

FOSSLight Hub 업데이트

Dependency & Security

석지영 책임 연구원
LG 전자



CONTENTS

01 Dependency

02 Security





01

Dependency



PURL 정보 제공 NEW

3rd party DEP SRC BIN BOM

FOSSLight Report [fosslight_report_dep_250930_1701.xlsx](#)
2025-09-30 17:02:11

ID	Package URL	OSS Name	OSS Version	License	Download Location	Homepage	Copyright Text	Vulnerability	Comments	Depends On
~	~	~	~	~	~	~	~	~	~	~
39	pkg:pypi/pillow@10...	pillow	10.4.0	HPND	https://pypi.o...	https://github... Different from DE				direct
5	pkg:pypi/aioitertools...	aioitertools	0.11.0	MIT	https://pypi.o...	https://github... Different from DE				transitive
47	pkg:pypi/pymysql@...	PyMySQL	1.1.0	MIT	https://pypi.o...	https://pypi.o... Different from DE				transitive
52	pkg:pypi/rsa@4.9.1	python-rsa	4.9.1	Apache-2.0	https://pypi.o...	https://github... Different from DE				transitive
3	pkg:pypi/aiobotocore...	aiobotocore	2.6.0	Apache-2.0	https://pypi.o...	https://pypi.p... Different from DE				transitive
24	pkg:pypi/fastapi@0....	fastapi	0.115.8	MIT	https://pypi.o...	https://github... Different from DE				direct
32	pkg:pypi/jsondiff@2...	jsondiff	2.0.0	MIT	https://pypi.o...	https://github... Different from DE				direct
51	pkg:pypi/requests@...	requests	2.31.0	Apache-2.0	https://pypi.o...	https://github... Different from DE				transitive

Page 1 of 1 200 Count: 62



PURL 정보 제공 NEW

Open Source Information

OSS Name ⓘ

aiokafka

Nickname

pypi:aiokafka

OSS Version

0.12.0

Vulnerability Info «**OSS Type****Declared License**

	License	Restriction
	Apache-2.0	

Detected License**Restriction****License Type**

Permissive

Obligation**Download Location**<https://pypi.org/project/aiokafka> (pkg:pypi/aiokafka)**Home Page**<https://github.com/aio-libs/aiokafka>**Copyright**

Copyright 2016 Taras Voinarovskiy

Summary Description**Important Notes****Attribution**



Dependency Tree

3rd party **DEP** SRC BIN BOM

FOSSLight Report [fosslight_report_dep_250930_1701](#)
2025-09-30 17:02:11



ID	Package URL	OSS Name	OSS Version	L
~	~	~	~	~
39	pkg:pypi/pillow@10.4.0	pillow	10.4.0	HPND
5	pkg:pypi/aioitertools@0.11.0	aioitertools	0.11.0	MIT
47	pkg:pypi/pymysql@1.1.0	PyMySQL	1.1.0	MIT
52	pkg:pypi/rsa@4.9.1	python-rsa	4.9.1	Apache-2.0
3	pkg:pypi/aiobotocore@2.6.0	aiobotocore	2.6.0	Apache-2.0
24	pkg:pypi/fastapi@0.115.8	fastapi	0.115.8	MIT
32	pkg:pypi/jsondiff@2.0.0	jsondiff	2.0.0	MIT
51	pkg:pypi/requests@2.31.0	requests	2.31.0	Apache-2.0

[Open LIS#panel_partner_list](#)

The Dependency Tree supports a maximum depth of 5 levels.

Dependency Tree (Package Url)

+ Expand All - Collapse All

pkg:pypi/pillow@10.4.0	
- pkg:pypi/fastapi@0.115.8	
- > pkg:pypi/starlette@0.45.3	
- > pkg:pypi/anyio@3.7.1	
- pkg:pypi/sniffio@1.3.0	
- pkg:pypi/idna@3.4	
- pkg:pypi/exceptiongroup@1.1.3	
- > pkg:pypi/pydantic@2.4.2	
- pkg:pypi/annotated-types@0.6.0	
- > pkg:pypi/pydantic-core@2.10.1	
- pkg:pypi/typing-extensions@4.8.0	
- pkg:pypi/typing-extensions@4.8.0	
- pkg:pypi/jsondiff@2.0.0	
- > pkg:pypi/requests@2.31.0	
- pkg:pypi/certifi@2025.1.31	
- pkg:pypi/urllib3@1.26.18	
- pkg:pypi/idna@3.4	
- pkg:pypi/charset-normalizer@3.3.0	

