LGE Internal Use Only

FOSSLight Hub로 보안취약점을 더 정교하게 관리해요

석지영 책임 연구원
LG 전자

LGE Internal Use Only

01

보안취약점 DB

LGE Internal Use Only

01 NVD 보안취약점 DB 수집

- **일 1회, NVD**에서 제공하는 **REST API**를 통해 **데이터 취득하여 DB에 저장**
- **NVD (National Vulnerability Database)**
  - CVE 정보를 바탕으로 상세 분석 정보를 제공하는 미국 정부 공식 데이터베이스
  - 웹사이트 : https://nvd.nist.gov

2.0 APIs

LGE Internal Use Only

CVE / CVSS / CPE

- **CVE (Common Vulnerabilities and Exposures)**
  - **전 세계 보안취약점에 고유한 ID를 부여하는 표준 식별 체계**
  - 형식 : CVE-[연도]-[일련번호] (ex. CVE-2021-44228)

- **CVSS (Common Vulnerability Scoring System)**
  - **취약점의 심각도를 수치로 나타내는 표준 점수 체계**
  - CVE ID별 CVSS score가 존재함
  - 점수 범위 : 0.0 (None) ~ 10.0 (Critical)
  - FOSSLight Hub 내 점수 우선순위 : CVSS v4 > CVSS v3.1 > CVSS v3 > CVSS v2

- **CPE (Common Platform Enumeration)**
  - **영향받는 소프트웨어/하드웨어 제품을 표준 형식으로 표기하는 체계**
  - 형식 : cpe:2.3:[type]:[vendor]:[product]:[version]:[update]:[edition]:[language]:[sw_edition]:[target_sw]:[target_hw]:[other]

01 CVE ID 예시

CVE-2026-30898 Detail

Description

An example of BashOperator in Airflow documentation suggested a way of passing dag_run.conf in the way that could cause unsanitized user input to be used to escalate privileges of UI user to allow execute code on worker. Users should review if any of their own DAGs have adopted this incorrect advice.

QUICK INFO

CVE Dictionary Entry:
CVE-2026-30898
NVD Published Date:
04/18/2026
NVD Last Modified:
04/21/2026
Source:

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sour

CVSS 3.x Severity and Vector Strings:

NIST: NVD	**Base Score:** N/A	NVD assessment not yet provided.	
ADP: CISA-ADP	**Base Score:** 8.8 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/	

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because t
information that would be of interest to you. No inferences should be drawn on account of other sites being reference
page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse th
or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may l
these sites. Please address comments about this page to nvd@nist.gov.

URL	Source(s)	Tag(s)
http://www.openwall.com/lists/oss-security/2026/04/17/7	CVE	Mailing List
https://github.com/apache/airflow/pull/64129	Apache Software Foundation	Issue Tracking
https://lists.apache.org/thread/26zmhfj1t95c1hld2r14ho81nzh1bdc8	Apache Software Foundation	Mailing List

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:apache:airflow:*:*:*:*:*:*:*:* — **Up to (excluding) 3.2.0**

Hide Matching CPE(s)

- cpe:2.3:a:apache:airflow:-:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.1:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.2:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.2.1:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.2.2:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.2.3:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.3:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.3.1:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.3.2:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.4:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.4.1:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.4.2:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.4.3:*:*:*:*:*:*:*
- cpe:2.3:a:apache:airflow:0.4.5:*:*:*:*:*:*:*

01 보안취약점 데이터 베이스와 OSS 매칭

- NVD CPE 데이터에서 product, version 값을 각각 OSS name(또는 nickname), OSS version 과 매칭하여 보안취약점 검출

CVE-2022-22978 Detail

Current Description

In spring security versions prior to 5.4.11+, 5.5.7+ , 5.6.4+ and older unsupported versions, RegexRequestMatcher can easily be misconfigured to be bypassed on some servlet containers. Applications using RegexRequestMatcher with `.` in the regular expression are possibly vulnerable to an authorization bypass.

+View Analysis Description

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

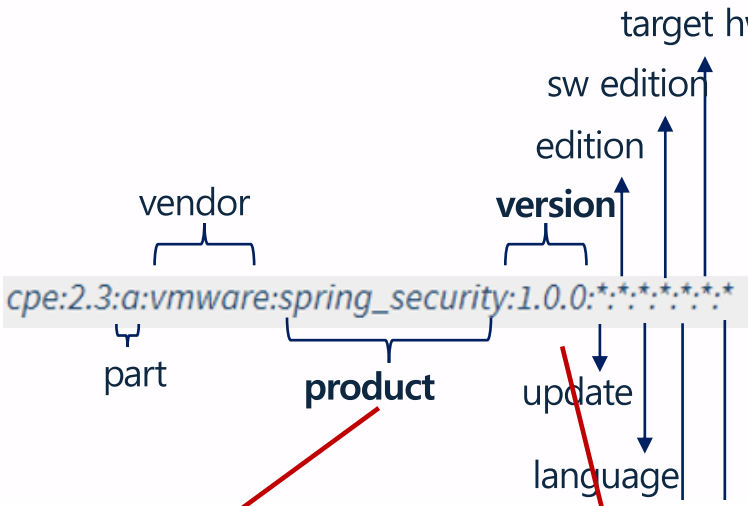
CVSS 3.x Severity and Vector Strings:

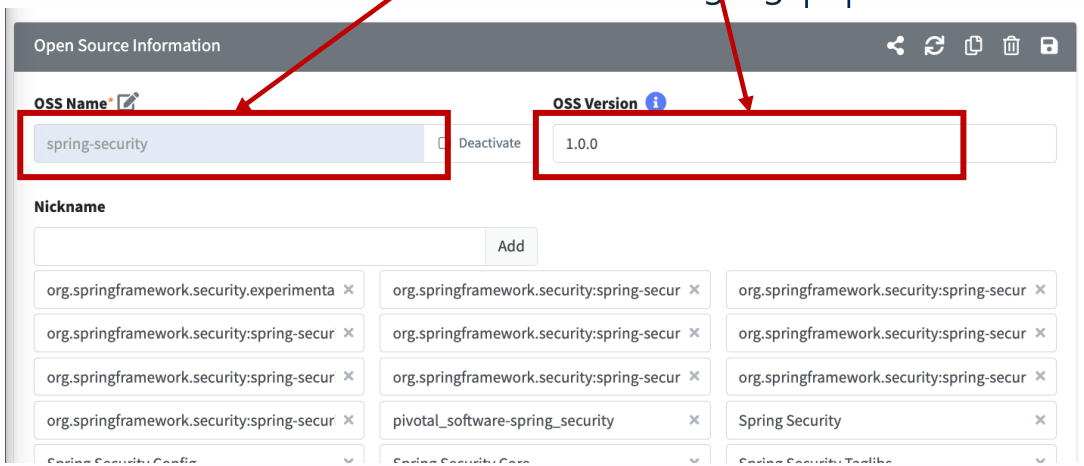
NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:vmware:spring_security:*:*:*:*:*:*:*:*	**Up to (excluding) 5.5.7**
Hide Matching CPE(s) ▲	
• *cpe:2.3:a:vmware:spring_security:-:*:*:*:*:*:*:**	
• *cpe:2.3:a:vmware:spring_security:1.0.0:*:*:*:*:*:*:**	
• *cpe:2.3:a:vmware:spring_security:1.0.1:*:*:*:*:*:*:**	
• *cpe:2.3:a:vmware:spring_security:1.0.2:*:*:*:*:*:*:**	

