LGE Internal Use Only

LG Electronics Open Source Program Office

FOSSLight Hub

강화된 보안 취약점 검출 능력

2026.10.28 | LG전자 최혜성

NVD 중심 조회를 넘어 OSV까지 연결한 SBOM 기반 취약점 관리 구조

LG Open Source

CONTENTS

1. 취약점 관리 강화 배경
2. FOSSLight Hub 취약점 관리 구조
3. 메뉴별 취약점 확인 방법
4. OSV 데이터 연계 및 기대효과
5. 향후 지원 예정: VEX

왜 OSV가 필요한가?

NVD의 강점을 유지하면서, 오픈소스 생태계별 취약점 정보의 빈틈을 보완

NVD 중심 조회의 한계

- 생태계별 Advisory를 통한 상세 취약점 정보 반영이 어려움
- CVE가 발급되지 않은 오픈소스 취약점까지 포괄하기 어려움

NVD+ OSV

OSV 데이터의 보완 역할

- CVE가 없는 오픈소스 취약점까지 식별 범위 확대
- 패키지 생태계별 버전 체계를 반영한 취약점 영향 범위 분석
- OSV 고유 ID를 활용한 취약점 추적성 강화

※ Advisory(보안 권고): 오픈소스 프로젝트가 직접 제공하는 취약점 및 대응 정보

FOSSLight Hub 취약점 관리 구조

Vulnerability 데이터를 SBOM 컴포넌트와 연계해 메뉴별 조회·분석 기능으로 제공

Project > Identification > SBOM

프로젝트 SBOM을 구성하는 컴포넌트에서 취약점의 존재와 심각도를 확인

컴포넌트 중심

“이 프로젝트에 포함된 오픈소스 컴포넌트 중 취약한 항목은 무엇인가?”