Page 1 of 1 200 Count: 62



02

Security



02 Security 템

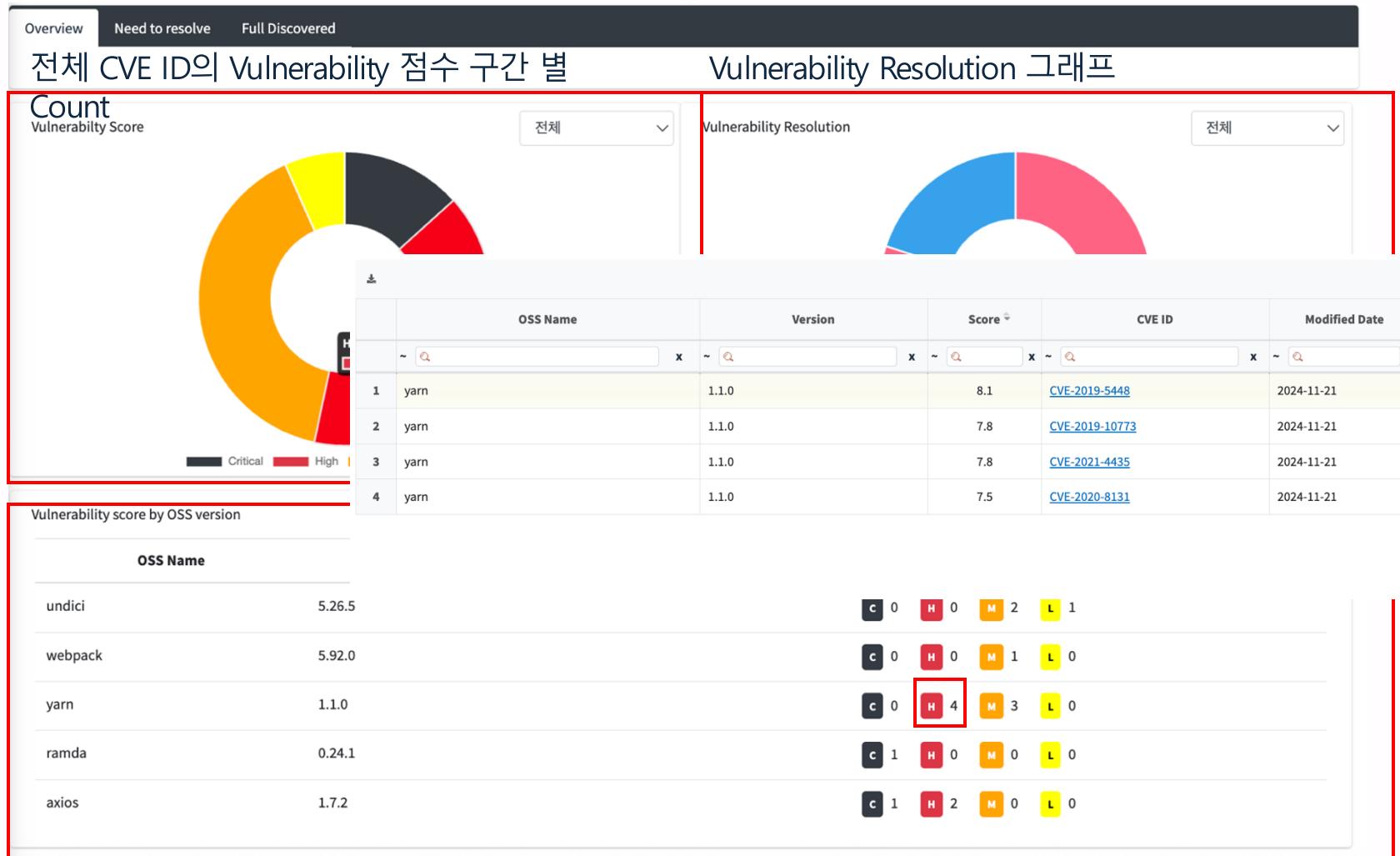
- 프로젝트별 보안취약점 관리

ID	Project Name	Status	OSC Process	Download	Security
747	datafile collector	Progress	Identification > Packaging		Need to resolve(9.8)
737	test_sec_mail	Request	Identification > Packaging		Discovered(N/A)
736	Test empty project (1.0)	Request	Identification > Packaging		Discovered(N/A)
735	dep-test (1)	Request	Identification > Packaging		Discovered(N/A)
734	qwer (1.0)	Request	Identification > Packaging		Discovered(N/A)
733	test_prj	Request	Identification > Packaging		Need to resolve(9.9)
732	my.project coffee	Request	Identification > Packaging		Need to resolve(9.8)
731	a123sdfs	Progress	Identification > Packaging		Need to resolve(7.5)