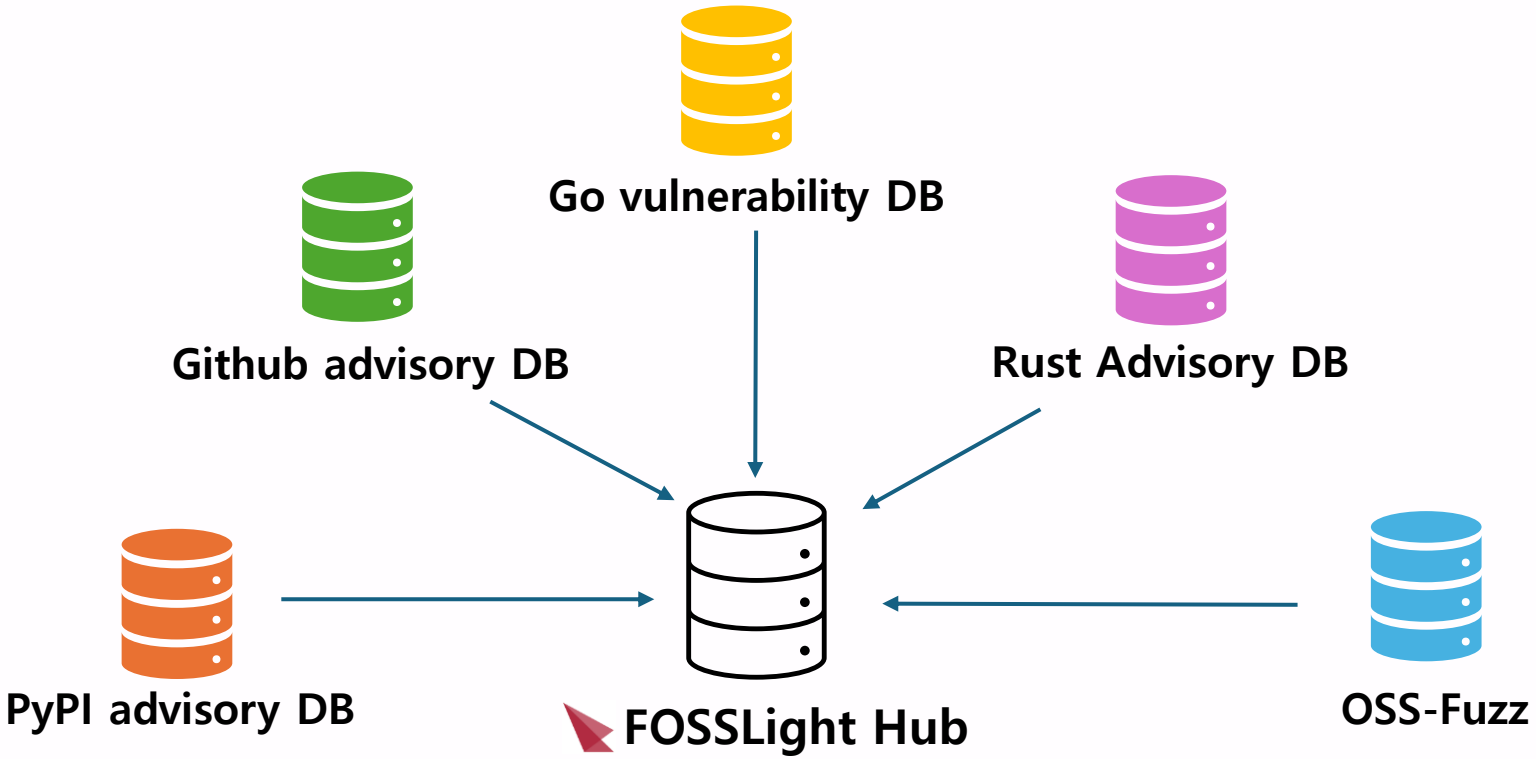




LGE Internal Use Only

01 보안취약점 DB 확장 (TO-BE)

- 패키지 매니저 보안취약점 검출 강화



LGE Internal Use Only

02

Version 관리

LGE Internal Use Only

02 보안취약점 버전 관리 (AS-IS)

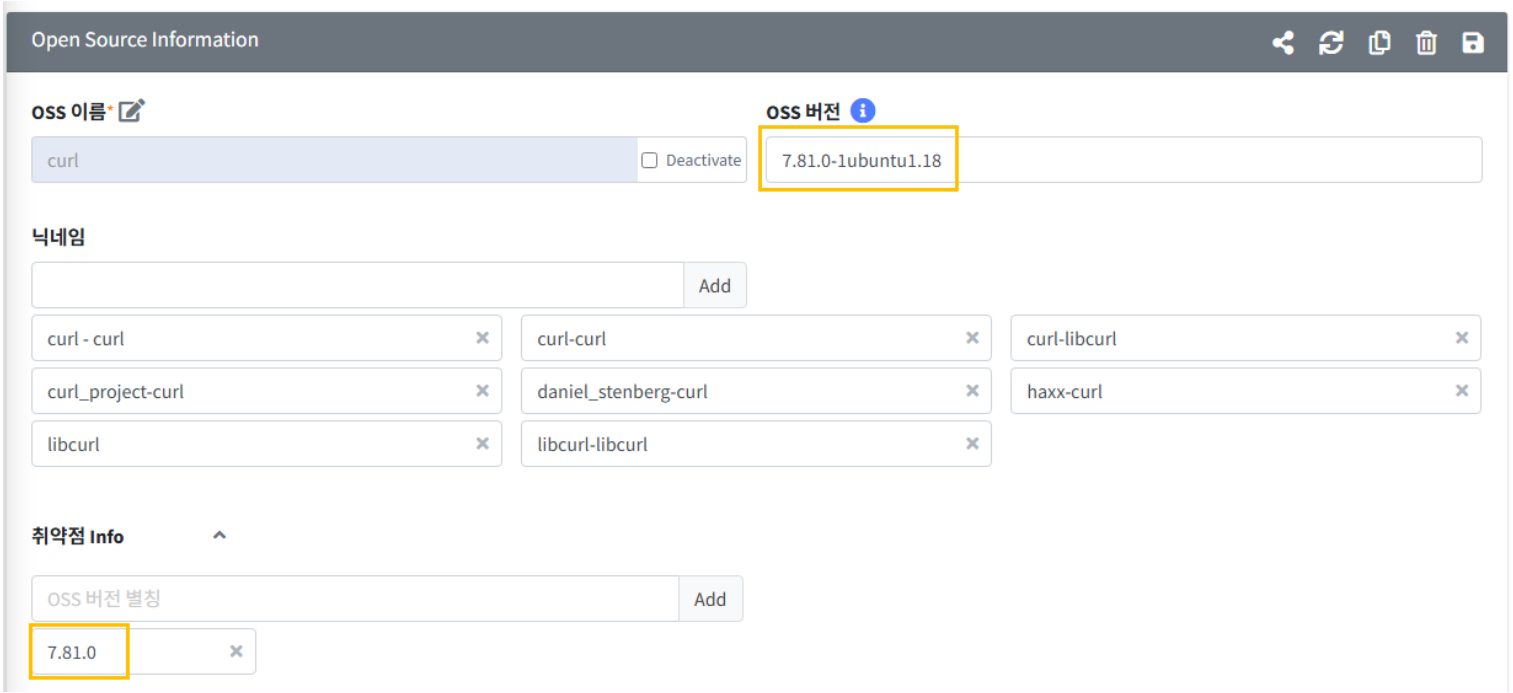
- NVD에서 제공하는 버전과 FOSSLight Hub에서 관리하는 버전을 매핑시켜 보안취약점 검출 가능하도록 기능 제공

