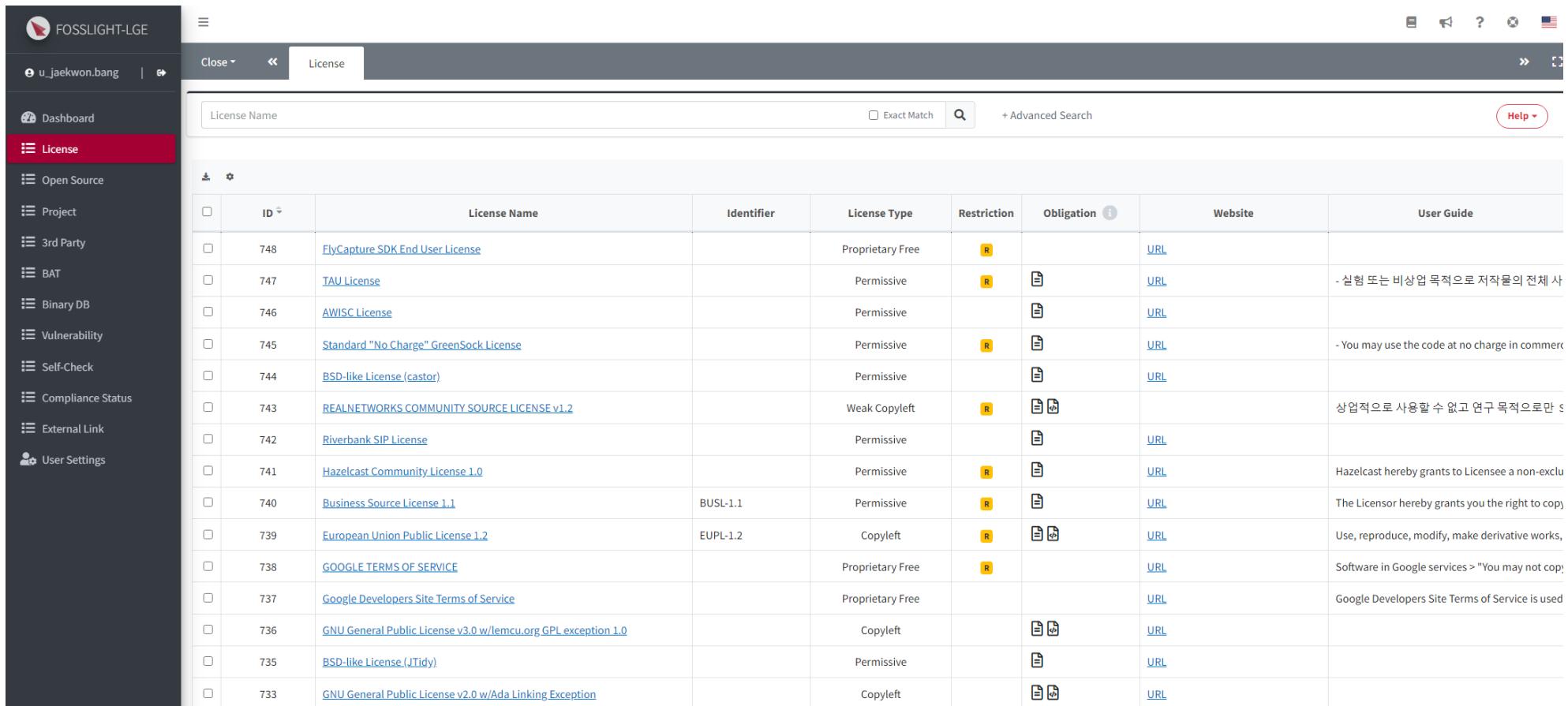
- 오픈소스 버전 별로 라이선스 및 의무 사항 관리

The screenshot shows the FOSSLIGHT-LGE web application interface for managing open-source components. The left sidebar has a dark theme with red highlights for 'Open Source'. The main area is titled 'Open Source' and includes a search bar with 'OSS Name' and 'Exact Match' options, and a 'Help' button. A table lists ten open-source entries:

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

라이선스 관리

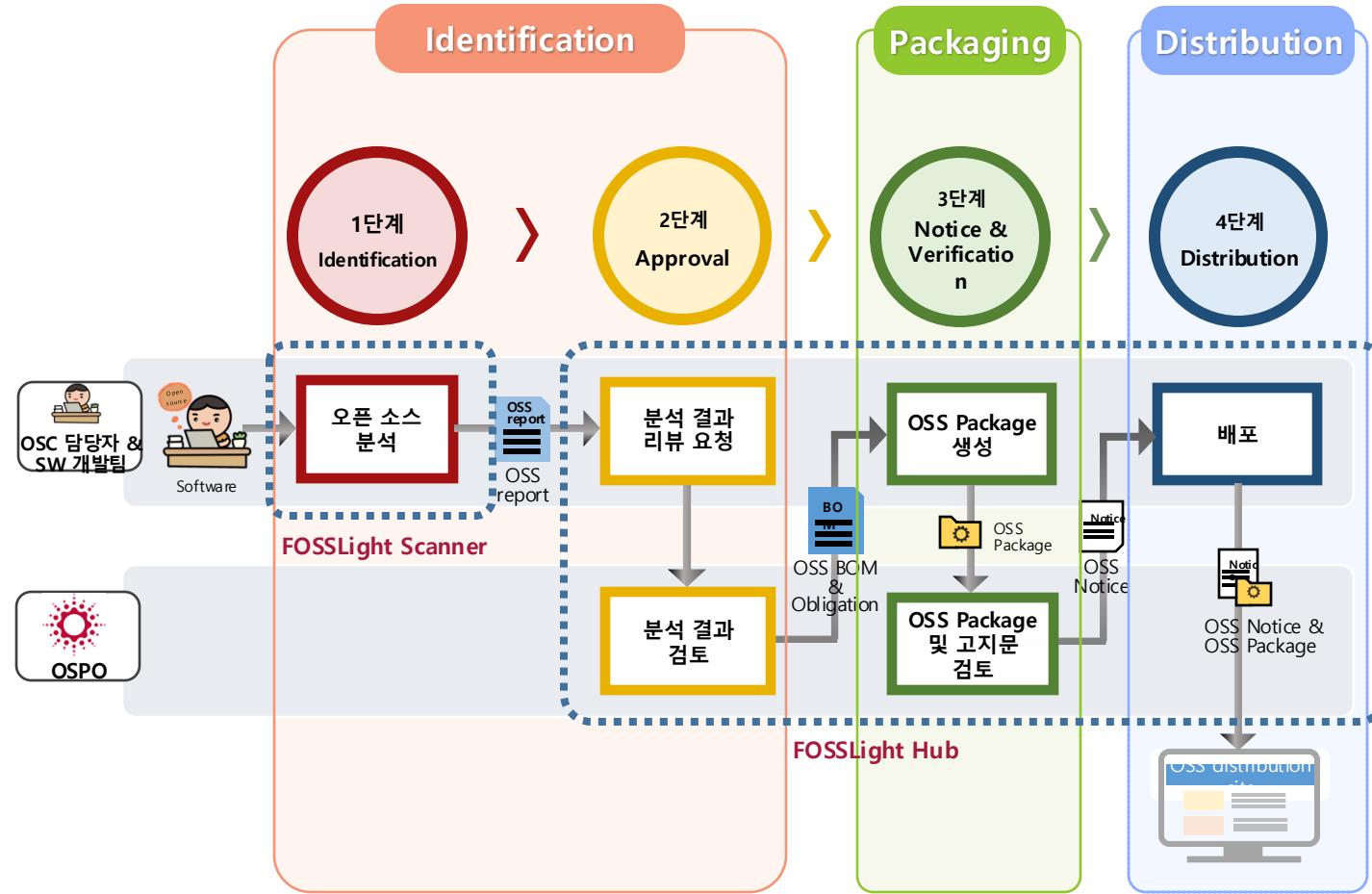
- 라이선스 별로 의무사항, 제약사항 관리



The screenshot shows the FOSSLIGHT-LGE web application interface for managing licenses. The left sidebar contains navigation links for Dashboard, License (which is selected and highlighted in red), Open Source, Project, 3rd Party, BAT, Binary DB, Vulnerability, Self-Check, Compliance Status, External Link, and User Settings. The main content area has a header with 'Close ▾', a back arrow, the title 'License', and a search bar with 'License Name', 'Exact Match' checkbox, and a magnifying glass icon. Below the header is a search bar with '+ Advanced Search' and a 'Help ▾' button. The main table lists various licenses with columns for ID, License Name, Identifier, License Type, Restriction, Obligation, Website, and User Guide. Each row includes a checkbox and a link to the license details.

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

참고) LG전자 오픈소스 컴플라이언스 프로세스



컴플라이언스 프로세스 관리

- 컴플라이언스 프로세스 단계별 진행 현황 및 이력 조회
- 프로젝트, 부서, 오픈소스별 검색

ID	Title	Progress	Identification	Packaging	Distribution	Discovered(N/A)	CTO SW센터	csg/*/SW...	2025-11-10	2025-11-10
13023	vuldoc_cvepatch_1110_203614_654	Progress	Identification >	Packaging >	Distribution	Discovered(N/A)	CTO SW센터	csg/*/SW...	2025-11-10	2025-11-10
13022	vuldoc_cvepatch_1110_203142_653	Progress	Identification >	Packaging >	Distribution	Discovered(N/A)	CTO SW센터	csg/*/SW...	2025-11-10	2025-11-10
13021	vuldoc_cvepatch_1110_184240_652	Progress	Identification >	Packaging >	Distribution	Discovered(N/A)	CTO SW센터	csg/*/SW...	2025-11-10	2025-11-10
13020	vuldoc_cvepatch_1110_182443_651	Progress	Identification >	Packaging >	Distribution	Discovered(N/A)	CTO SW센터	csg/*/SW...	2025-11-10	2025-11-10
13019	[STYLER]SC3GME50_MAIN(1)	Request	Identification >	Packaging >	Distribution	Discovered(N/A)	HS	조태환/선...	2025-11-10	2025-11-12