- Need to resolve(XX) : 기준 점수 이상 보안취약점이 존재하는 경우
- Discovered(XX) : 기준 점수 이상 보안취약점이 존재하지 않는 경우
- Resolved(XX) : Need to resolve 템 기준 점수 이상 취약점이 모두 'Fixed' resolution인 경우
- BOM 템 기준임. 각 상태 (괄호) 안에서 프로젝트 내 vulnerability max score 확인 가능함



Security – Overview NEW



OSS 버전별로 Vulnerability 점수에 대한 count 및 상세 정보 제공

02

Security - Need to resolve / Full discovered

- Need to resolve : 기준 점수 이상인 CVE ID 목록 확인 가능
- Full Discovered : 검출된 전체 CVE ID 목록

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 Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerability Link	Affected SW Version Range	Security Comments
cocoon	2.1.9	CVE-2020-11991	7.5	2020-09-11	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2020-11991	From (including) : 2.1 Up to (including) : 2.1.12	
cocoon	2.1.9	CVE-2025-24783	7.5	2025-01-27	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2025-24783	N/A	
Linux Kernel	2.6.27	CVE-2009-4538	10.0	2010-01-12	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2009-4538	Up to (including) : 2.6.32.3	
Linux Kernel	2.6.27	CVE-2015-1421	10.0	2015-03-16	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2015-1421	From (including) : 2.6.24 Up to (excluding) : 3.2.67	
Linux Kernel	2.6.27	CVE-2008-5134	10.0	2008-11-18	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2008-5134	Up to (including) : 2.6.27.4	



Custom column 적용 NEW

NEW

- 테이블 내 원하는 column명만 보일 수 있도록 커스터마이징 가능



Affected SW Version Range 정보 NEW

- Affected SW Version Range 및 Running on/with 정보 표시

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 ([hide](#))

~~cpe:2.3:a:google:chrome:*~~;~~**~~;~~**~~;~~**~~;~~**~~;~~*~~

[Show Matching CPE\(s\)▼](#)

Running on/with

~~cpe:2.3:o:microsoft:windows:*~~;~~**~~;~~**~~;~~**~~;~~**~~;~~*~~

[Show Matching CPE\(s\)▼](#)

Up to (excluding)
136.0.7103.113

OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerability Link	Affected SW Version Range	Security Comments
chrome	9.0.597.5	CVE-2025-4609	9.6	2025-08-22	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2025-4609	Up to (excluding) : 136.0.7103.113 Running on/with microsoft:windows	
chrome	9.0.597.5	CVE-2022-0452	9.6	2022-04-05	Deferred (Not Available)	https://nvd.nist.gov/vuln/detail/CVE-2022-0452	Up to (excluding) : 98.0.4758.80	
chrome	9.0.597.5	CVE-2020-6469	9.6	2020-05-21	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2020-6469	Up to (excluding) : 83.0.4103.61	
chrome	9.0.597.5	CVE-2022-4920	9.6	2023-07-29	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2022-4920	Up to (excluding) : 101.0.4951.41	
chrome	9.0.597.5	CVE-2021-21121	9.6	2021-02-09	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2021-21121	Up to (excluding) : 88.0.4324.96	
chrome	9.0.597.5	CVE-2018-17472	9.6	2018-11-14	Deferred (Not Available)	https://nvd.nist.gov/vuln/detail/CVE-2018-17472	Up to (excluding) : 70.0.3538.67 Running on/with apple:iphone_os	



신규 보안취약점 발견시 메일 발송

- Security Vulnerability Score 이상인 신규 보안취약점 발견시, 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	<p>In the Linux kernel, the following vulnerability has been resolved:</p> <p>Bluetooth: qca: add missing firmware sanity checks</p> <p>Add the missing sanity checks when parsing the firmware files before downloading them to avoid accessing and corrupting memory beyond the vmallocoed buffer.</p> <p>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 vmallocoed.</p>	2024-05-30	2025-09-30