OSS version
7.81.0-1ubuntu1.1.8

=

NVD
7.81.0

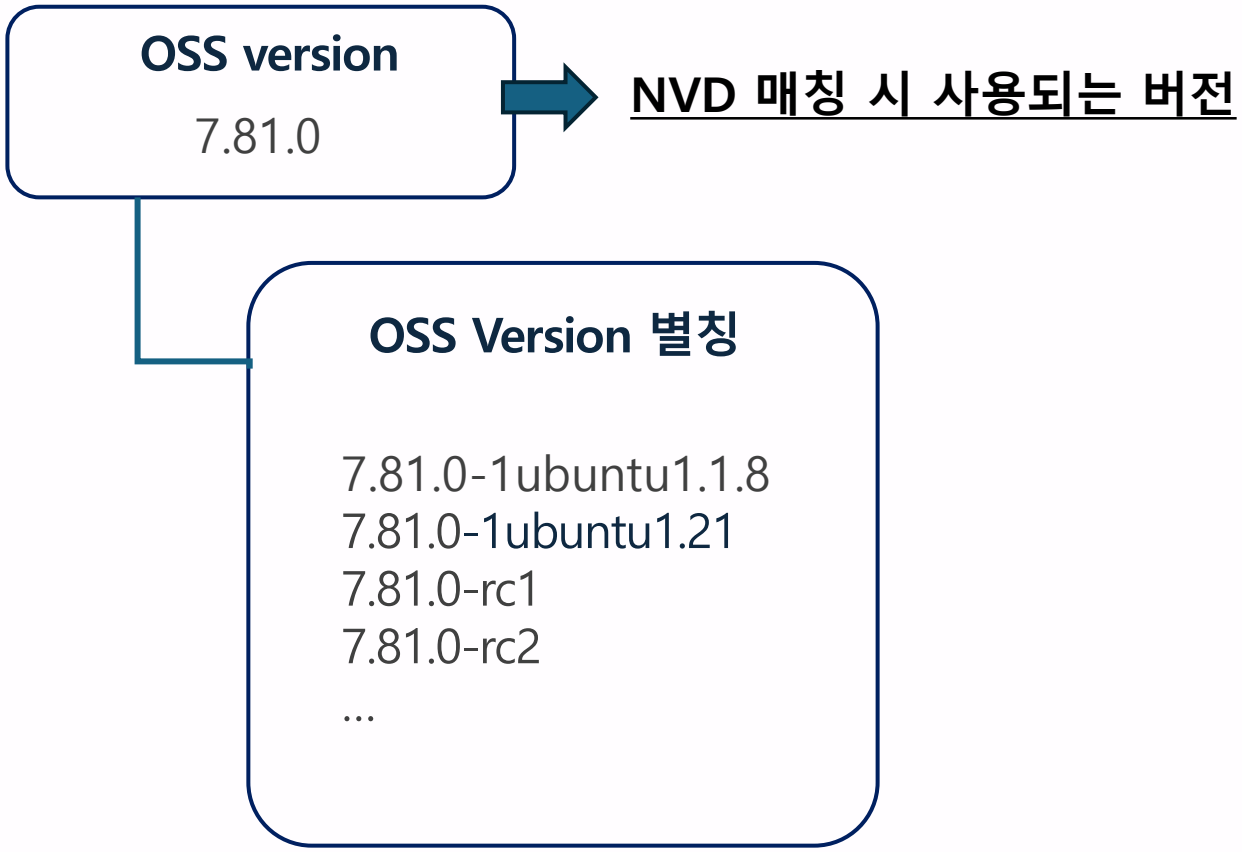
→ **OSS Version 별칭에 추가**



LGE Internal Use Only

02 보안취약점 버전 관리 (TO-BE)