OSS(Open Source Software) 고지문 발급

- 사용된 오픈소스와 저작권, 라이선스를 고지하기 위한 OSS 고지문 발급
- 공개 대상 소스코드를 취합한 OSS 패키지 리뷰
- 지원 포맷 : HTML, TEXT, SPDX, CycloneDX

Open Source Software Notice

OSSN

This product from LG Electronics, Inc. contains the open source software detailed below (hereinafter referred to as "the Program"). The following table provides information about each piece of open source software included following this notice for the terms and conditions of their use.

Open Source	License	
junit 4.12	EPL-1.0	

The source code for the above may be obtained free of charge from LG Electronics, Inc. upon request. LG Electronics, Inc. also provide open source code to you on CD-ROM for a charge covering the cost of shipping, handling, and packaging. This offer is valid for three years after our last shipment of this product.

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 오픈소스 및 라이선스 리스트 업로드 후 의무사항, 보안 취약점 확인 가능

The screenshot shows the FOSSLight Self-Check interface. At the top, there's a navigation bar with 'Close', 'Self-Check', and the project ID '1341_selfCheck'. Below it is a 'Watcher' section. The main content area has tabs for 'Self-Check' (which is active) and 'Notice'. On the left, there's a 'FOSSLight Report' section with a file named 'fosslight.xlsx' from March 29, 2024, at 17:23:37. On the right, there's a detailed view of the Apache License 2.0, including its text and terms.

License Name	Identifier	License Obligat	Restrict	Website	Nick Name
Apache License 2.0	Apache-2.0	Permis:		URL	#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.

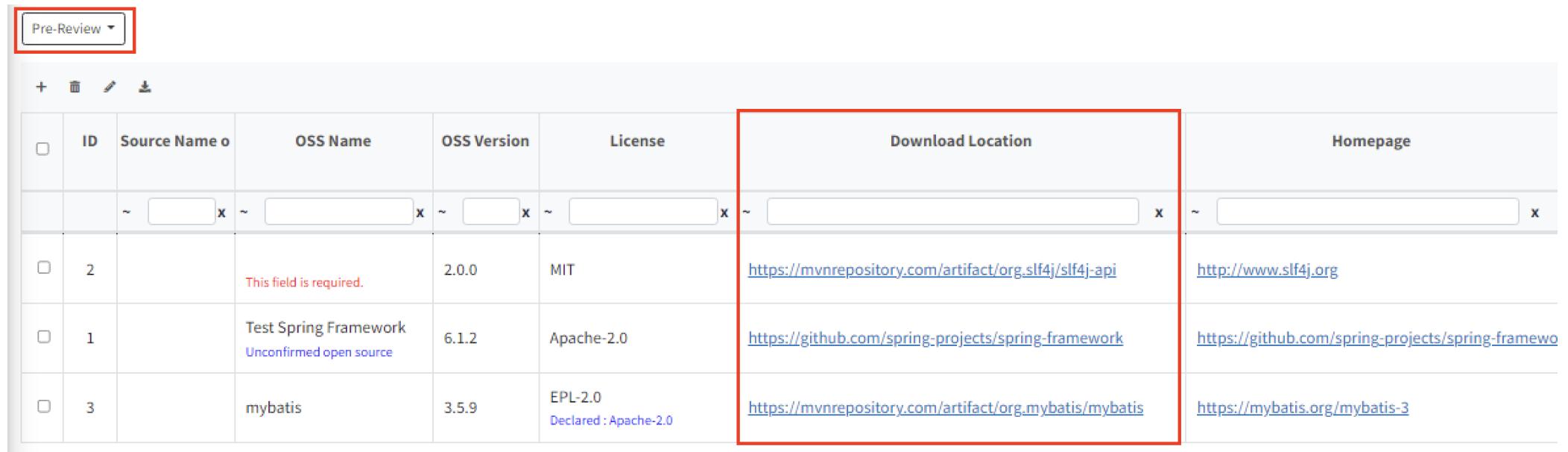
"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether 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 (Pre-Review)

