

# SBOM Tool Essentials

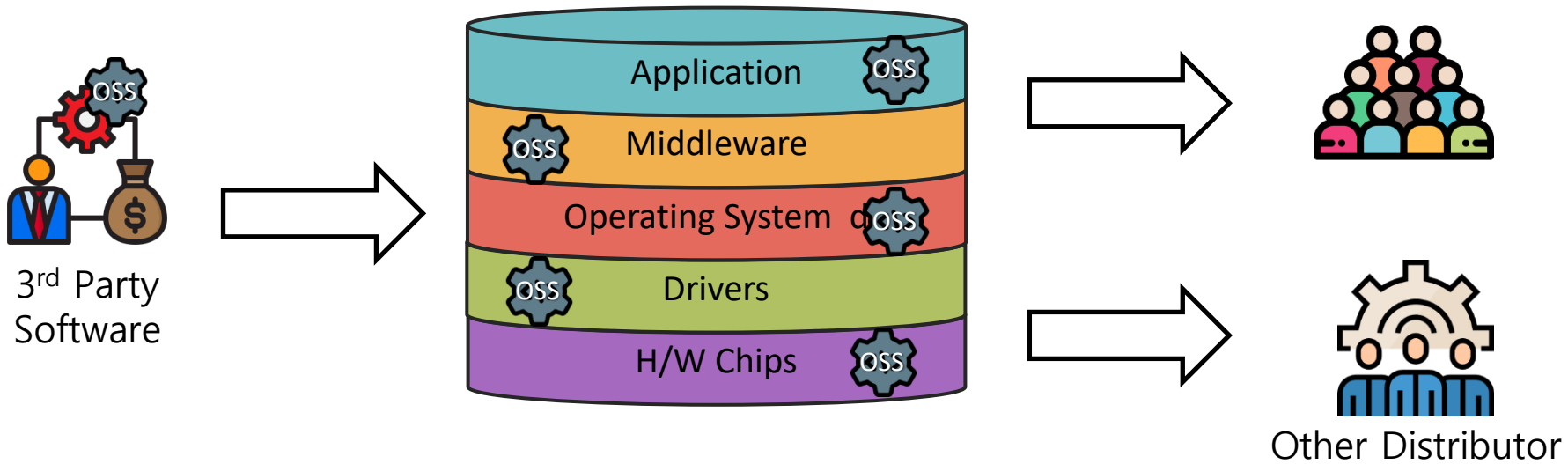
LG Electronics, Kyoungae Kim



# SBOM Tool

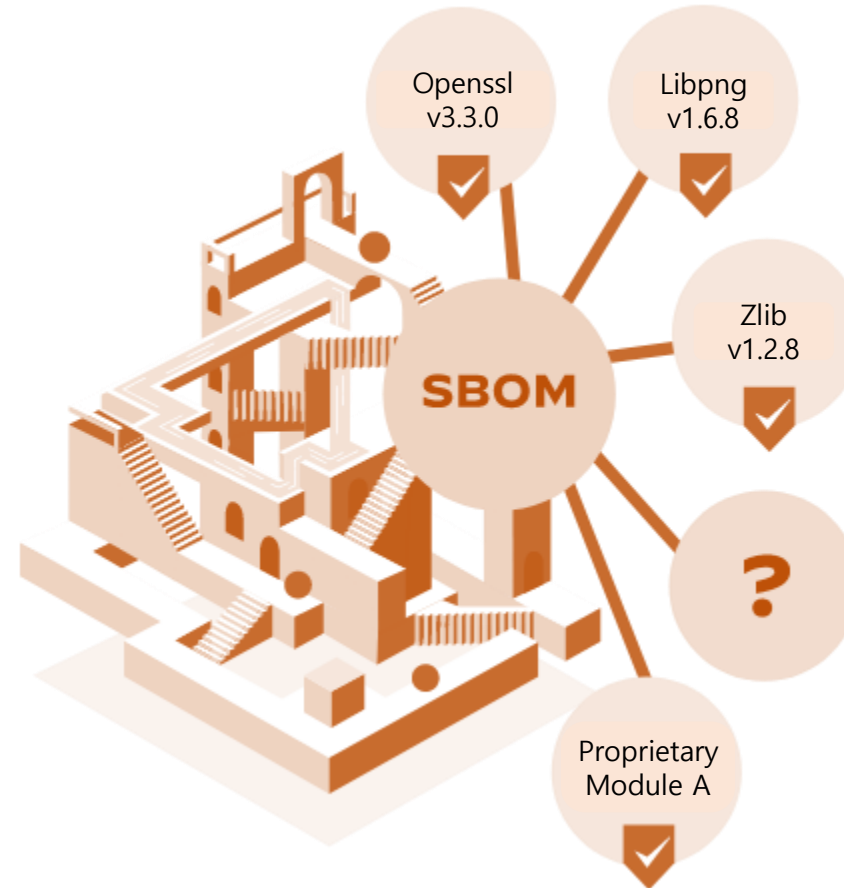
---

# Supply Chain Software



# SBOM (Software Bill Of Materials)

Baseline Software Component Information
Supplier Name
Component Name
Component Version
Unique Identifier
Dependency Relationship
Data Author Name
Timestamp
Licenses
Vulnerabilities



# Automation Support



**SBOM Creation Automation**

**SBOM Document Auto Creation**  
(ex. SPDX, CycloneDX, SWID Tags)

**CLI/API Support for Automation**

# Dependency Support



Dependency Scanning

Support Transitive Dependency

Ex. Support SPDX Document Field "relationships"

