FOSSLight Hub 업데이트

Dependency & Security

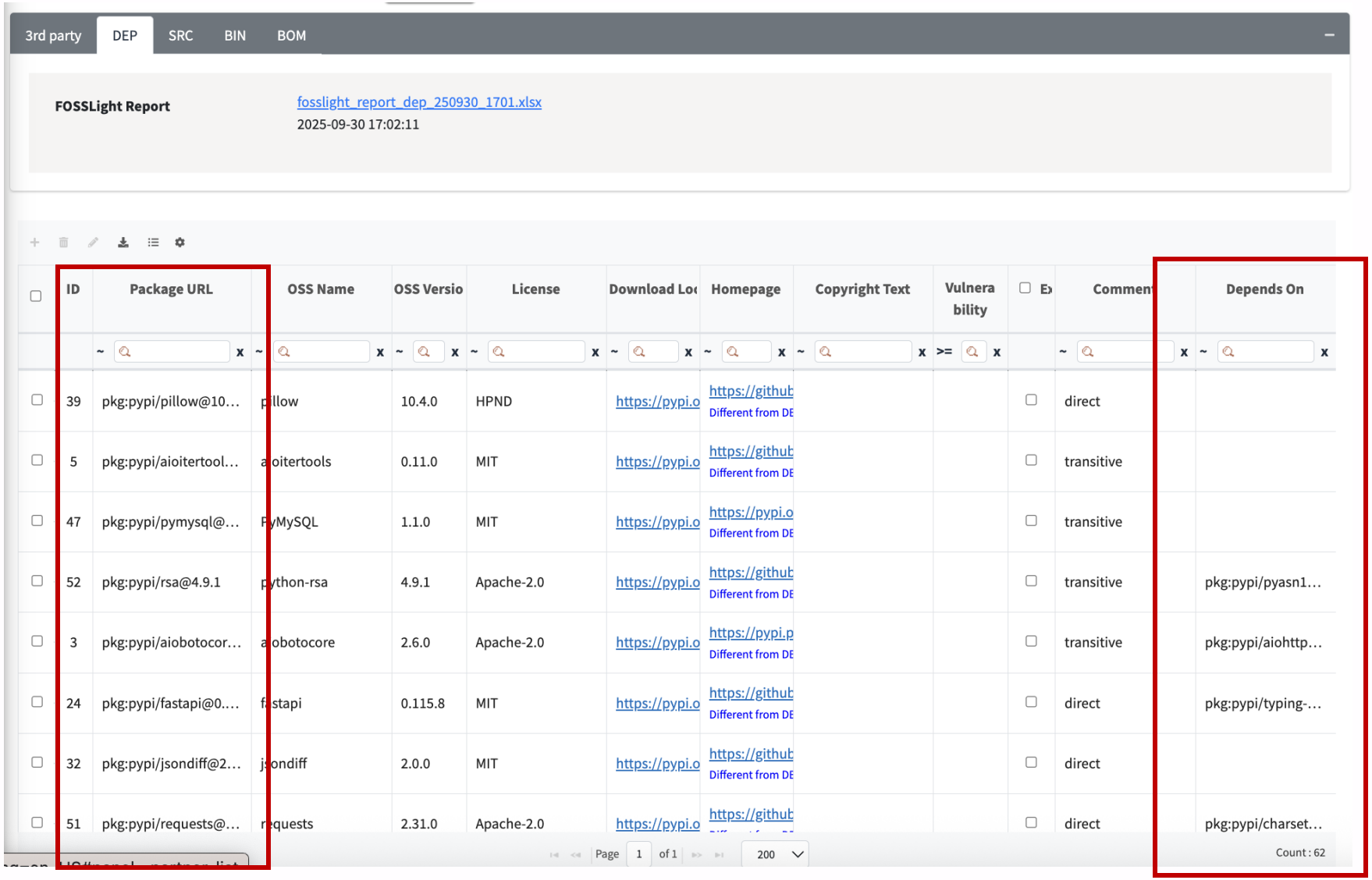
석지영 책임 연구원
LG 전자

Contents

01

Dependency

01 PURL 정보 제공 NEW

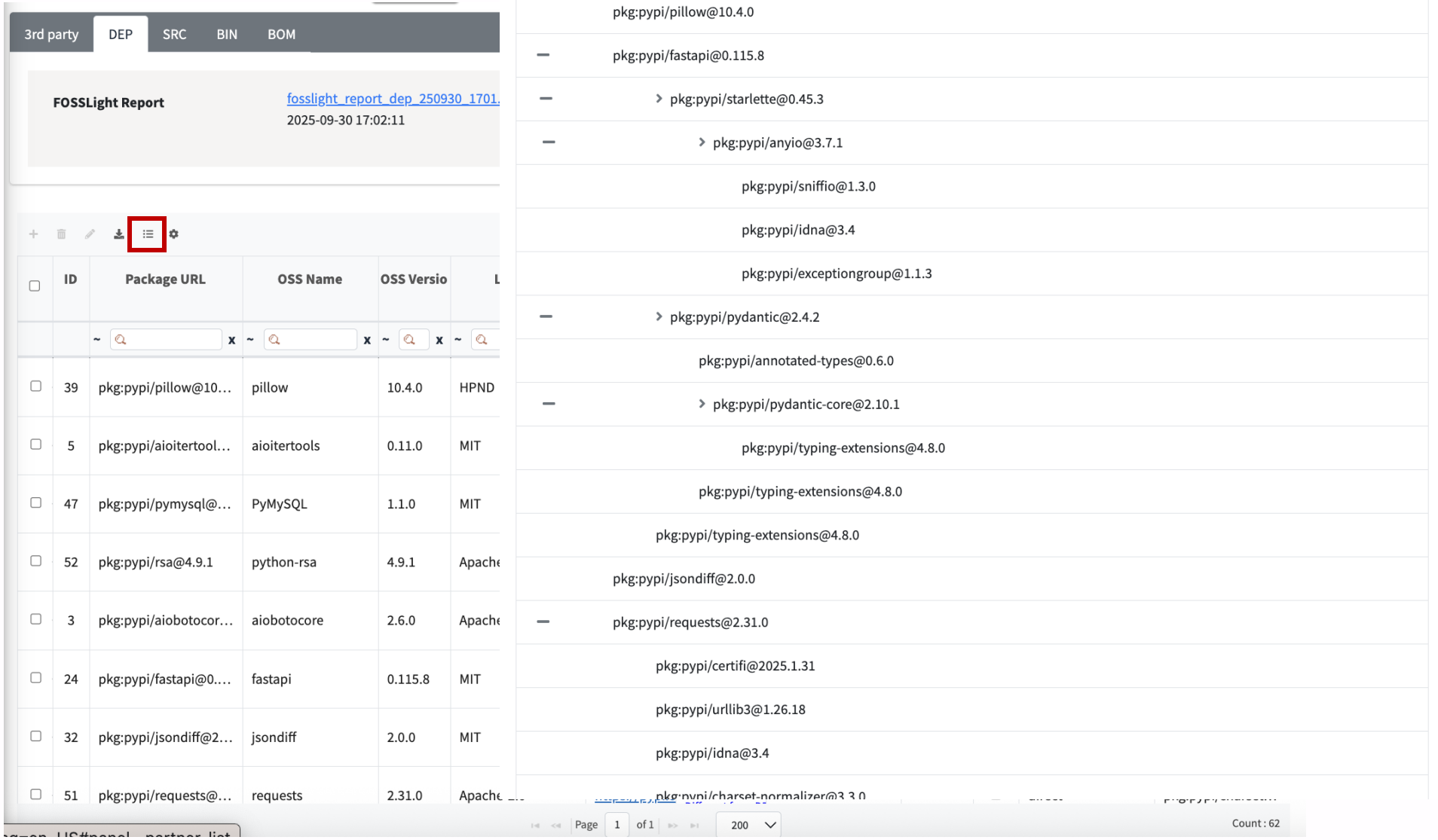


01 PURL 정보 제공 NEW

Open Source Information

OSS Name	aiokafka
Nickname	pypi:aiokafka
OSS Version	0.12.0
Vulnerability Info	
OSS Type	
Declared License	License: Apache-2.0 (Restriction)
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 Voinarovskyi
Summary Description	
Important Notes	
Attribution	