- FOSSLight Hub에서 관리하는 OSS version에 대해 version nickname 개념 추가



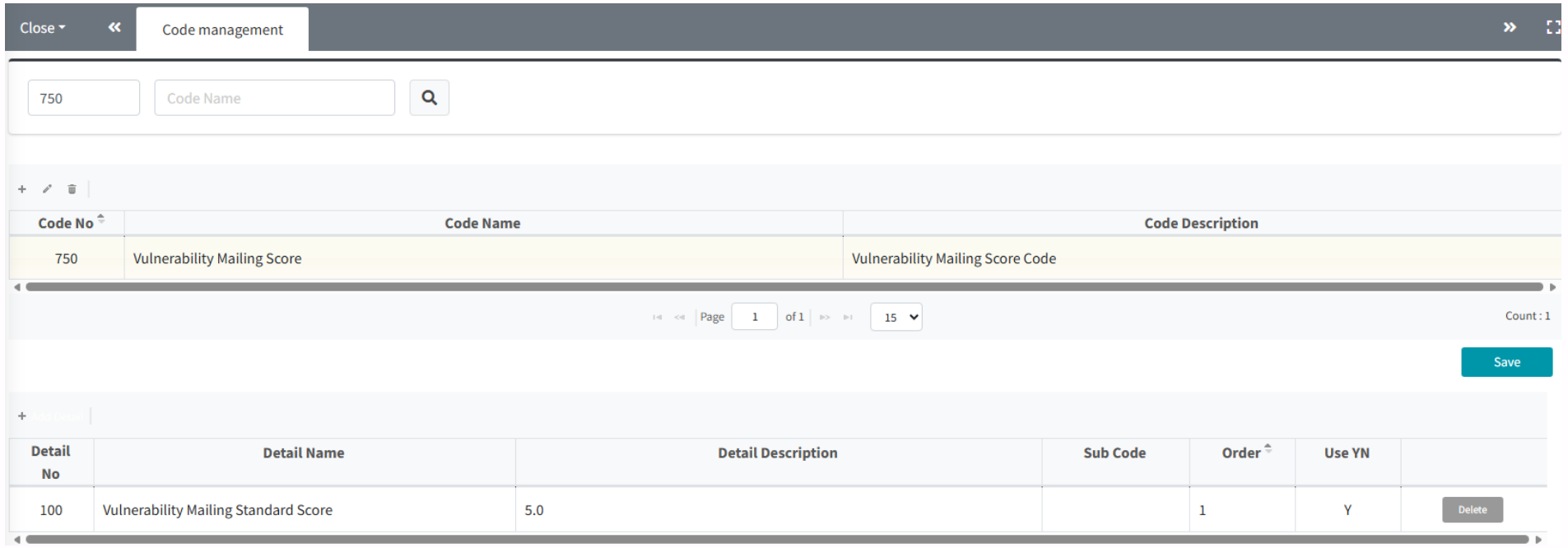
LGE Internal Use Only

03

보안취약점 모니터링 mailing

03 Vulnerability Mailing Score

- Vulnerability Mailing Score (System>Code management>Code No. 750) 통해 취약점 관리하고자 하는 점수 설정 가능



03 프로젝트 신규 보안취약점 발견 메일 발송

- 프로젝트에 Vulnerability Mailing Score 이상인 신규 보안취약점 발견 시, Discovered 알림 메일 발송

FOSSLight Hub Notification

[TEST][OSC] Vulnerability Discovered : "(5230)user-test-android (3.0)"

Comment

이 프로젝트에서 사용된 Open Source 중 다음과 같은 보안 취약점이 발견되었습니다.
해당 취약점에 대한 조치 방안은 로 문의해 주시고, 보안 취약점의 검출과 관련된 문의는 | 통해 이슈 생성 바랍니다.

Security vulnerabilities have been identified in the open source used in this project as follows.
For measures regarding the vulnerabilities, please contact . For inquiries related to the detection of these vulnerabilities, please create an issue at

	Registered Data
Project Name	user-test-android
Project Version	3.0
Security Mail	Enable
Security Responsible Person	
Operating System	Linux
Distribution Type / Network Service Only?	General / N
Distribution Site	opensource.lge.com
OSS Notice	Platform-generated
Priority	P2
Creator	CTO 블록체인연구실 시스템관리자(oscAdmin)
Division	CTO SW센터
Reviewer	CTO 블록체인연구실 시스템관리자(oscAdmin)

≪ Vulnerability Information ≫

OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
Linux Kernel	5.4.96	CVE-2024-36880	7.8	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: qca: add missing firmware sanity checks Add the missing sanity checks when parsing the firmware files before downloading them to avoid accessing and corrupting memory beyond the vmalloced buffer. En el kernel de Linux, se resolvió la siguiente vulnerabilidad: Bluetooth: qca: agregar comprobaciones de integridad del firmware faltantes Agregue las comprobaciones de integridad del firmware faltantes al analizar los archivos de firmware antes de descargarlos para evitar acceder y dañar la memoria más allá del búfer vmalloced.	2024-05-30	2025-09-30

03 신규 보안취약점 발견 메일 목록 발송 (daily)

- 데일리 업데이트 이후, Vulnerability Mailing Score 이상인 신규 보안취약점 발견 시, 해당 목록에 대해 Discovered 알림 메일 발송

FOSSLight Hub Notification

[TEST][OSC] Vulnerability Discovered

« Vulnerability Information »

OSS ID	OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
32233	Apache Tomcat	7.0.100	CVE-2026-29146	7.5	Padding Oracle vulnerability in Apache Tomcat's EncryptInterceptor with default configuration. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.0.0-M1 through 10.1.52, from 9.0.13 through 9..115, from 8.5.38 through 8.5.100, from 7.0.100 through 7.0.109. Users are recommended to upgrade to version 11.0.19, 10.1.53 and 9.0.116, which fixes the issue.	2026-04-09	2026-04-10
25546	Apache Tomcat	7.0.106	CVE-2026-29146	7.5	Padding Oracle vulnerability in Apache Tomcat's EncryptInterceptor with default configuration. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.0.0-M1 through 10.1.52, from 9.0.13 through 9..115, from 8.5.38 through 8.5.100, from 7.0.100 through 7.0.109. Users are recommended to upgrade to version 11.0.19, 10.1.53 and 9.0.116, which fixes the issue.	2026-04-09	2026-04-10
17137	Apache Tomcat	8.5.42	CVE-2026-29146	7.5	Padding Oracle vulnerability in Apache Tomcat's EncryptInterceptor with default configuration. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.0.0-M1 through 10.1.52, from 9.0.13 through 9..115, from 8.5.38 through 8.5.100, from 7.0.100 through 7.0.109. Users are recommended to upgrade to version 11.0.19, 10.1.53 and 9.0.116, which fixes the issue.	2026-04-09	2026-04-10
19103	Apache Tomcat	9.0.22	CVE-2026-29146	7.5	Padding Oracle vulnerability in Apache Tomcat's EncryptInterceptor with default configuration. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.0.0-M1 through 10.1.52, from 9.0.13 through 9..115, from 8.5.38 through 8.5.100, from 7.0.100 through 7.0.109. Users are recommended to upgrade to version 11.0.19, 10.1.53 and 9.0.116, which fixes the issue.	2026-04-09	2026-04-10

03 보안취약점 CVSS Score 변동 목록 메일 발송 (daily)

- 데일리 업데이트 이후, CVSS Score가 Vulnerability Mailing Score 이상이었던 보안취약점이 Vulnerability Mailing Score 미만으로 변동 시, 해당 목록에 대해 Recalculated 알림 메일 발송

FOSSLight Hub Notification

[TEST][OSC] Vulnerability Recalculated

« Vulnerability Information »

OSS ID	OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
25391	react		CVE-2025-55182 -> NONE	10.0 -> 0.0			
6518	zipArchive		CVE-2022-36943 -> NONE	8.1 -> 0.0			

* This mail was sent by https://osc-dev.lge.com

03 보안취약점 모니터링 메일 발송 (daily)

- 하나의 OSS에 매칭되는 CVE-ID 중 [vendor]:[product]가 다른 경우가 존재하는 경우

FOSSLight Hub Notification

Vulnerability Difference Vendor

« Vulnerability Information »