- 다운로드 경로(URL)로 오픈소스 및 라이선스 정보 확인 가능



	ID	Source Name	OSS Name	OSS Version	License	Download Location	Homepage
	2		This field is required.	2.0.0	MIT	https://mvnrepository.com/artifact/org.slf4j/slf4j-api	http://www.slf4j.org
	1		Test Spring Framework Unconfirmed open source	6.1.2	Apache-2.0	https://github.com/spring-projects/spring-framework	https://github.com/spring-projects/spring-framework
	3		mybatis	3.5.9	EPL-2.0 Declared : Apache-2.0	https://mvnrepository.com/artifact/org.mybatis/mybatis	https://mybatis.org/mybatis-3

사전 점검 (Pre-Review)

- 다운로드 경로(URL)로 오픈소스 및 라이선스 정보 확인 가능

Pre-Review

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

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

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

Change License

사전 점검 (Pre-Review)

- 다운로드 경로(URL)로 오픈소스 및 라이선스 정보 확인 가능

The screenshot shows a software interface titled "Pre-Review". At the top left is a dropdown menu with "Pre-Review" selected. Below it is a toolbar with icons for add (+), search (magnifying glass), edit (pencil), and delete (trash). The main area is a table with columns: ID, Source Name (with a required field indicator), OSS Name, OSS Version, License, Download Location, and Homepage.

ID	Source Name	OSS Name	OSS Version	License	Download Location	Homepage
2		This field is required.	2.0.0	MIT	https://mvnrepository.com/artifact/org.slf4j/slf4j-api	http://www.slf4j.org
1		Test Spring Framework Unconfirmed open source	6.1.2	Apache-2.0	https://github.com/spring-projects/spring-framework	https://github.com/spring-projects/spring-framework
3		mybatis	3.5.9	EPL-2.0 Declared : Apache-2.0	https://mvnrepository.com/artifact/org.mybatis/mybatis	https://mybatis.org/mybatis-3

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

A modal dialog box displays a table with four columns: Result, Download location, OSS name (now), and Registered OSS name (to be changed). The second row of the table is highlighted with a red box.

Result	Download location	OSS name (now)	Registered OSS name (to be changed)
	https://mvnrepository.com/artifact/org.slf4j/slf4j-api	This field is required.	slf4j
	https://github.com/spring-projects/spring-framework	Test Spring Framework Unconfirmed open source	Spring Framework

At the bottom left of the modal is a button labeled "Change OSS Name".

사전 점검 (Pre-Review)

- 오픈소스 라이선스 의무 사항 확인 가능함

The screenshot displays the FOSSLight Self-Check application interface. On the left, there's a sidebar with tabs for 'Watcher' (selected), 'Self-Check' (active), and 'Notice'. Below it is a 'FOSSLight Report' section with a file named 'fosslight.xlsx' from 2024-03-29 17:23:37. On the right, a detailed view of the Apache-2.0 license is shown, including its name, identifier, obligations, restrictions, website, and nickname. A 'License text' section provides the full Apache License text, which includes definitions for terms like 'License', 'Licensor', 'Legal Entity', and 'You', along with terms for reproduction, distribution, and modification.

License Name	Identifier	License Obligat	Restrict	Website	Nick Name
Apache License 2.0	Apache-2.0	Permis:		URL	#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 레포지토리 주소 입력만으로 오픈소스 라이선스 의무사항 확인 가능

The screenshot shows a web-based application interface for managing open-source software. At the top, there are tabs for "Self-Check" and "Notice". The "Self-Check" tab is active, indicated by a dark grey background. On the right side of the header are icons for sharing, deleting, and other actions.

In the main area, there are two radio button options: "Upload Analysis" (unchecked) and "URL" (checked). Below this is a text input field labeled "Enter the link of the source to be analyzed" containing the URL "http://github.com/LGE-OSS/example". To the right of the URL input is a blue "send" button.

Below the analysis section is a dropdown menu labeled "Pre-Review". Underneath it are several small icons: a plus sign, a trash can, a pencil, and a download arrow.

The most prominent feature is a large table with a light grey header and white rows. The columns are labeled as follows:

ID	Binary Name or So	OSS Name	OSS Ver:	License	Download	Homepage	Copyright Text	OSS Licer	User	Vuln	Oblig	Resti	Guidability
	~	x	~	x	~	x	~	x	~	x	~	x	=

FOSSLight Hub로 보안 취약점 관리하기

보안 취약점 조회

- 오픈소스 버전별 보안 취약점 점수 및 상세 내용 확인 가능

The screenshot shows the FOSSLIGHT-LGE web application interface. On the left, there is a sidebar with various navigation options: Dashboard, License, Open Source, Project, 3rd Party, BAT, Binary DB, Vulnerability (which is highlighted in red), Self-Check, Compliance Status, External Link, User Settings, and System Restart Time (12 ~ 13, 18 ~ 19 (KST)).

The main content area has a search bar at the top with the text "Vulnerability" and a search term "tomcat". Below the search bar is a table with the following columns: OSS Name, Version, Score, CVE ID, and Modified Date.