01 Dependency Tree



02

Security

02 Security 탭

- 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)

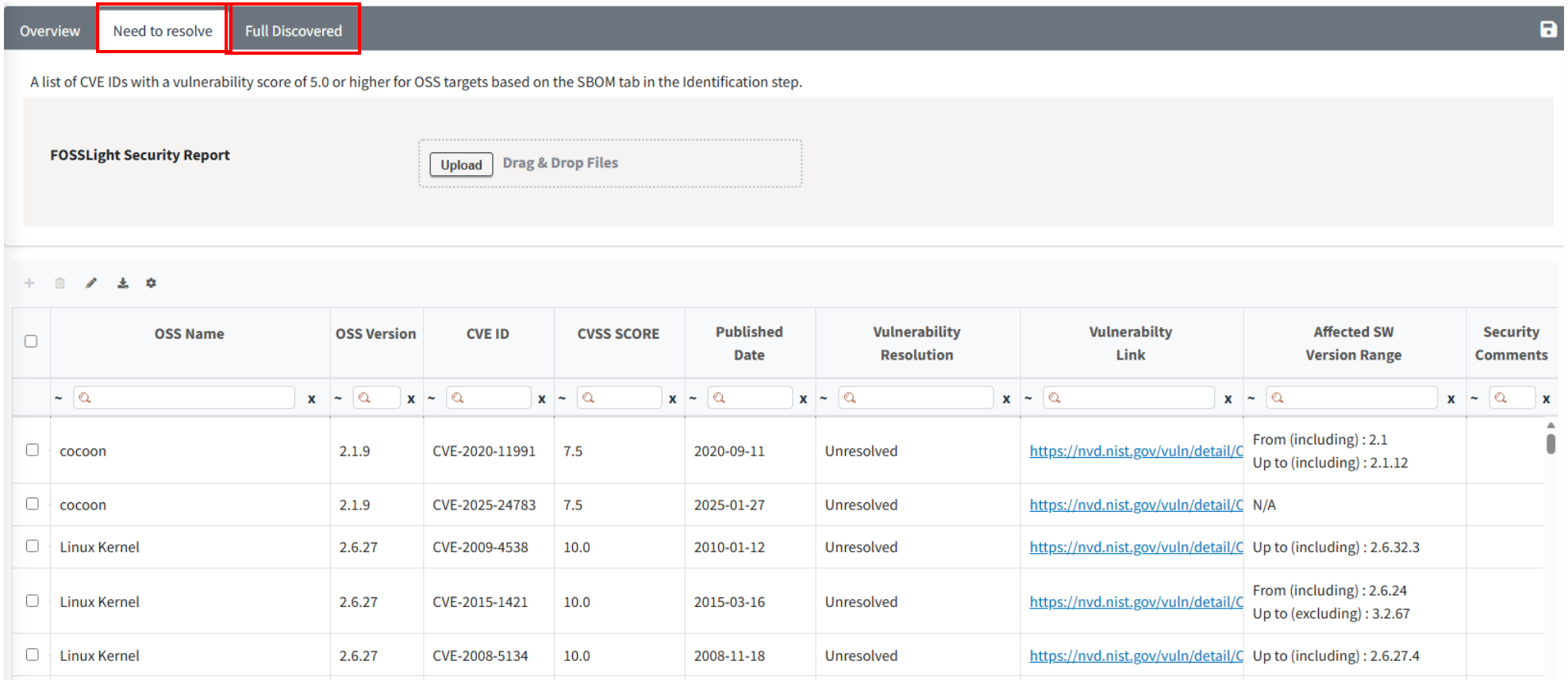
- Need to resolve(XX) : 기준 점수 이상 보안취약점이 존재하는 경우
- Discovered(XX) : 기준 점수 이상 보안취약점이 존재하지 않는 경우
- Resolved(XX) : Need to resolve탭 기준 점수 이상 취약점이 모두 'Fixed' resolution인 경우
- BOM탭 기준임. 각 상태 (괄호) 안에서 프로젝트 내 vulnerability max score 확인 가능함