# Component Identification



**Many different component names should be managed by one**

**Ex. Apache tomcat, tomcat, apache-tomcat**

**-> One component**

# Operation



Support SBOM search

Tracking SBOM Changes

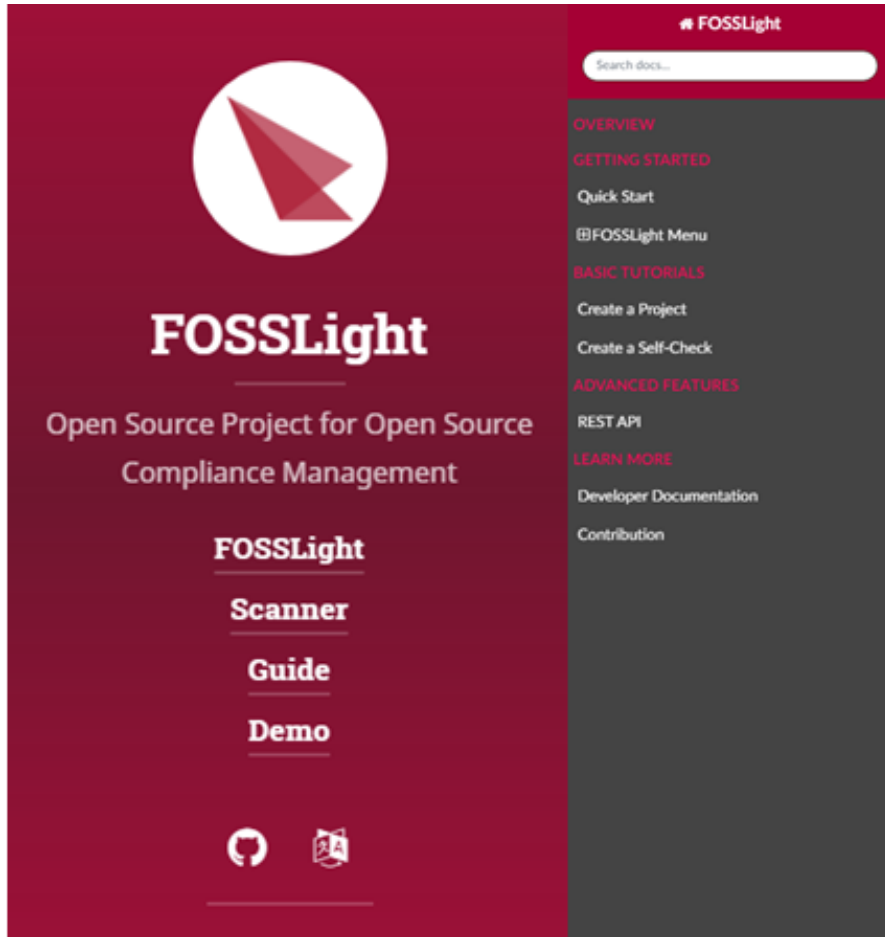
Real-time Notification



# FOSSLight

---

# FOSSLight Open Source Project



# / README.md

Kor / ㉿

## FOSSLight

To develop and distribute software containing open source software, you need to follow the OSC(Open Source Compliance) process. FOSSLight system is an integrated system that can process three steps of the OSC process sequentially.

### Features

#### Compliance Workflow



It can process the open source compliance workflow.

#### Compliance Hub



You can manage everything about open source compliance such as license, oss, vulnerability and others.

#### Scalability



It can be used with additional features (including FOSSLight scanner or other plugins).