	OSS Name	Version	Score	CVE ID	Modified Date
1	tomcat_native	1.1.23	7.4	CVE-2018-8019	2023-11-07
2	tomcat_native	1.1.23	7.4	CVE-2018-8020	2023-11-07
3	tomcat_native	1.1.23	5.9	CVE-2017-15698	2023-11-07

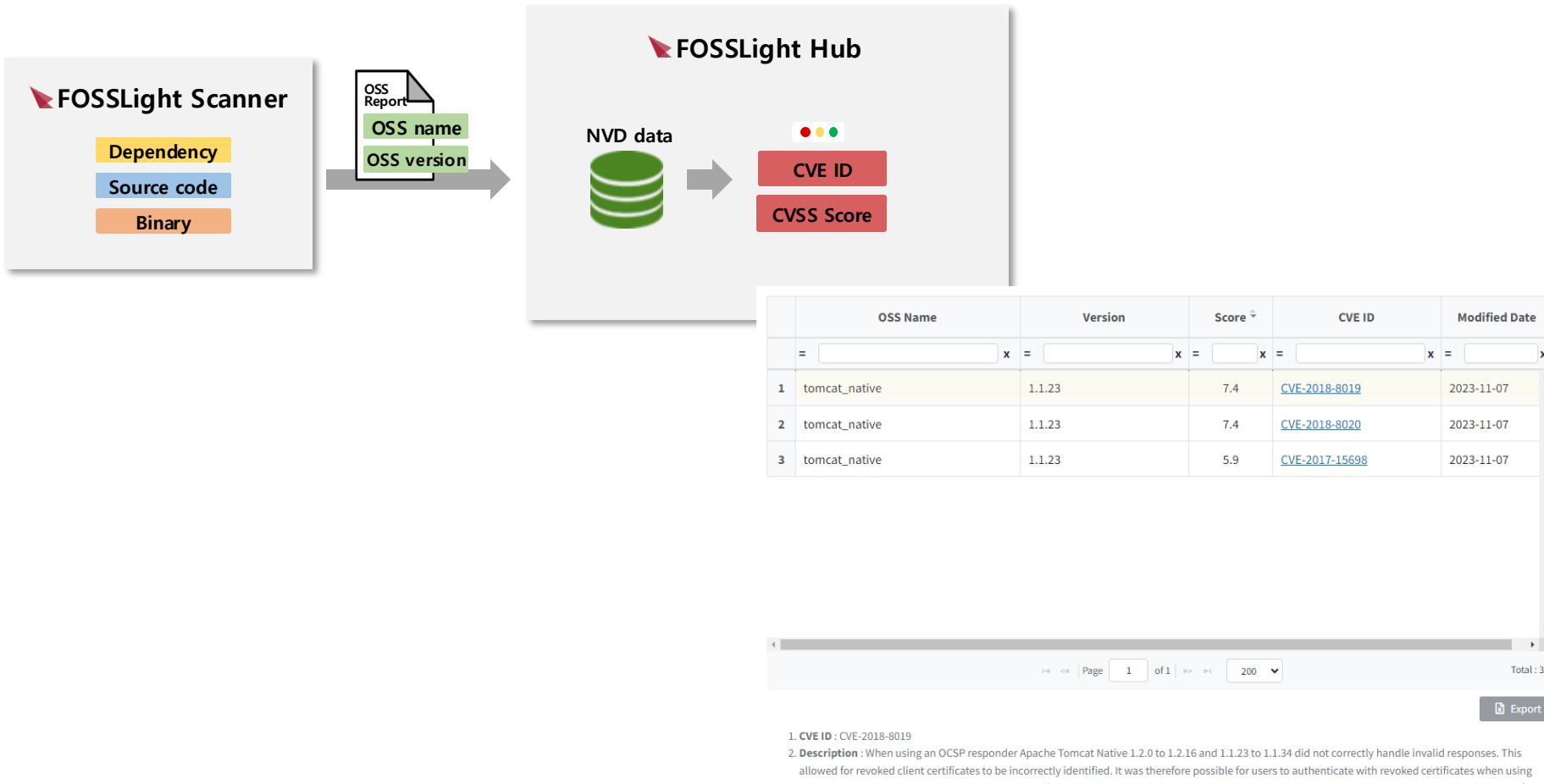
Below the table, there is a list of links labeled "Apache Tomcat" (repeated 8 times). At the bottom right of the table, there is a "Total : 3" label and an "Export" button.

Below the table, there is a detailed description of the first vulnerability:

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.