OSS Name	CVE ID	VENDOR:PRODUCT
cups-filters	CVE-2025-64524 CVE-2023-24805	openprinting:cups-filters linuxfoundation:cups-filters
resty	CVE-2023-45286 CVE-2025-13435	resty_project:resty dreampie:resty
jsonwebtoken	CVE-2022-23540 CVE-2026-25537	auth0:jsonwebtoken keats:jsonwebtoken
iperf	CVE-2025-54351 CVE-2016-4303	iperf_project:iperf es:iperf
JSON-java	CVE-2026-33210 CVE-2022-45690	ruby-lang:JSON-java stleary:JSON-java
asn1c	CVE-2017-12966 CVE-2016-5080	asn1c_project:asn1c objective_systems:asn1c
libsndfile	CVE-2017-12562 CVE-2015-7805	libsndfile_project:libsndfile mega-nerd:libsndfile
MQTT.js	CVE-2020-13849 CVE-2017-10910	mqtt:MQTT.js mqtt.js_project:MQTT.js
rsync	CVE-2017-15994 CVE-2007-6200	samba:rsync rsync:rsync

→ Product = OSS name(또는 nickname) 경우, 매칭됨

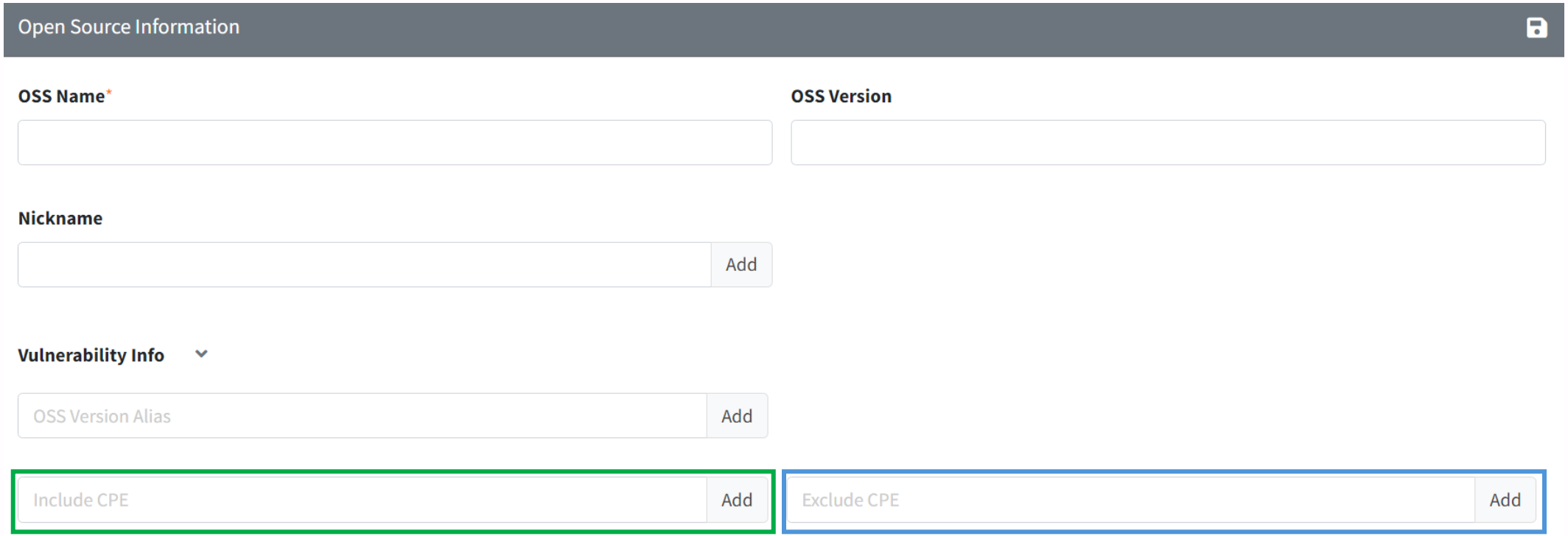
✓ *Vendor가 다른 경우, 같은 OSS에 매칭되는 것이 맞는지 확인 필요*