### Function



Project



License / OSS



Vulnerability

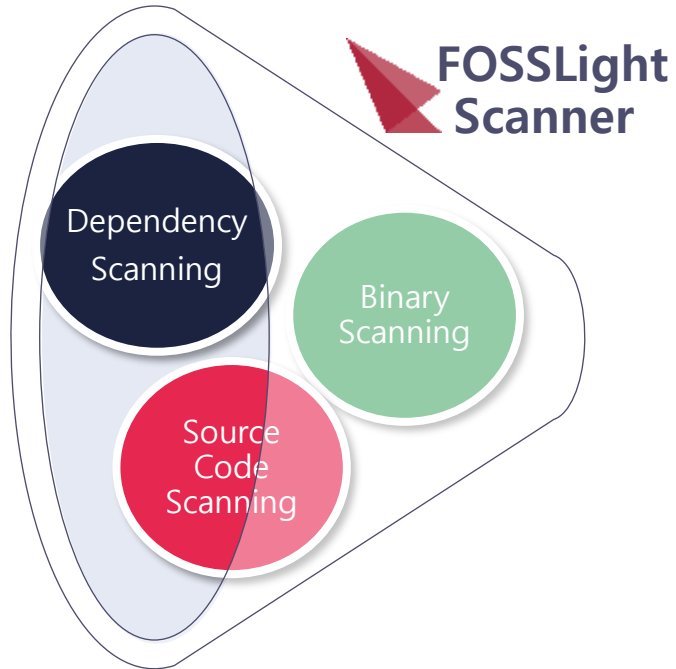


3rd Party



Self-Check

# FOSSLight Scanner + FOSSLight Hub

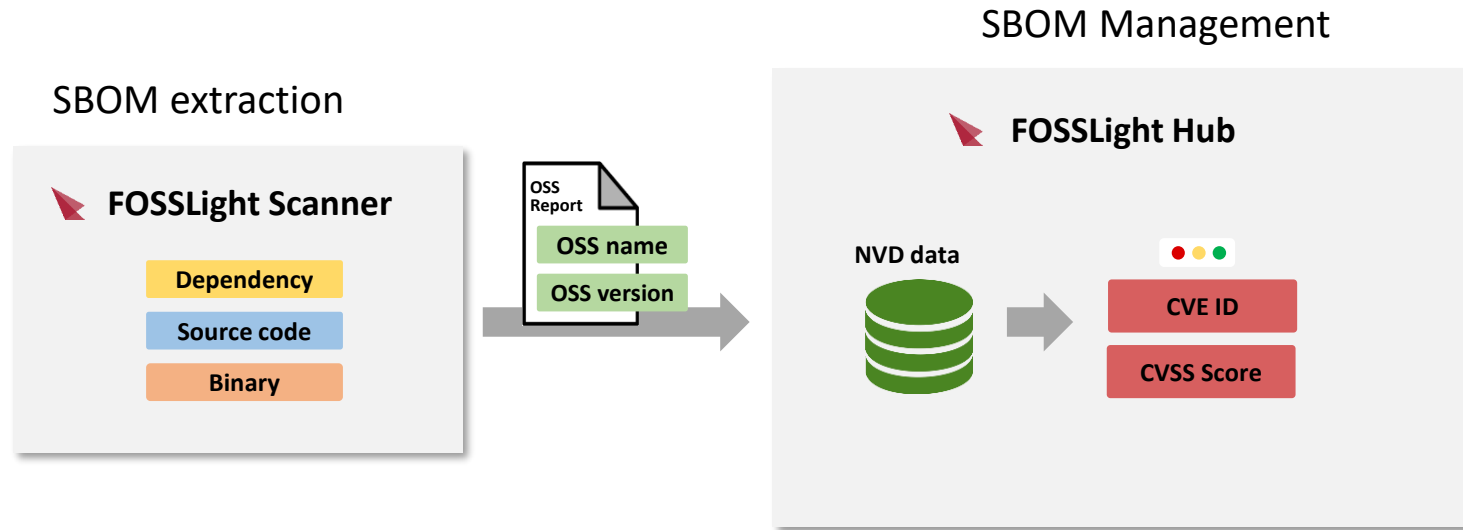


## OSS BOM

ID	Source Name or Path	OSS Name	OSS Version	License	Download Location	Homepage	Copyright Text
-	[Name of the Source File or Path / ]	[Name of the OSS used]	[Version Number]	[License of the OSS. Use]	[Download URL or a specific file]	[Web site that serves as a reference]	[The copyright holder]
1	/src/tools/busybox/	busybox	1.4	GPL-2.0	https://busybox.net/download	https://www.busybox.net	Copyright (c) 1999-20
2	/src/framework/curl/	curl	7.50.3	curl	https://github.com/curl/curl	http://curl.haxx.se	Copyright (c) 1996 -
3	/src/application/calendar/view.c	-	-	BSD-3-Clause	-	-	Copyright (c) 2016, N



# FOSSLight + Vulnerability



	OSS Name	Version	Score ⇅	CVE ID	Published Date
	= <input type="text"/> x	= <input type="text"/> x	= <input type="text"/> x	= <input type="text"/> x	= <input type="text"/> x
1	aihttp	3.6.2	6.1	<a href="#">CVE-2021-21330</a>	2022-08-11

# FOSSLight Hub

## Essential for SBOM Management

**FOSSLight**

v1.4.5

English

시스템관리 | Logout

Statistics

License List

OSS List

Project List

3rd Party List

Vulnerability

Self-Check List

Configuration

System

Code management

User management

History List

Notification

Sent Mail List

Vulnerability Log

License List | OSS List | **Project List** | 3rd Party List | Vulnerability | Self-Check List

ID:  Project Name:  Created Date:  ~  Search

Division:  Creator:  Reviewer:

Distribution Type:  Network Service:  Model Name:

Status:  Progress  Request  Review  Complete  Drop

Priority:

---

OSS Name:  OSS Version:  License Name:

Additional Information:  Comment:

Binary Name:  3rd party:

Expand

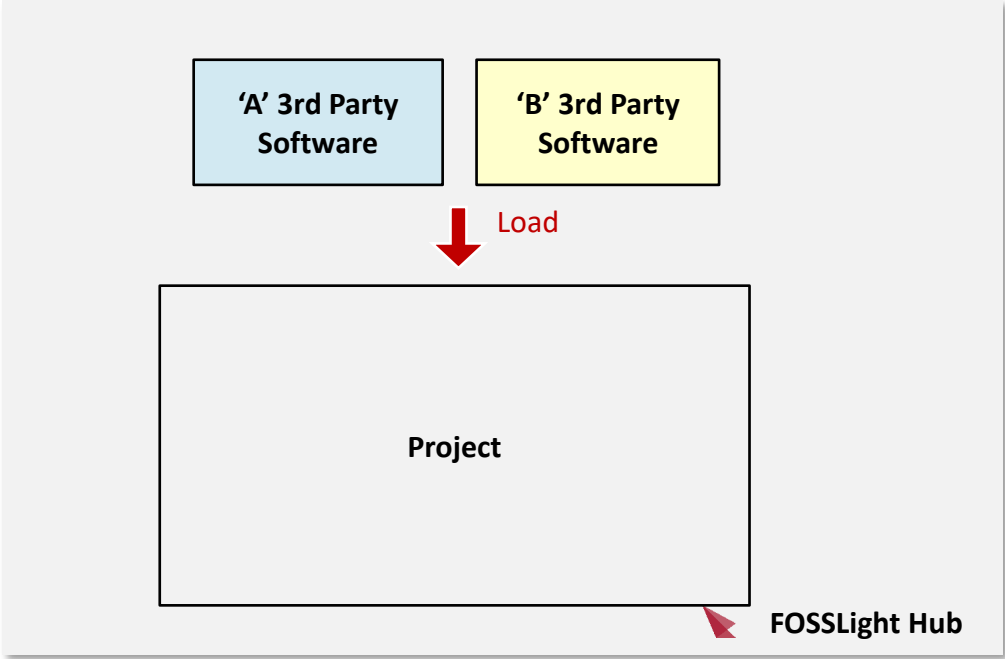
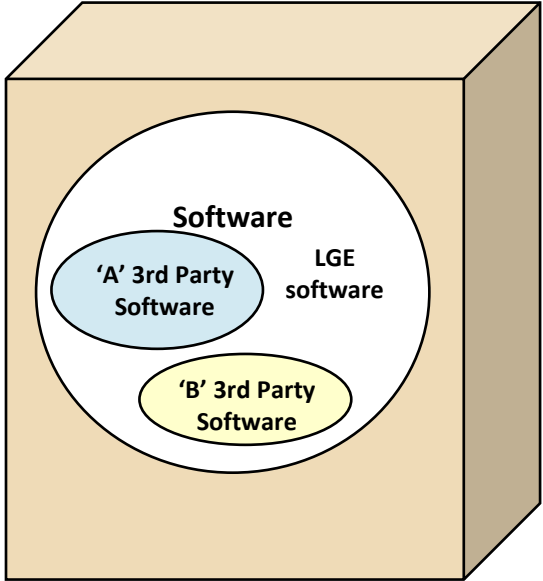
Copy | Change Status | BOM Compare | Export | Add

ID	Project Name (Version)	Status	Identification	Packaging	Download	Distribution T	Vulnerability	Division	Creator	Created Date	Updated Date	Reviewer	Additional Information
278	fossight_source_scanner	R	Request 3rd SRC BIN			General Model		SW Lab	시스템관리	2022-07-11	2022-07-11		
276	tuna_project	R	Confirm 3rd SRC BIN	Confirm		General Model	!	SW Lab	시스템관리	2022-07-09	2022-07-11	시스템관리	
266	test_1 (ver 1.0.0)	R	Review 3rd SRC BIN			General Model	!	N/A	고대은	2022-06-21	2022-06-21	시스템관리	
261	mytest	R	Review 3rd SRC BIN			General Model	!	N/A	이지형	2022-06-20	2022-06-20	시스템관리	
257	Moo (ver 1.0.0)	R	Confirm 3rd SRC BIN	Confirm		General Model	!	N/A	parkmuhy	2022-06-15	2022-06-15	시스템관리	
243	webgoat (ver 8.2.0)	R	Review 3rd SRC BIN			General Model	!	SW Lab	시스템관리	2022-05-20	2022-05-20	테스터	webgoat
229	test-ellie	R	Request 3rd SRC BIN			General Model		N/A	ellie	2022-04-19	2022-05-04		
211	3rd party reg (ver 2)	R	Request 3rd SRC BIN			General Model	!	N/A	크리스틴	2022-03-11	2022-03-17		Copied fr
189	copy test (ver 3)	R	Request 3rd SRC BIN			Transfer in-ho		N/A	크리스틴	2022-03-03	2022-03-17	시스템관리	Copied fr
187	mymytest (ver 1.0)	R	Request 3rd SRC BIN			B2B	!	N/A	사용자	2022-02-22	2022-03-03	테스터	HD
127	testttt (ver 44444)	R	Confirm 3rd SRC BIN	N/A		General Model		N/A	시스템관리	2021-12-03	2021-12-03	시스템관리	
126	testt (ver 2)	R	Confirm 3rd SRC BIN	N/A		General Model		N/A	시스템관리	2021-12-03	2021-12-03		Copied fr
112	my test 211112	R	Confirm 3rd SRC BIN	N/A		General Model		N/A	시스템관리	2021-11-12	2021-11-12	테스터	
107	test download location	R	Confirm 3rd SRC BIN	Confirm		General Model		N/A	시스템관리	2021-11-05	2021-11-05	시스템관리	
103	PackingTest	R	Confirm 3rd SRC BIN	N/A		General Model			사용자	2021-10-14	2021-10-22	시스템관리	