1 / 식별

- OSS Name · OSS Version 등 → SBOM 목록

2 / 등급

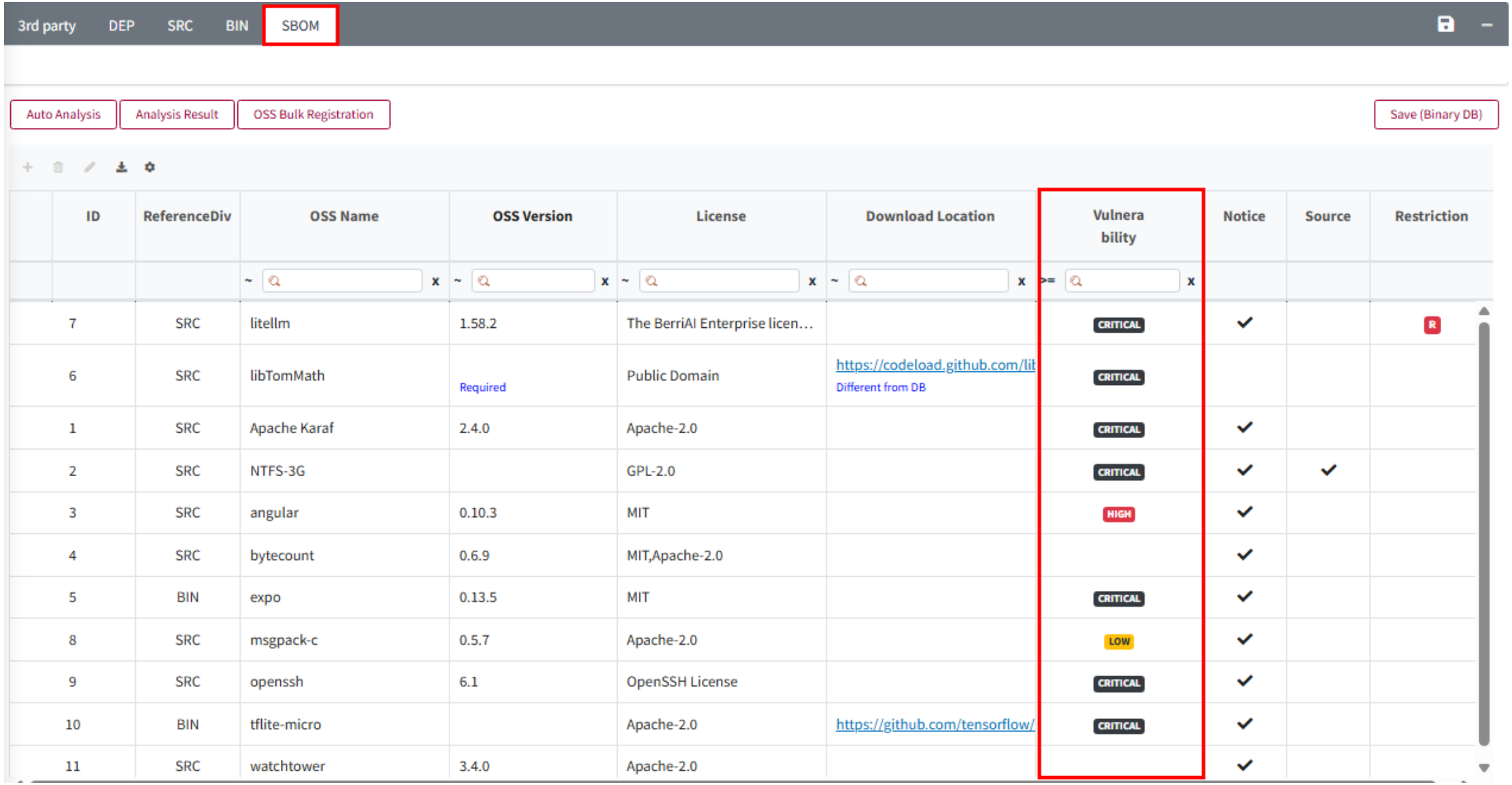
- Critical
- High
- Medium
- Low
- 미확인

3 / 상세

- 취약점 상세 팝업 (NVD / OSV ID)