02 Security – Overview NEW

OSS 버전별로 Vulnerability 점수에 대한 count 및 상세 정보 제공

02 Security - Need to resolve / Full discovered

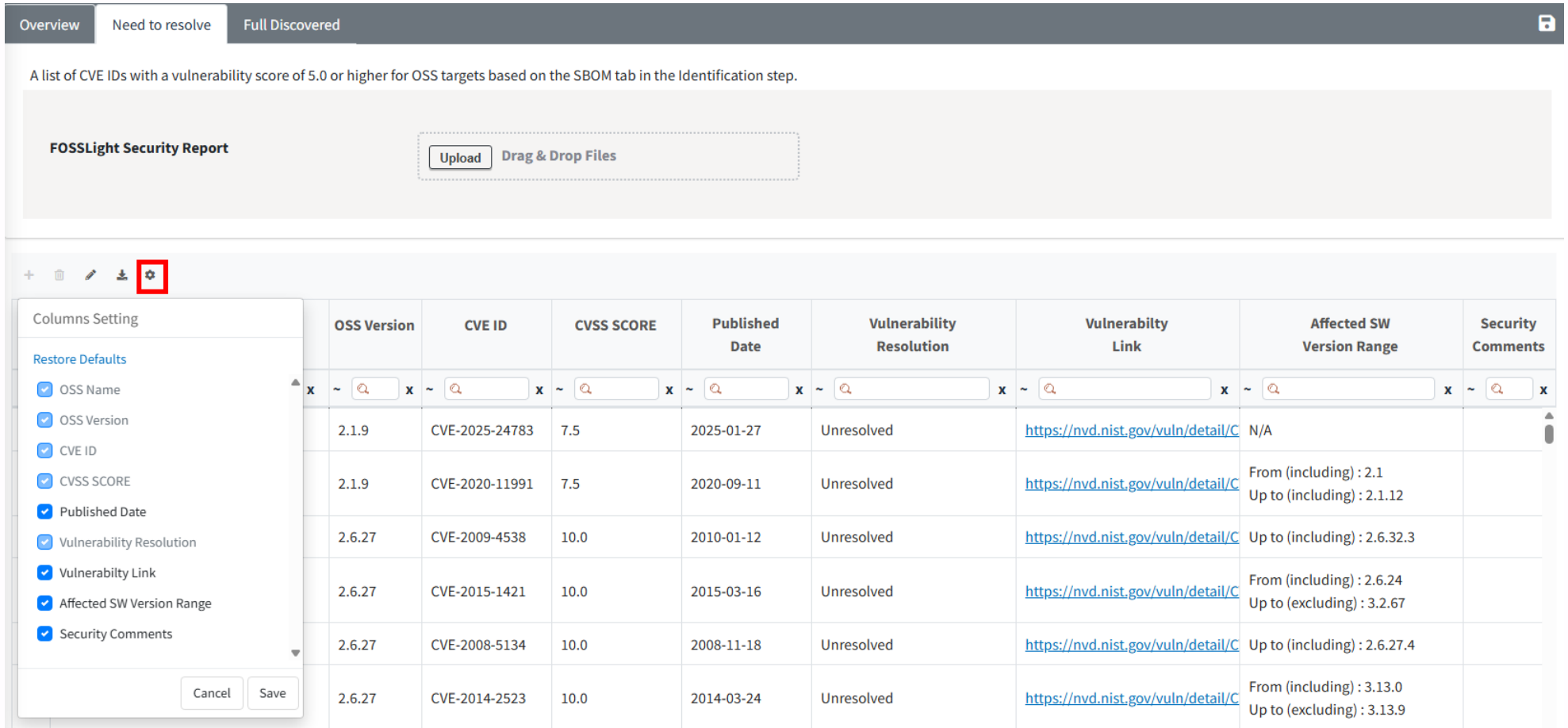
- Need to resolve : 기준 점수 이상인 CVE ID 목록 확인 가능
- Full Discovered : 검출된 전체 CVE ID 목록



OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerabilty 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/C	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/C	N/A	
Linux Kernel	2.6.27	CVE-2009-4538	10.0	2010-01-12	Unresolved	https://nvd.nist.gov/vuln/detail/C	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/C	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/C	Up to (including) : 2.6.27.4	

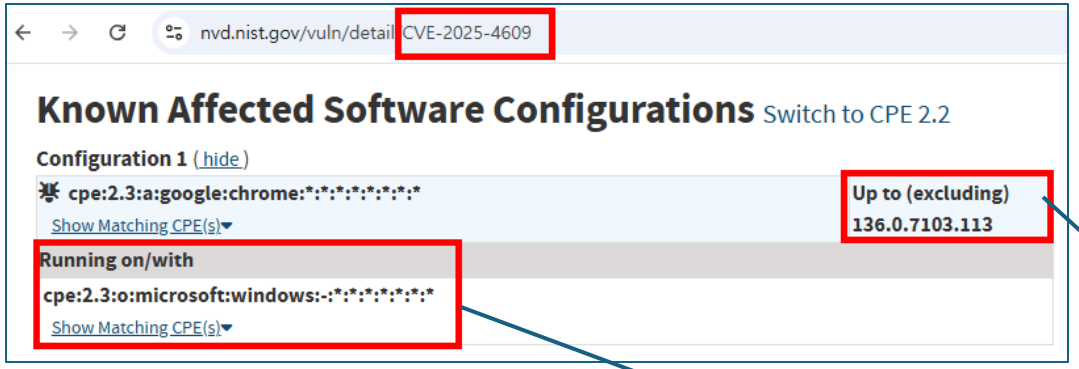
02 Custom column 적용 NEW

- 테이블 내 원하는 column명만 보일 수 있도록 커스터마이징 가능



02 Affected SW Version Range 정보 NEW

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



OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerabilty 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/C	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/C	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/C	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/C	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/C	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/C	Up to (excluding) : 70.0.3538.67 Running on/with apple:iphone_os	

02 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

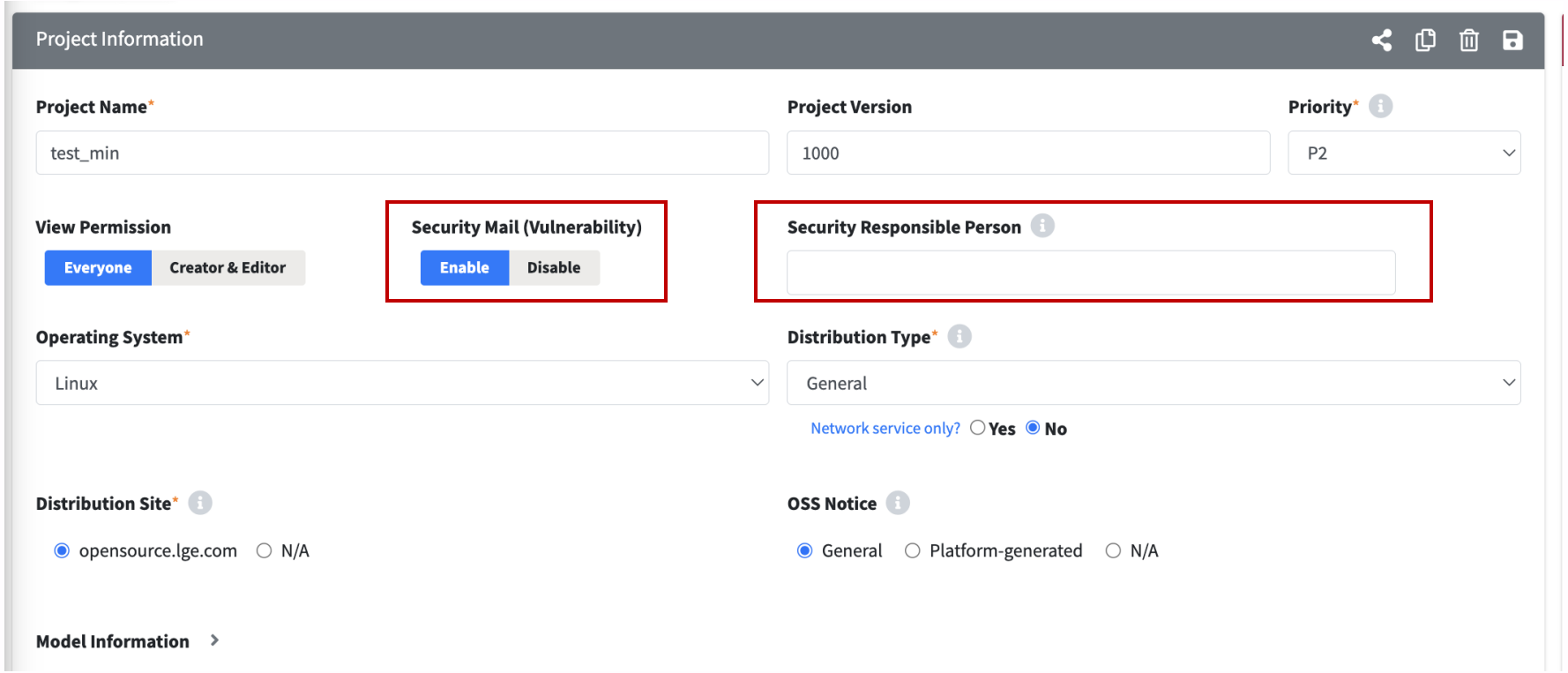
	Registered Data
Project Name	user-test-android
Project Version	3.0
Security Mail	Enable
Security Responsible Person	
Operating System	Linux
Distribution Type / Network Service Only?	General / N
Distribution Site	opensource.lge.com
OSS Notice	Platform-generated
Priority	P2
Creator	CTO 블록체인연구실 시스템관리자(oscAdmin)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