Page 1 of 3 | 15 | View 1 - 15 of 42

Copy | Change Status | BOM Compare | Export | Add

# Supply Chain Management



# Supply Chain Management

## □ Using "3rd Party List"

ID

3rd Party Software Name

Status  Progress  Request  Review  Confirm

Created Date  ~

3rd Party Name

3rd Party Software Version

Creator

Division

Reviewer

**Search**

Expand ▼


Export
Add

ID	3rd Party Name	Software Name (Version)	Status	Delivery Form	Description	Vulnerability	Division	Creator	Created Date	Updated Date	Reviewer
539	seongsik89.kim_Company	Training device app (ver 1.	C	B	3rd party 정보입니다.	▲	CTO 컨버전스센터	김성식/선임연구원	2021-09-07	2022-02-24	김경애/Task Leader/S
538	Brian_Moon_Company	Training device app	C	S		▲	VS 스마트개발센터	문경규/책임연구원	2021-09-07	2022-02-24	김경애/Task Leader/S
537	red.kim_he	Training device app	C	S		▲	HE CAV	김영기/책임/HE서	2021-09-07	2022-02-24	석지영/선임연구원/S
535	hosc-1104	Sample_software_from_3rd	P	S			CTO SW센터	일반박원재	2021-09-03	2022-02-24	박원재/선임연구원/S
534	OSC-1756 test	(test)170308_pwj_3rdParty	R	S		▲	CTO SW센터	시스템관리자	2021-08-03	2022-02-24	시스템관리자
533	test	Sample_software_from_3rd	R	S			CTO SW센터	시스템관리자	2021-08-03	2022-02-24	시스템관리자
532	한글로 작성된 경우 테스트	한글로 작성된 경우 테스트	P	S		▲	CTO SW센터	시스템관리자	2021-05-12	2022-02-24	
531	test 3rd party item	좋은 소프트웨어	C	S		▲	CTO SW센터	시스템관리자	2021-04-26	2022-02-24	시스템관리자
530	Test_JK_3rd	SW_3rd_JK_Test (ver 0.0.1	C	S	Test		CTO SW센터	방재권/선임연구원	2021-04-16	2022-02-24	김소임/선임연구원/S
528	delete 3rd party test	mail_plugin	C	S			CTO SW센터	시스템관리자	2020-11-26	2022-02-24	시스템관리자

# SBOM with Supply Chain

Can manage product SBOM including supply chain

ID	<input type="text"/>	Project Name	<input type="text"/>	Created Date	<input type="text"/> ~ <input type="text"/>	<input type="button" value="Search"/>
Division	<input type="text"/>	Creator	<input type="text"/>	Reviewer	<input type="text"/>	
Distribution Type	<input type="text"/>	Network Service	<input type="text"/>	Model Name	<input type="text"/>	
Status	<input type="checkbox"/> Progress <input type="checkbox"/> Request <input type="checkbox"/> Review <input type="checkbox"/> Complete <input type="checkbox"/> Drop					
Priority	<input type="text"/>					
OSS Name	<input type="text"/>	OSS Version	<input type="text"/>	License Name	<input type="text"/>	
Additional Information	<input type="text"/>					
Binary Name	<input type="text"/>	3rd party	<input type="text" value="Test 3rd party"/>			