LGE Internal Use Only

04

Include cpe / exclude cpe 활용법

04 Include cpe / Exclude cpe



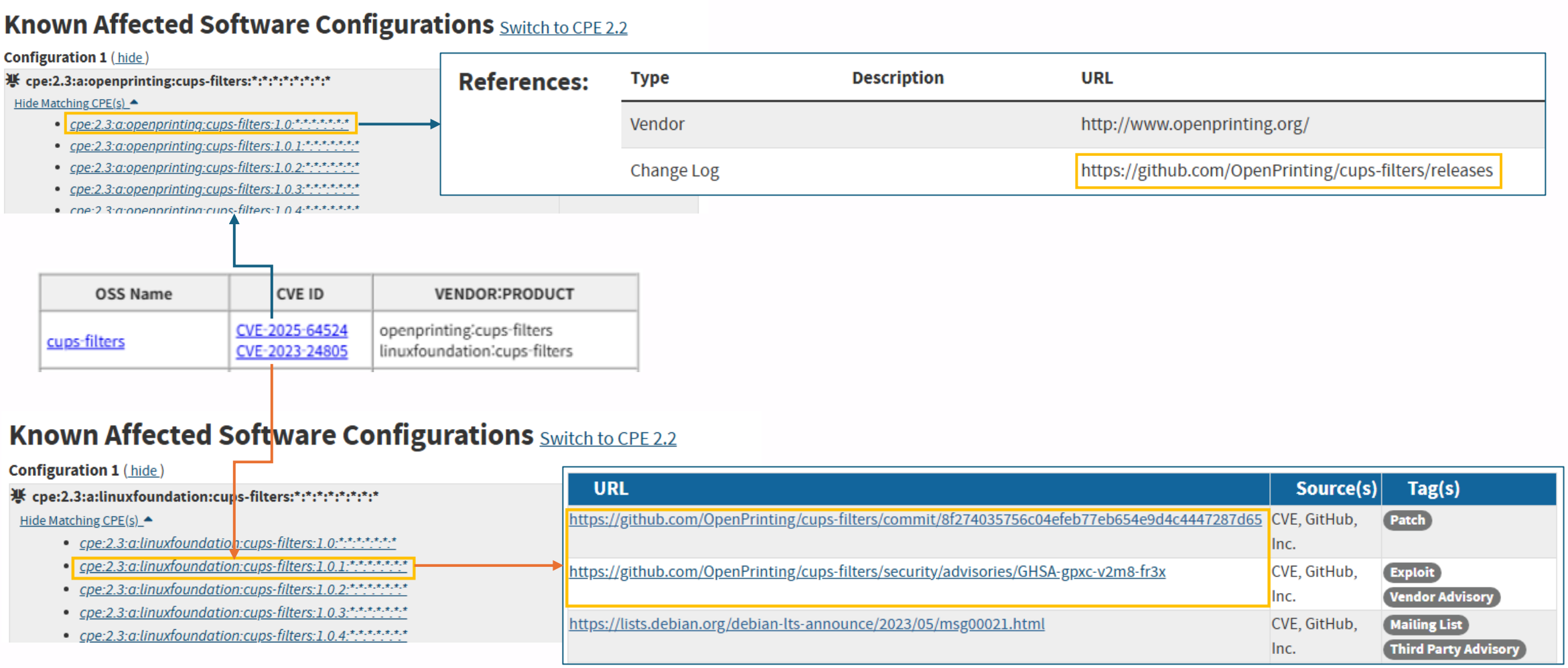
보안취약점 매칭을 위한 추가 CPE

- **vendor:product**
- **cpe:2.3:a:vendor:product:*:*:*:*:*:*:language:*:***

보안취약점 매칭 제외를 위한 CPE

04 Vendor Different 조치 방법 (include cpe 활용)

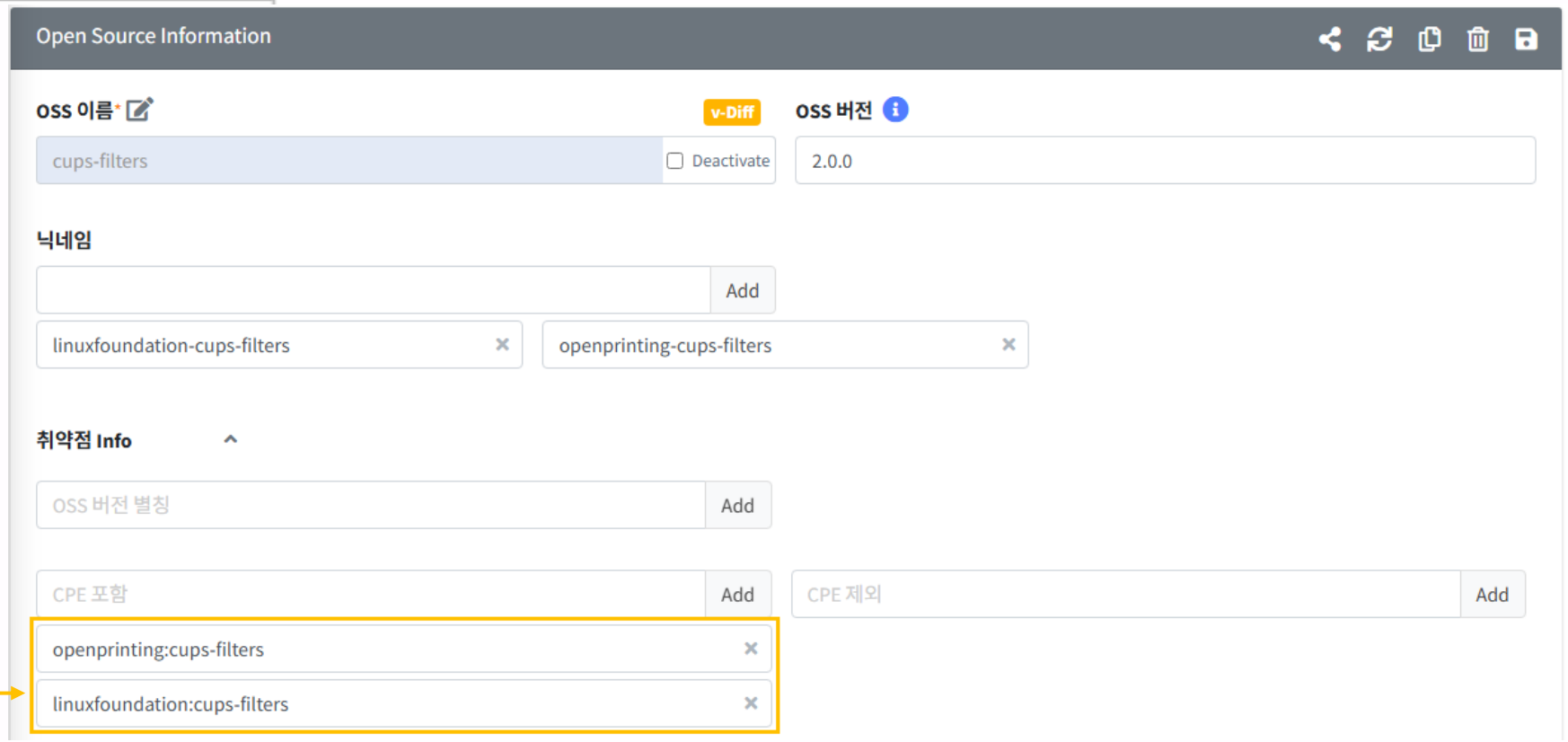
- NVD 사이트에서 CVE ID의 reference확인 결과, 동일 OSS에 해당하는 경우



04 Vendor Different 조치 방법 (include cpe 활용)

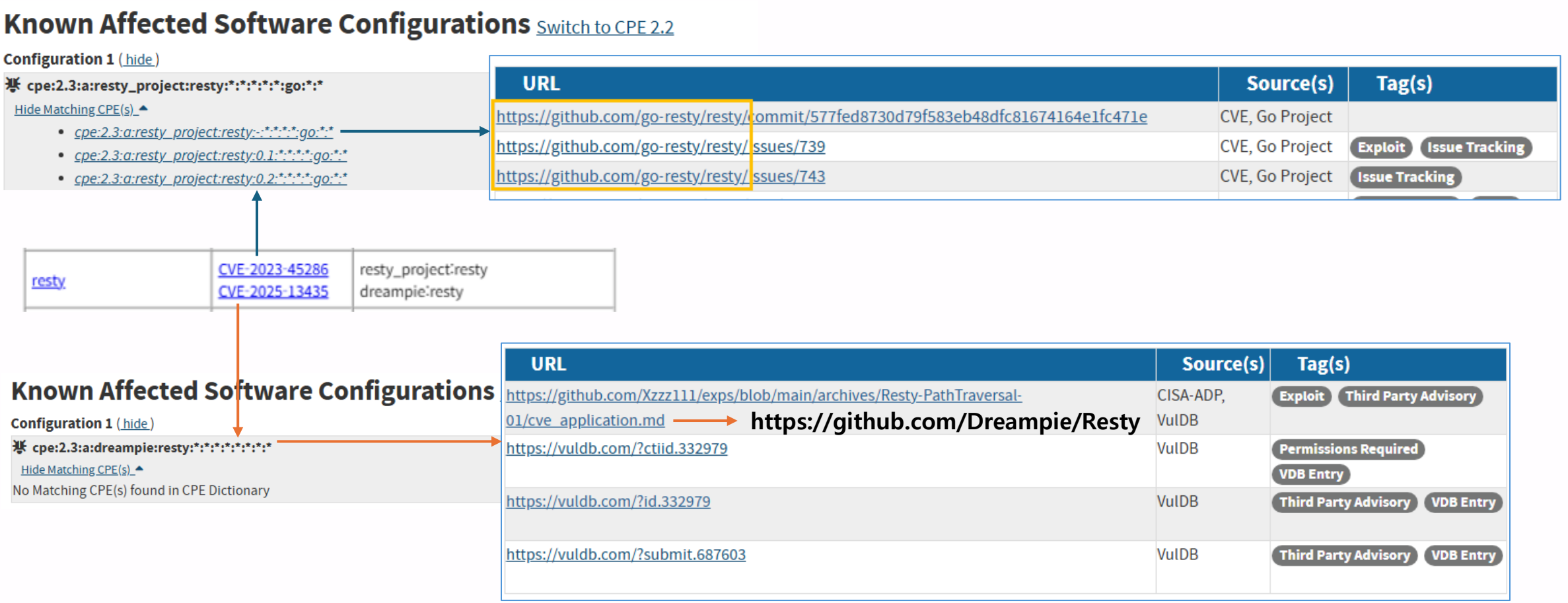
- NVD 사이트에서 CVE ID의 reference확인 결과, 매칭된 OSS와 동일 OSS에 해당하는 경우