02 보안취약점 메일링 및 담당자 설정 NEW

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



02 보안취약점 데이터 베이스 수집

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

NIST

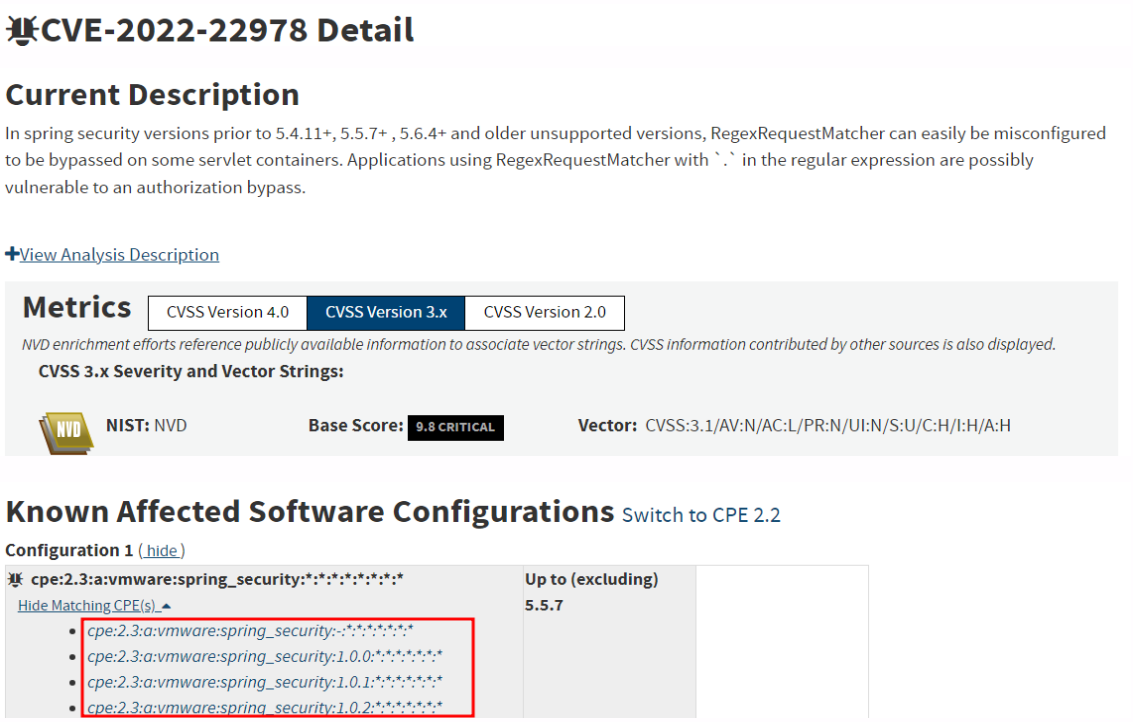
Information Technology Laboratory

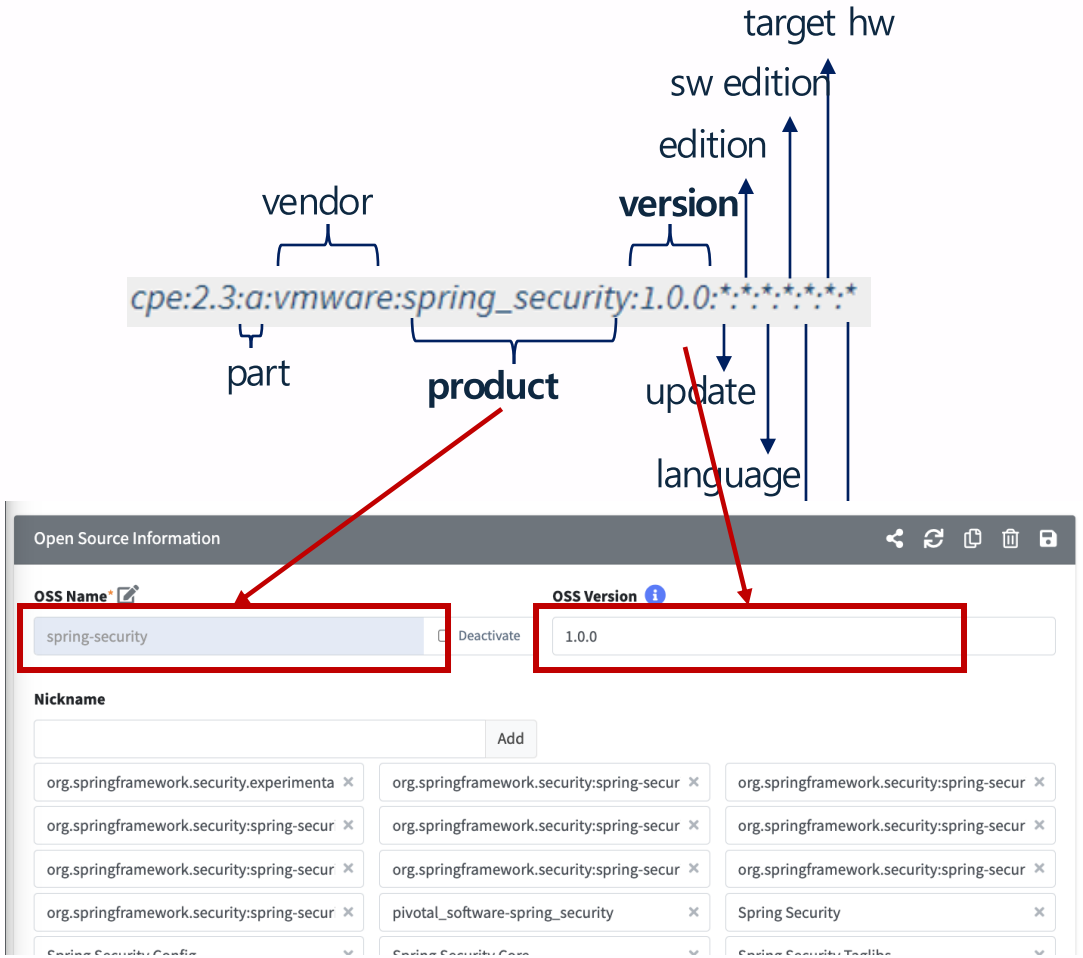
NATIONAL VULNERABILITY DATABASE

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