02 보안취약점 메일링 및 담당자 설정 NEW

- 메일링 Enable/Disable 설정 가능
- Security 담당자 설정 가능

Project Information

Project Name*Project VersionPriority*

test_min

1000

P2

View PermissionSecurity Mail (Vulnerability)Security Responsible Person

EveryoneCreator & EditorEnable Disable

Operating System*Distribution Type*

Linux

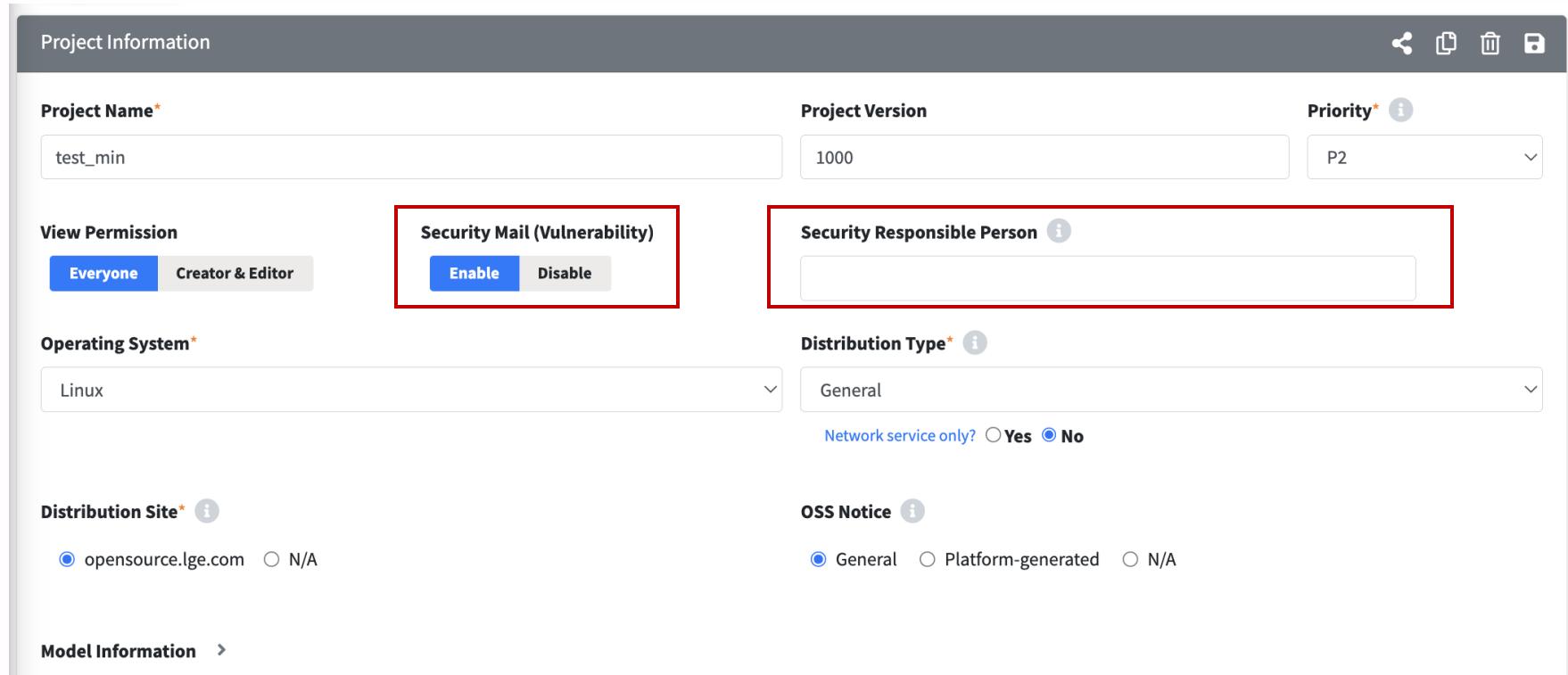
General
Network service only? Yes No

Distribution Site*OSS Notice

opensource.lge.com N/A

General Platform-generated N/A

[Model Information >](#)