Expand ▲

Copy Change Status BOM Compare

<input type="checkbox"/>	ID	Project Name (Version)	Status	Identification	Packaging	Download	Distribution T	Vulnerability	Division	Creator	Created Date	Updated Date	Reviewer	Additional Information
<input type="checkbox"/>	224	my test 1 (ver 1.0)	P	Confirm 3rd SRC BIN	Start		General Model	▲	SW Lab	시스템관리	2022-03-29	2022-04-15	Vo Trung H	test addit
<input type="checkbox"/>	144	test1216 (ver 1.0)	P	Progress 3rd SRC BIN			General Model	▲	N/A	Dinesh Ra	2021-12-17	2022-03-29		
<input type="checkbox"/>	124	partner copy test	P	Confirm 3rd SRC BIN	Start		General Model	▲	N/A	시스템관리	2021-11-30	2021-11-30		Copied fr
<input type="checkbox"/>	121	1124proj (ver 1.1.1)	P	Confirm 3rd SRC BIN	Start		General Model	▲	N/A	시스템관리	2021-11-24	2021-11-24		dfadfadgaf
<input type="checkbox"/>	113	my test 211112_2	C	Confirm 3rd SRC BIN	Confirm		General Model	▲	N/A	시스템관리	2021-11-12	2022-04-26	phuvd	

Page 1 of 1 15

View 1 - 5 of 5

Copy Change Status BOM Compare



# SBOM Search

## Search for specific component/version

Project List ✕

3 ID

Division

Distribution Type

Status  Progress  Request  Review  Complete  Drop

Priority

Project Name

Creator

Network Service

View My Projects Only  2

Created Date  ~

Reviewer

Model Name

5 **Search**

4 OSS Name

Additional Information

Binary Name

OSS Version

Comment

3rd party

License Name

1 **Expand** ▲

Copy

Change Status

BOM Compare

Export

<input type="checkbox"/>	ID	Project Name (Version)	Status	Identification	Packaging	Distribution	Download	Distribution T	Vulnerability	Division	Creator	Created Da	Updated Di	Reviewer
<input type="checkbox"/>	4027	TEST_general_user	<span style="color: green;">P</span>	Progress <span style="background-color: #333; color: white; padding: 2px;">3rd</span> <span style="background-color: #333; color: white; padding: 2px;">SRC</span> <span style="background-color: #333; color: white; padding: 2px;">BIN</span>				General Model	<span style="color: red;">▲</span>	기타	일반김소임	2021-12-03	2021-12-03	
<input type="checkbox"/>	3123	webOS Auto (ver 2.0)	<span style="color: blue;">C</span>	Confirm <span style="background-color: #333; color: white; padding: 2px;">3rd</span> <span style="background-color: #333; color: white; padding: 2px;">SRC</span> <span style="background-color: #333; color: white; padding: 2px;">BIN</span>	Confirm	N/A		Transfer in-hou	<span style="color: red;">▲</span>	LGSI	Aditi Jain	2020-10-06	2020-11-04	김소임
<input type="checkbox"/>	2735	LMQ920N_Android_Q	<span style="color: blue;">C</span>	Confirm <span style="background-color: #333; color: white; padding: 2px;">Android</span>	Confirm	Done		General Model	<span style="color: red;">▲</span>	MC	김용석	2020-06-08	2020-11-04	김소임