OSS Name	CVE ID	VENDOR:PRODUCT
cups-filters	CVE-2025-64524 CVE-2023-24805	openprinting:cups-filters linuxfoundation:cups-filters



04 Vendor Different 조치 방법 (include/exclude cpe 활용)

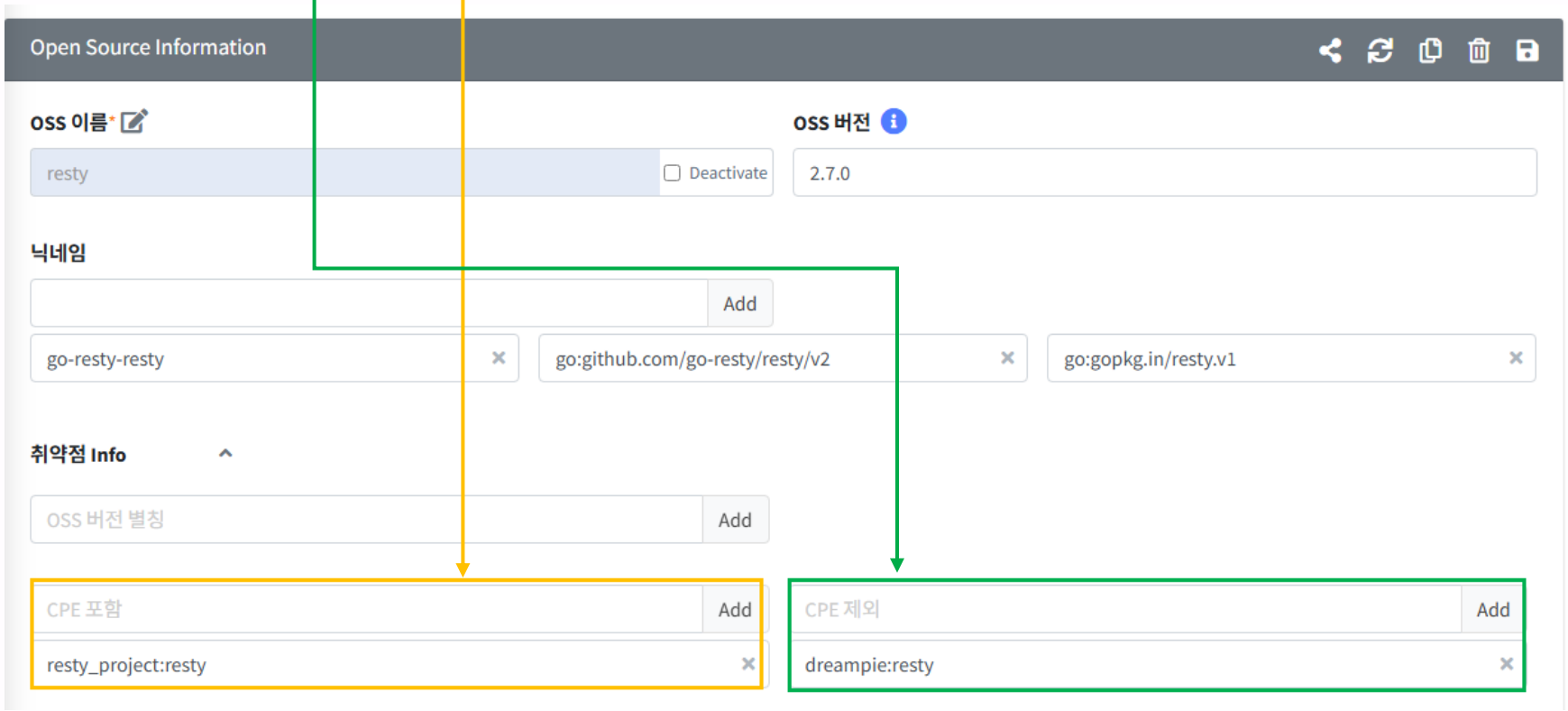
- NVD 사이트에서 CVE ID의 reference확인 결과, 다른 OSS에 해당하는 경우