02 보안취약점 데이터 베이스 수집

- 일 1회, NVD에서 제공되는 REST API를 통해 데이터 취득하여 DB에 저장



2.0 APIs



02 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

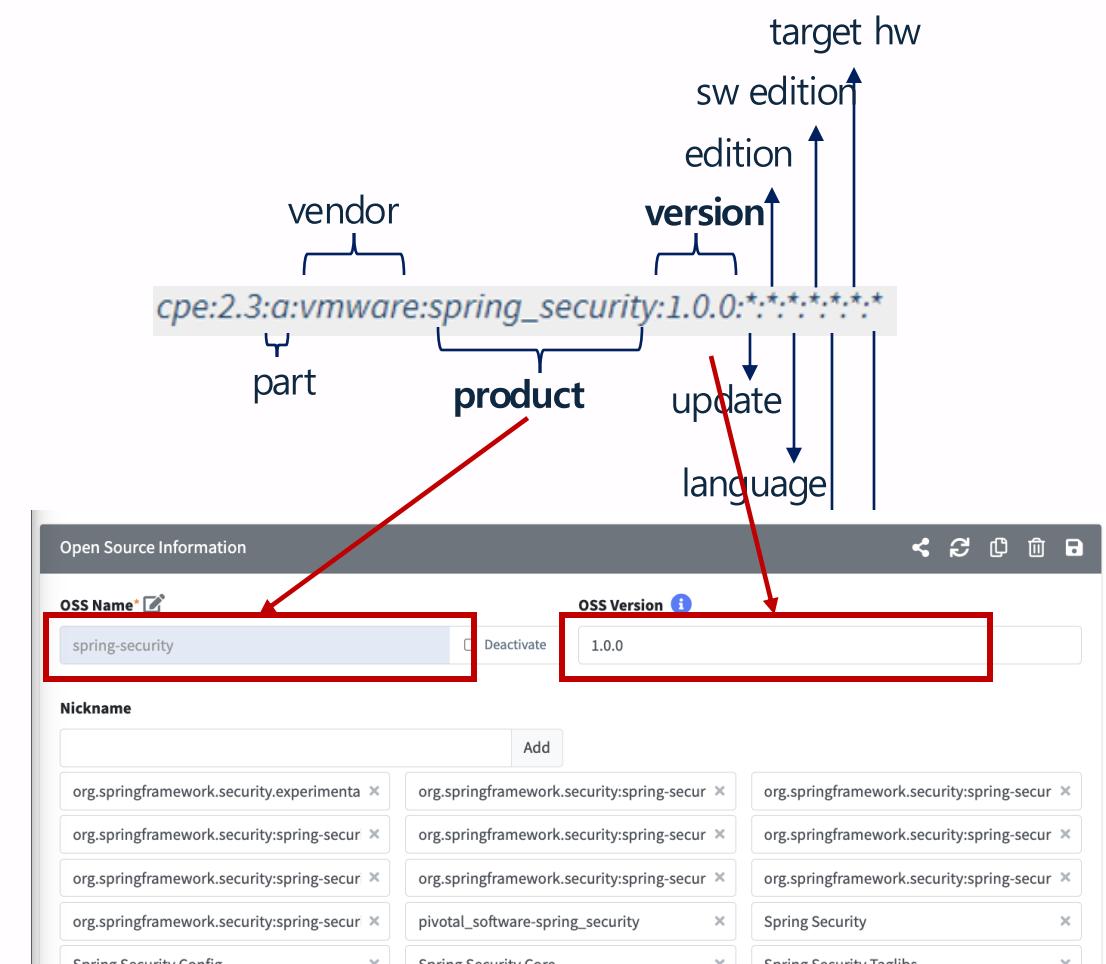
Configuration 1 ([hide](#))

cpe:2.3:a:vmware:spring_security:* [Hide Matching CPE\(s\) ▾](#)

- 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:***

Up to (excluding)