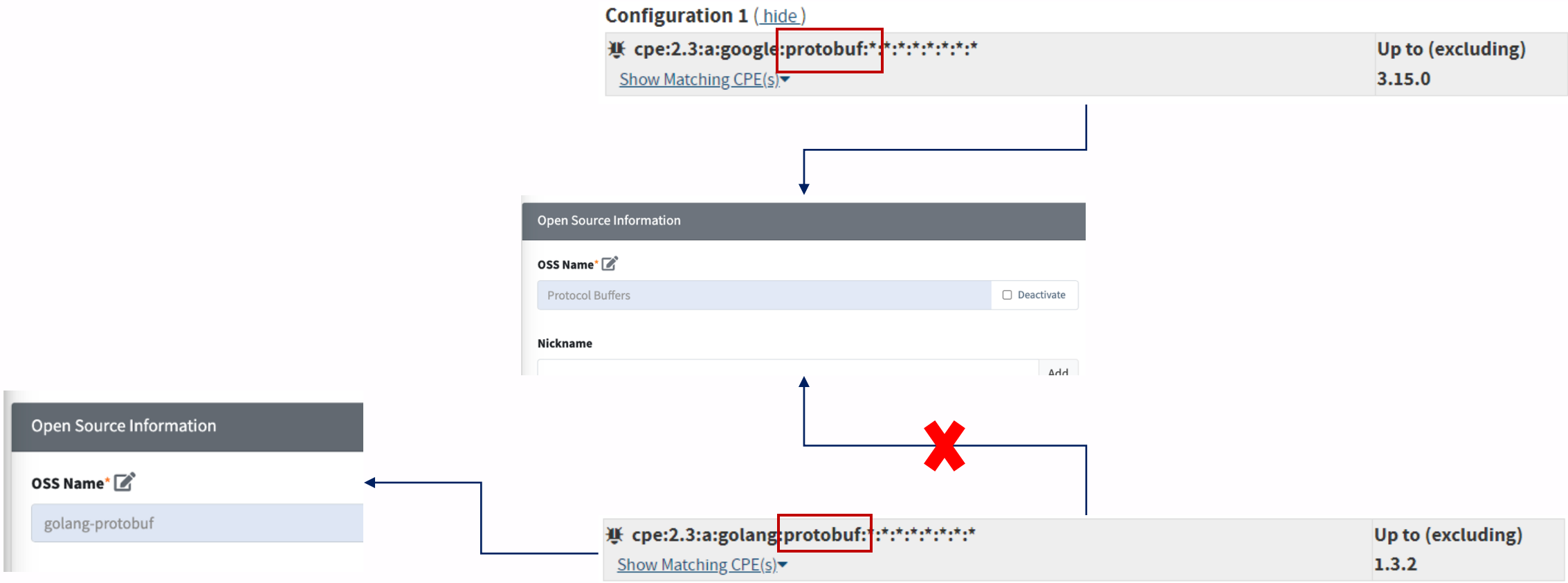
02 보안취약점 버전 관리

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

FOSSLight Hub		NVD
7.81.0-1ubuntu1.1.8 버전	=	7.81.0 버전

02 Include CPE

- OSS에 매핑이 누락된 보안취약점 정보를 추가하는 기능 제공

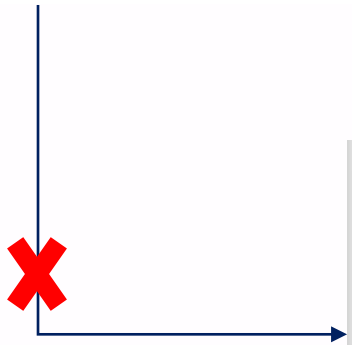


02 Exclude CPE

- OSS에 잘못 매핑된 보안취약점 정보를 제외하는 기능 제공

Configuration 1 (hide)

cpe:2.3:a:npmjs:tar:*:*:*:*:*:node.js:*:* Show Matching CPE(s)	Up to (excluding) 4.4.16	
cpe:2.3:a:npmjs:tar:*:*:*:*:*:node.js:*:* Show Matching CPE(s)	From (including) 5.0.0	Up to (excluding) 5.0.8
cpe:2.3:a:npmjs:tar:*:*:*:*:*:node.js:*:* Show Matching CPE(s)	From (including) 6.0.0	Up to (excluding) 6.1.7



감사합니다

FOSSLight Hub 2.0