04 Vendor Different 조치 방법 (include/exclude cpe 활용)

- NVD 사이트에서 CVE ID의 reference확인 결과, 다른 OSS에 해당하는 경우

resty	CVE-2023-45286 CVE-2025-13435	resty_project:resty dreampie:resty



LGE Internal Use Only

04 Language별 취약점 구분 방법 (full cpe 활용)

- bson OSS language별 취약점 구분 필요

CVE-2015-4412

Vendor:product -> mongodb:bson

Reference : https://github.com/mongodb/bson-ruby

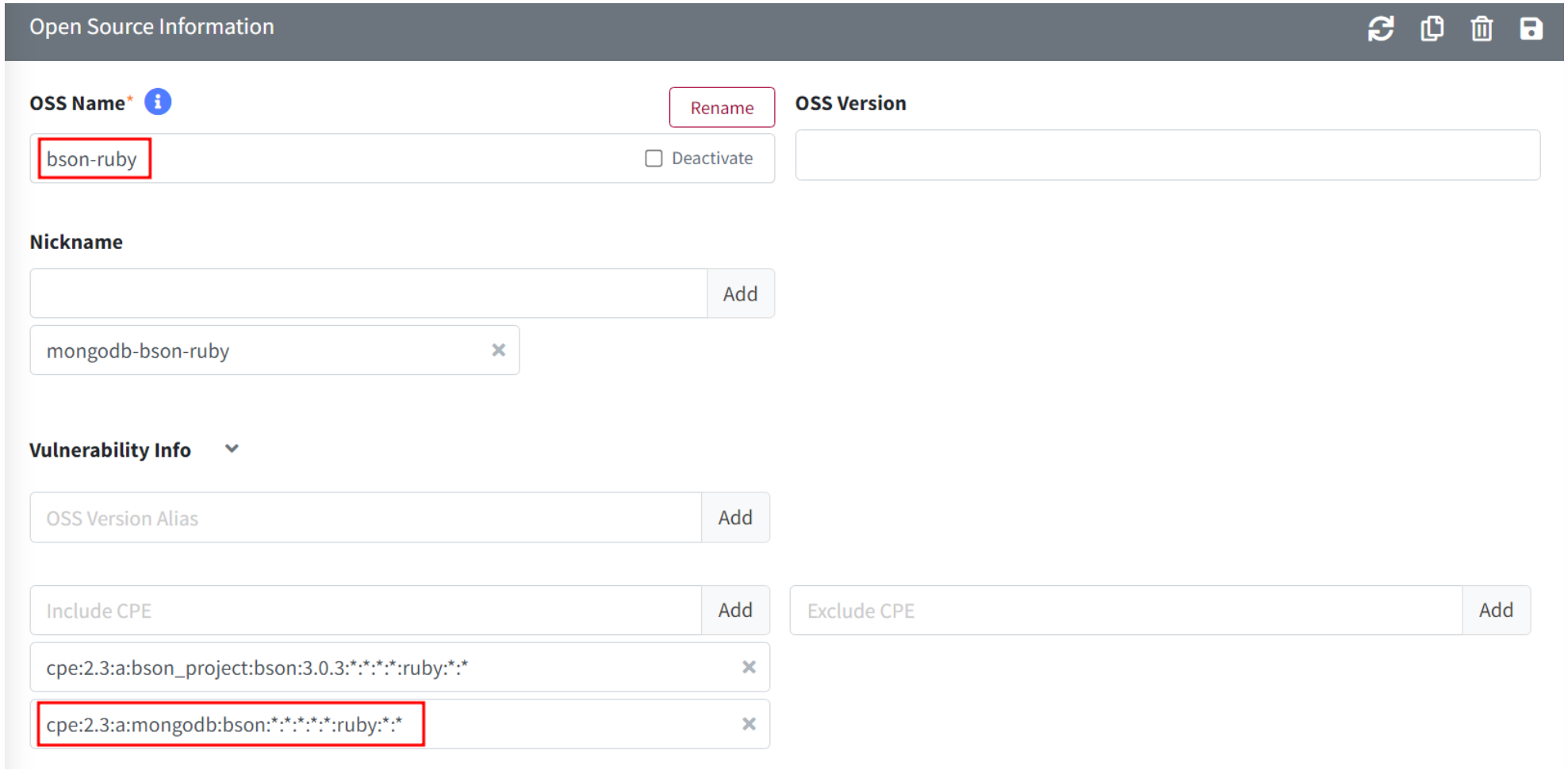
CVE-2020-7610

Vendor:product -> mongodb:bson

Reference : https://github.com/mongodb/js-bson

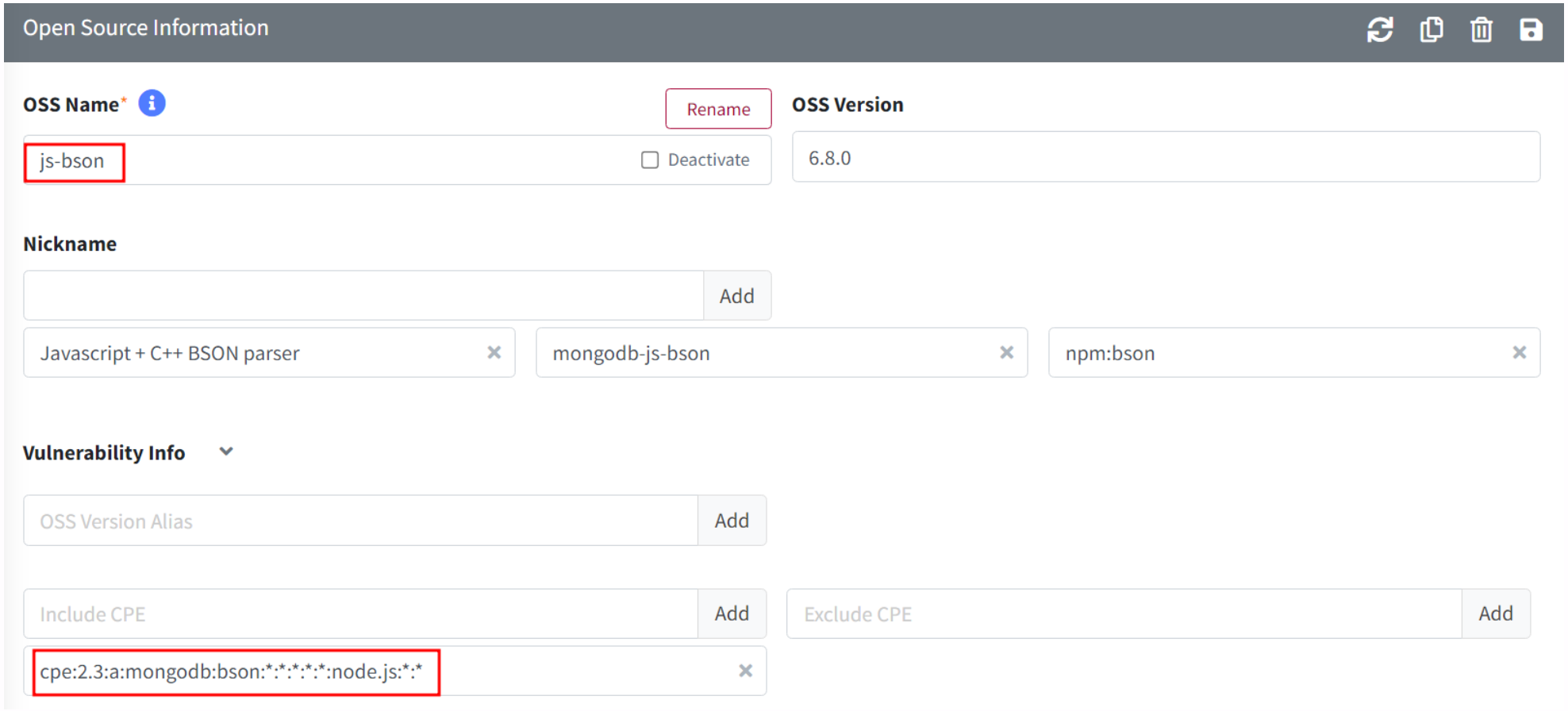
04 Language별 취약점 구분 방법 (full cpe 활용)

- bson-ruby OSS에 ruby language full cpe 추가



04 Language별 취약점 구분 방법 (full cpe 활용)

- js-bson OSS에 node.js language full cpe 추가



LGE Internal Use Only

감사합니다

FOSSLight Hub 2.0