보안 취약점 관리

- 오픈소스 분석한 결과를 FOSSLight Hub에 업로드하여 보안 취약점 조회 및 관리 가능



보안 취약점 확인

- 제품별 프로젝트 등록을 통한 보안 취약점 확인

The screenshot shows a software application interface for managing open source projects and their vulnerabilities. The main window has a dark header bar with 'Close ▾' and '<>' buttons, followed by tabs for 'Project' (selected), '3rd party', 'DEP', 'SRC', 'BIN', and 'BOM'. Below the tabs is a toolbar with '+ Add' (highlighted in red), 'Project ID or Name', 'Copy', 'Change', 'BOM Compare', and a search icon. On the right side of the toolbar are 'Auto Analysis' and 'OSS bulk registration' buttons, and a 'Save (Binary DB)' button.

The left panel displays a table of projects:

ID	Project Name	Status
5165	Auto Update Program	Pro
5113	test (23 Copied54)	Final
5070	Sample (23)	Final
5069	User Management System	Pro
5068	Scanner	Pro
5067	db test (2 Copied)	Pro
5066	Source Analyzer (1)	Re
5065	db test (2)	Re
5044	Purchase Management	Re

The right panel displays a detailed table of dependencies and their vulnerabilities:

ID	Referen	OSS Name	OSS Version	License	Download Locat	Homepage	Copyright Text	Vulnerability	Notify Sourc	Restrictio	admin check
50	DEP	gax-java	0.74.0 Unconfirmed vc	BSD-3-Clause	https://mvnrepo	https://mv			<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
36	DEP	OSGi Resource L	1.0.1 Unconfirmed vc	CDDL-1.1	https://mvnrepo	https://mv			<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
17	DEP	gax-java	1.57.0 Unconfirmed vc	BSD-3-Clause	https://mvnrepo	https://mv			<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
100	DEP	Netty	4.1.50 Unconfirmed vc	Apache-2.0	https://mvnrepo	https://mv		HIGH	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
60	DEP	firebase-admin	7.1.0 Unconfirmed vc	Apache-2.0	https://mvnrepo	https://mv			<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
82	DEP	Netty	4.1.66 Unconfirmed vc	Apache-2.0	https://mvnrepo	https://mv		HIGH	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

At the bottom of the interface, there is a navigation bar with icons for back, forward, and search, followed by 'Page 1 of 1' and a page number '15'.

보안 취약점 실시간 알림

- 보안 취약점 변경 사항 발생 시 관리자 및 프로젝트 담당자에게 이메일 알림

FOSSLight Hub Notification

[OSC] Vulnerability Discovered

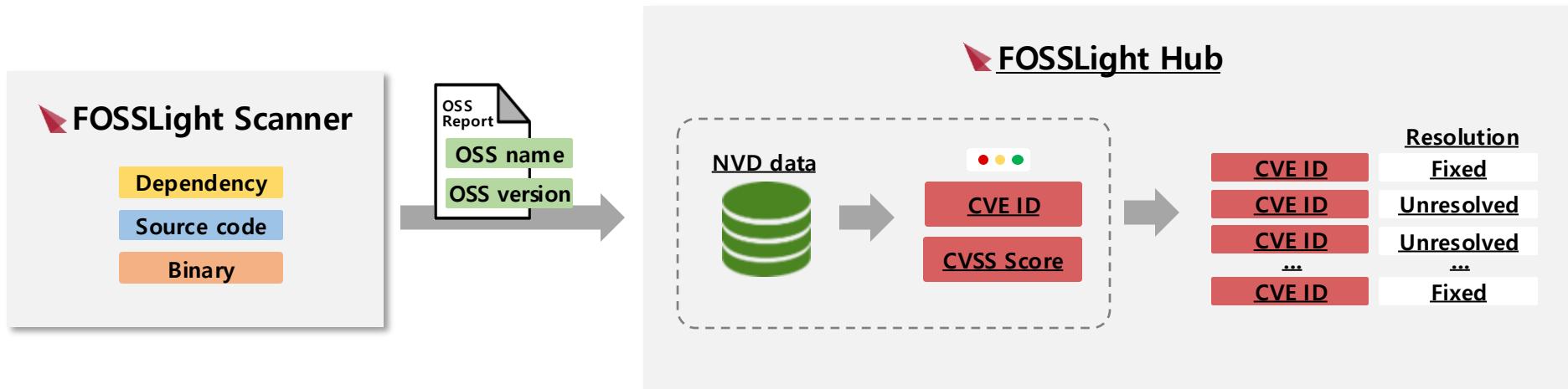
« Vulnerability Information »

OSS ID	OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
22869	json-smart-v2	2.2.1	CVE-2021-27568	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	CVE-2021-27568	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

제품 보안취약점 수정 여부 관리 기능

- 프로젝트별 발견된 보안 취약점 확인과 해결 상태 관리 가능



Security 탭

- 프로젝트별 사용된 오픈 소스의 보안취약점 목록을 CVE ID별로 확인하고 해결 여부를 관리할 수 있음

The screenshot shows a web-based security reporting tool. At the top, there are three tabs: 'Overview' (selected), 'Need to resolve' (highlighted in red), and 'Full Discovered'. Below the tabs, a message states: 'A list of CVE IDs with a vulnerability score of 5.0 or higher for OSS targets based on the SBOM tab in the Identification step.' A section titled 'FOSSLight Security Report' includes an 'Upload' button and a 'Drag & Drop Files' area. The main content is a table with the following columns: OSS Name, OSS Version, CVE ID, CVSS SCORE, Published Date, Vulnerability Resolution, Vulnerability Link, and Security Comments. The 'Vulnerability Resolution' column is highlighted with a red border. The table lists nine entries, all of which are marked as 'Unresolved'.

OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerability Link	Security Comments
cocoon	2.1.9	CVE-2025-2...	7.5	2025-01-27	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2025-2	
cocoon	2.1.9	CVE-2020-1...	7.5	2020-09-11	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2020-1	
Linux Kernel	2.6.27	CVE-2010-2...	10.0	2010-09-07	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2010-2	
Linux Kernel	2.6.27	CVE-2010-2...	10.0	2010-09-08	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2010-2	
Linux Kernel	2.6.27	CVE-2009-0...	10.0	2009-01-07	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2009-0	
Linux Kernel	2.6.27	CVE-2009-4...	10.0	2010-01-12	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2009-4	
Linux Kernel	2.6.27	CVE-2015-1...	10.0	2015-03-16	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2015-1	
Linux Kernel	2.6.27	CVE-2008-5...	10.0	2008-11-18	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2008-5	

Security 탭 – Vulnerability Resolution

- **Vulnerability Resolution**

- 수정 여부에 따라 Resolution 값 저장 가능

A list of CVE IDs with a vulnerability score of 5.0 or higher for OSS targets based on the SBOM tab in the Identification step.

FOSSLight Security Report

Upload Drag & Drop Files

	OSS Name	OSS Ver	CVE ID	CVSS SCOF	Published Date	Vulnerability Resolution	Vulnerability Link	Security Comm
<input checked="" type="checkbox"/>	cocoon	2.1.9	CVE-2...	7.5	2020-...	Unresolved	https://nvd.nist.gov/	
<input type="checkbox"/>	cocoon	2.1.9	CVE-2...	7.5	2025-...	Unresolved	https://nvd.nist.gov/	
<input type="checkbox"/>	Linux Kernel	2.6...	CVE-2...	10.0	2014-...	Unresolved	https://nvd.nist.gov/	
<input type="checkbox"/>	Linux Kernel	2.6...	CVE-2...	10.0	2015-...	Unresolved	https://nvd.nist.gov/	

SBOM 관리

- 특정 오픈소스 버전을 사용하는 프로젝트 조회 가능

The screenshot shows a web-based application for managing SBOM (Software Bill of Materials) data. At the top, there is a navigation bar with tabs: 'Project' (selected), 'Self-Check', '315_selfCheck', and '324_selfCheck'. Below the navigation bar is a search panel with the following fields:

- + Add
- Project ID or Name:
- My Project
-
- + Advanced Search
option selected
- Status:
- Created Date:
- Divison:
- Creator:
- Reviewer:
- Watcher:
- Network Service:
- Priority:
- Binary Name:
- Model Name:
- Distribution Type:
- OSS Notice:
- License Name:
- Additional Information:
- Comment:
- 3rd Party Name:

Below the search panel are three buttons: 'save conditions' (with a download icon), 'reset' (with a circular arrow icon), and 'Copy', 'Change', and 'BOM Compare'.

The main content area displays a table with the following columns:

	ID	Project Name	Status	OSC Process	Download	Creator	Created Date
<input type="checkbox"/>	632	sbom test	Progress	Identification > Packaging	<input type="button" value=""/>	ab	2023-12-06

SBOM 변경 추적

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		

공급망 관리

- 타사에서 전달받은 Software 별 SBOM 관리 가능

Mobile application (1.2) | Progress

3rd party

Pre-Review ▾ OSS bulk registration Save (Binary DB)

ID	Binary Name	OSS Name	OSS Version	License	Download	Homepage	Copyright	Trademarks	Vulnerability
1	sample.jar	android-logging-log4j	1.0.3	Apache-2.0	https://ossindex-project.org/	https://ossindex-project.org/	Copyright (c) 2023	Apache Software Foundation	Log4j
2	multi.jar	angularjs-dropdown-multiselect	1.11.8	MIT	https://ossindex-project.org/	https://ossindex-project.org/	Copyright (c) 2023	AngularJS	AngularJS
3	dbus.so	dbus-java	2.7	AFL-2.1	https://ossindex-project.org/	https://ossindex-project.org/	Copyright (c) 2023	Free Software Foundation	DBus

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, CycloneDX 문서 지원 (ISO 표준)