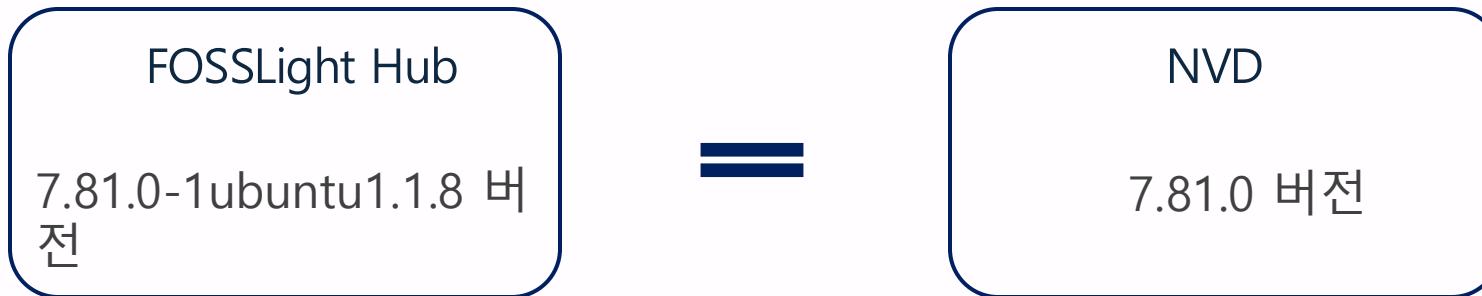
5.5.7





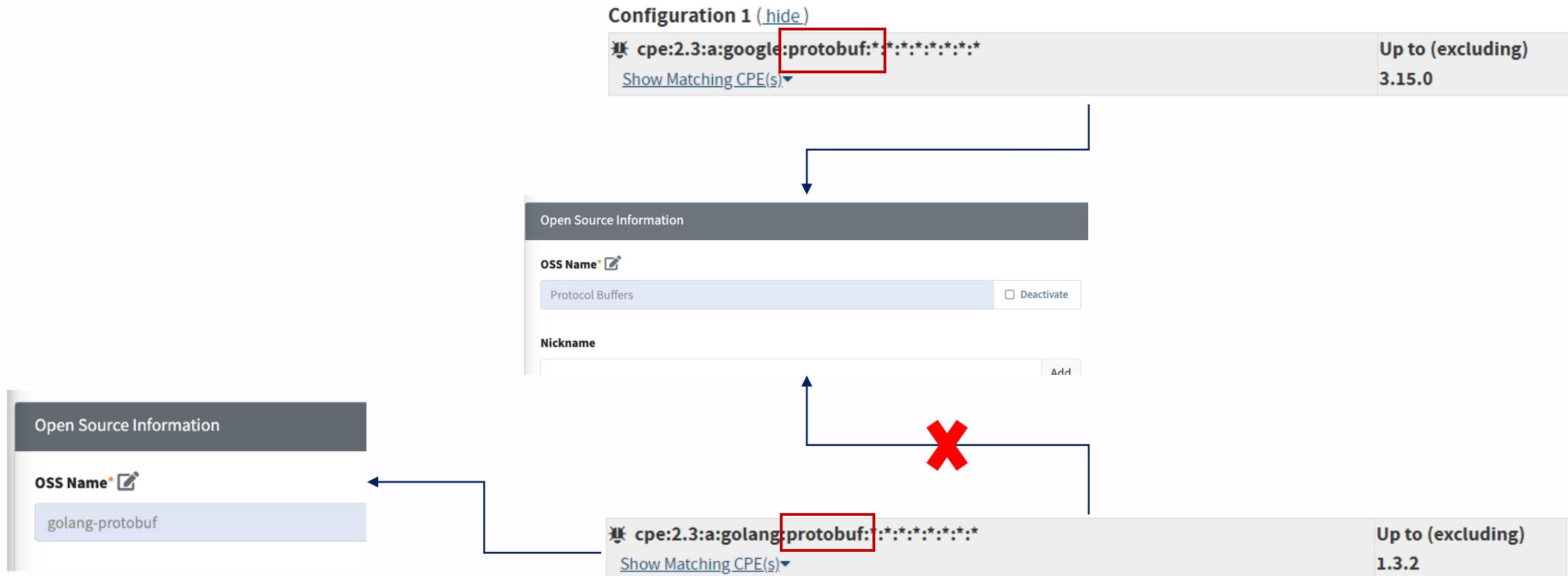
02 보안취약점 버전 관리

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



02 Include CPE

- OSS에 매핑이 누락된 보안취약점 정보를 추가하는 기능 제공



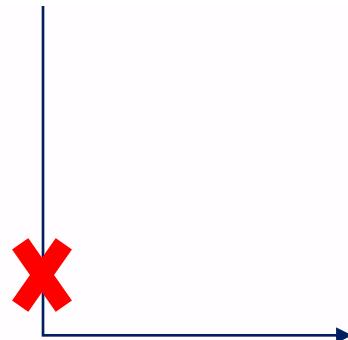
02

Exclude CPE

- OSS에 잘못 매팅된 보안취약점 정보를 제외하는 기능 제공

Configuration 1 ([hide](#))

cpe:2.3:a:npmj...tar:...:...:...:node.js:...*	Up to (excluding)	
	4.4.16	
cpe:2.3:a:npmj...tar:...:...:...:node.js:...*	From (including)	Up to (excluding)
	5.0.0	5.0.8
cpe:2.3:a:npmj...tar:...:...:...:node.js:...*	From (including)	Up to (excluding)
	6.0.0	6.1.7



Open Source Information

OSS Name* v-Diff Deactivate

Nickname

감사합니다
FOSSLight Hub 2.0