# SBOM Tracking

## Support SBOM Compare

Copy

Change Status

BOM Compare

Before Project id After Project id 

Search

Excel download

Status	OSS_Before	License_Before	OSS_After	License_After
add			cJSON (1.7.10)	MIT
add			openssl (1.1.1f)	OpenSSL
delete	base-files (3.0.14)	GPL-2.0-only		
delete	lcdtest (2.0)	GPL-2.0-only, GPL-3.0, MPL-1.1		
change	cairo(1.12.12)	GPL-3.0	cairo(1.12.14)	GPL-3.0, MPL-1.1
change	apmd(3.2.2-14)	GPL-2.0-only	apmd(3.2.2-14)	GPL-2.0
change	BusyBox	GPL-2.0-only	BusyBox	GPL-2.0
change	usbutils(007)	GPL-2.0-only	usbutils(008)	GPL-2.0

Page  of

View 1 - 8 of 8

# Vulnerability Review

## □ Vulnerability Review for product

<input type="checkbox"/>	ID ↕	Project Name (Version)	Status ?	Identification	Packaging	Download ?	Security	Vulnerability	Distribution Type	Division	Creator	Created Date	Updated Date	Reviewer	Additional Information
<input type="checkbox"/>	499	newOne	P	<input type="text" value="Start"/>					General Model	SW Lab	Admin	2023-05-08	2023-05-08		
<input type="checkbox"/>	498	mytestproject12345	P	Confirm <input type="text" value="3rd"/> SRC <input type="text" value="BIN"/> <input type="text" value="BOM"/>	<input type="text" value="Start"/>		<input type="text" value="SEC"/>		General Model	SW Lab	Admin	2023-05-03	2023-05-03	Admin	
<input type="checkbox"/>	497	cdh_test	R	Confirm <input type="text" value="3rd"/> SRC <input type="text" value="BIN"/> <input type="text" value="BOM"/>	<input type="text" value="Confirm"/>		<input type="text" value="SEC"/>		General Model	SW Lab	Admin	2023-04-25	2023-04-25	Admin	
<input type="checkbox"/>	496	bxxt	P	Progress <input type="text" value="3rd"/> SRC <input type="text" value="BIN"/> <input type="text" value="BOM"/>			<input type="text" value="SEC"/>		General Model	SW Lab	사용자	2023-04-21	2023-04-21		

## □ Security Review Tab

Total

Fixed

Not Fixed

Show Comment History

Comment Edit ▾

Export

Save

OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerability Link
~ <input type="text" value=""/>	~ <input type="text" value=""/>	~ <input type="text" value=""/>	~ <input type="text" value=""/>	~ <input type="text" value=""/>	~ <input type="text" value=""/>	~ <input type="text" value=""/>
Protocol Buffers		CVE-2015-5237	8.8	2017-09-25	Unresolved	<a href="https://nvd.nist.gov/vuln/detail/">https://nvd.nist.gov/vuln/detail/</a>
Protocol Buffers		CVE-2021-3121	8.6	2021-01-11	Unresolved	<a href="https://nvd.nist.gov/vuln/detail/">https://nvd.nist.gov/vuln/detail/</a>
SnakeYAML	1.27	CVE-2022-1471	9.8	2022-12-01	Unresolved	<a href="https://nvd.nist.gov/vuln/detail/">https://nvd.nist.gov/vuln/detail/</a>
Spring Framework	5.3.1	CVE-2016-1000027	9.8	2020-01-02	Unresolved	<a href="https://nvd.nist.gov/vuln/detail/">https://nvd.nist.gov/vuln/detail/</a>
Spring Framework	5.3.1	CVE-2022-22965	9.8	2022-04-01	Unresolved	<a href="https://nvd.nist.gov/vuln/detail/">https://nvd.nist.gov/vuln/detail/</a>
Spring Framework	4.3.30	CVE-2016-1000027	9.8	2020-01-02	Unresolved	<a href="https://nvd.nist.gov/vuln/detail/">https://nvd.nist.gov/vuln/detail/</a>

# Vulnerability Real-time Notification

## 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)

## Takeaways and Conclusions

- ❑ Automation for SBOM generation and management is important
- ❑ It is difficult to determine the minimum unit of SBOM component.

## Suggestions for SG17

- ❑ Consider to make a guideline for SBOM component unit such as the necessary for commercial software or self-developed software and so on.