SW 공급망 관리

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

FOSSLight 설치 및 관리

개발 환경 설정

- https://fosslight.org/hub-guide/advanced/1_developer.html

The screenshot shows the FOSSLight Guide website with the URL https://fosslight.org/hub-guide/advanced/1_developer.html. The page title is "Developer Documentation". The left sidebar contains navigation links for "FOSSLIGHT HUB", "FOSSLIGHT HUB BASIC TUTORIALS", "FOSSLIGHT HUB ADVANCED", "REST API", "FOSSLIGHT SCANNER", and "LEARN MORE". The main content area includes a "Note" section about downloading the source code, a "FOSSLight Hub 소스 다운로드" section, a "설치 및 실행 방법 - 1" section with Docker instructions, a "개발 환경" section listing Docker and Docker Compose, a "빌드 및 실행" section with a command-line interface example, a "설치 및 실행 방법 - 2" section, a "요구사항" section with system requirements (Java 11+, MariaDB/MySQL 5.6+, 8GB+ memory), and another "개발 환경" section with IDE and framework requirements.

Developer Documentation

Note

FOSSLight Hub 소스를 다운로드받아 직접 컴파일하여 실행할 수 있습니다.

FOSSLight Hub 소스 다운로드

FOSSLight Hub에서 소스를 다운로드 받습니다.

설치 및 실행 방법 - 1

Docker를 이용하여 빌드 및 실행합니다.

개발 환경

- Docker
- Docker Compose

빌드 및 실행

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

설치 및 실행 방법 - 2

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
- Git : <https://github.com/fosslight/fosslight>
- IDE : Spring Tool Suite
 - Lombok 설치 필요
- Project Character Set: UTF-8

개발 환경 설정

- 소스 코드 빌드 & 실행

- Java, MariaDB 설치 필요

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

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

More ...

- Docker로 빌드 & 실행

- 자동으로 DB, Java 세팅하여 쉽게 실행 가능

개발 환경

- Docker
- Docker Compose

빌드 및 실행

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

NVD Data 초기
다운로드 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
```

plaintext

```
$ mysqldump -ufosslight -pfosslight fosslight > fosslight_backup.sql
```

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

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

plaintext

```
$ mysqldump -ufosslight -pfosslight fosslight --no-create-info > fosslight_backup.sql
```

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

plaintext

```
$ mysql -ufosslight -pfosslight fosslight < fosslight_backup.sql
```

Migration
Script 제공

REST API

- 다른 툴과 연동할 수 있도록 REST API를 제공
 - TOKEN은 User Management에서 발행 가능

The screenshot shows the FOSSLight Hub Open API documentation interface. At the top, there is a header with the Swagger logo and a dropdown menu labeled "Select a definition" set to "v2". Below the header, the title "FOSSLight Hub Open API" is displayed with a small "1" indicating it's the latest version. A note below the title specifies the base URL as "enterprise.fosslight.org/" and provides a direct link: "https://enterprise.fosslight.org/v2/api-docs?group=v2". On the right side of the header, there is a green "Authorize" button with a lock icon. The main content area is divided into sections: "1. OSS & License", "2. 3rd Party", "3. Project", "4. Vulnerability", and "5. SelfCheck". Each section has a corresponding "Api" and "Controller" label. Under "1. OSS & License", there are four API endpoints listed: "GET /api/v2/licenses Search License Info", "GET /api/v2/oss Search OSS List", "POST /api/v2/oss Register New OSS" (this endpoint is highlighted with a green background), and "GET /api/v2/refine-download-location Refine OSS Download Location". Each endpoint entry includes a lock icon on the right.

System 메뉴

- Admin 권한으로 확인 가능한 시스템 관리 메뉴

The screenshot shows the FOSSLight web application interface. On the left is a dark sidebar with a navigation menu. The 'System' item is highlighted with a red box, and its sub-items are listed below it. The 'Code management' item is also highlighted with a red box. The main content area has a title bar with tabs: 'Close', '<<', 'Self-Check' (which is active), and 'Code management'. Below the title bar is a search bar with fields for 'Code No.' and 'Code Name' and a search icon. The main content is a table titled 'Code management' with columns: 'Code No.', 'Code Name', and 'Code Description'. The table contains 20 rows of data, each with a unique code number, name, and description. At the bottom of the table is a page navigation bar.

Code No.	Code Name	Code Description
100	Number of rows per a page	Number of records to be loaded per a page
101	order by cast column	Define cases for converting string to int for grid display
102	email type	
103	email contents	
104	email list contents	
110	email template file path	
111	email default contents	
120	File upload Extension	
121	Download Sample File	Location of sample files
122	Network Server license list	Licenses that has obligations for network server
200	Division	
201	License Type	
203	License Division	
204	License Composition Type	
205	Project Status	



THANK YOU !