Project > Identification > SBOM

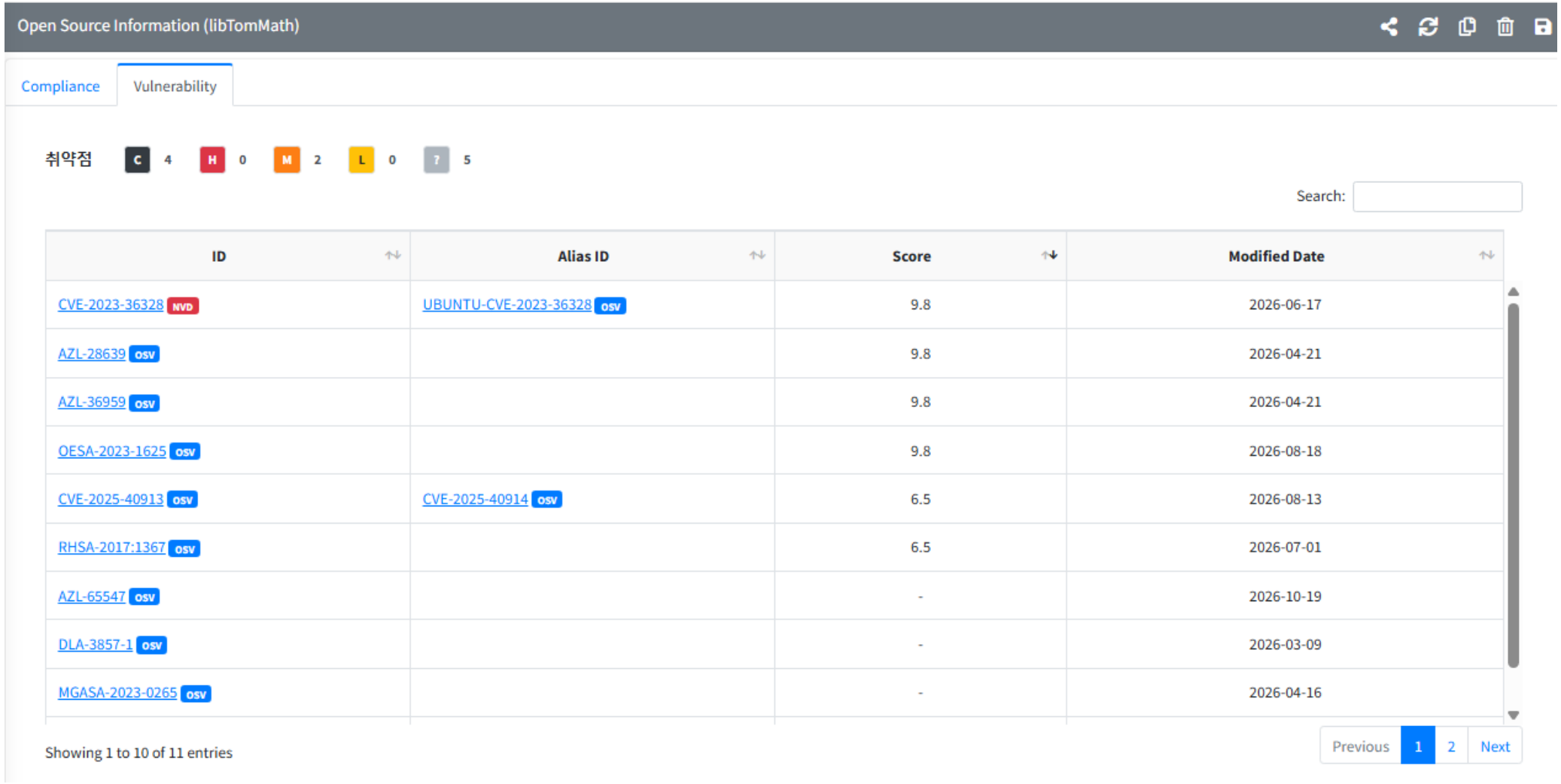
SBOM



	ID	ReferenceDiv	OSS Name	OSS Version	License	Download Location	Vulnerability	Notice	Source	Restriction
			~ x	~ x	~ x	~ x	>= x			
	7	SRC	litellm	1.58.2	The BerriAI Enterprise licen…		CRITICAL	✓		R
	6	SRC	libTomMath	Required	Public Domain	https://codeload.github.com/lit Different from DB	CRITICAL			
	1	SRC	Apache Karaf	2.4.0	Apache-2.0		CRITICAL	✓		
	2	SRC	NTFS-3G		GPL-2.0		CRITICAL	✓	✓	
	3	SRC	angular	0.10.3	MIT		HIGH	✓		
	4	SRC	bytecount	0.6.9	MIT,Apache-2.0			✓		
	5	BIN	expo	0.13.5	MIT		CRITICAL	✓		
	8	SRC	msgpack-c	0.5.7	Apache-2.0		LOW	✓		
	9	SRC	openssh	6.1	OpenSSH License		CRITICAL	✓		
	10	BIN	tflite-micro		Apache-2.0	https://github.com/tensorflow/	CRITICAL	✓		
	11	SRC	watchtower	3.4.0	Apache-2.0			✓		

Project > Identification > SBOM

Open Source > Information > Vulnerability



LG Electronics Open Source Program Office

Project > Security

프로젝트 취약점을 심각도와 해결 상태로 나누어 조치 흐름을 관리

Overview

- 취약점 Score 구간별 통계 및 차트 확인
- OSS Version별 취약점 Score 분포 확인
- Vulnerability Resolution별 건수 확인

Need to resolve

- 설정된 기준 점수 이상인 OSS에서 검출된 취약점 목록 확인
- Vulnerability ID, Score, Published Date 등 취약점 상세 정보 확인
- Vulnerability Resolution 및 패치 정보 관리

Full Discovered

- Need to resolve와 동일한 취약점 상세 정보를 전체 OSS를 대상으로 확인

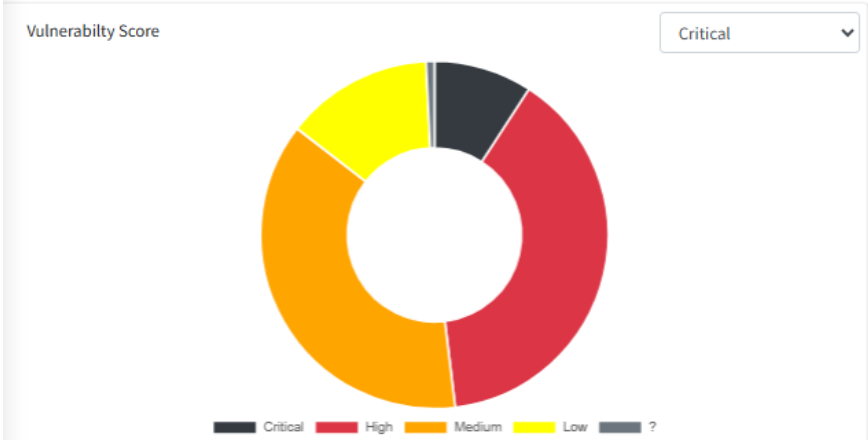
Project > Security

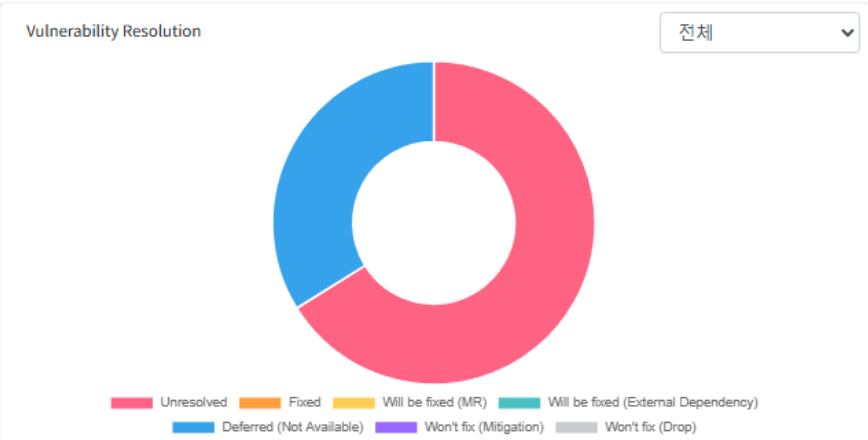
Overview

Overview | Need to resolve | Full Discovered

다음 오픈소스는 버전이 입력되지 않아 전체 CVE 정보를 출력할 수 없습니다. Identification 탭에서 다음 오픈소스 버전 정보를 입력해주시기 바랍니다.

- libTomMath, NTFS-3G, tflite-micro





Vulnerability score by OSS version

OSS Name	OSS Version	Vulnerability Score
angular	0.10.3	C 0 H 18 M 8 L 0 ? 0
Apache Karaf	2.4.0	C 4 H 6 M 7 L 0 ? 0
expo	0.13.5	C 1 H 0 M 0 L 0 ? 1
litellm	1.58.2	C 3 H 9 M 5 L 10 ? 0
msgpack-c	0.5.7	C 0 H 0 M 0 L 1 ? 0
openssh	6.1	C 4 H 18 M 29 L 7 ? 0

Project > Security

Need to resolve

Overview | Need to resolve | Full Discovered

FOSSLight Security Report

Upload Drag & Drop Files

OSS Name	OSS Version	Vulnerability ID	Score	CPE	Published Date	Vulnerability Resolution	Vulnerabilty Link	Official Security Patch Link	Security Patch Link for Internal	Affected SW Version Range
angular	0.10.3	CVE-2025-66412	8.5	cpe:2.3:a:an…	2025-12-01	Unresolved	https://nvd.nist.gov/vuln/deta	https://github.com/angular/a	N/A	From (including) : 21.0.0 Up to (excluding) : 21.0.2 From (including) : 19.0.0 Up to (excluding) : 19.2.17 From (including) : 20.0.0 Up to (excluding) : 20.3.15 Up to (including) : 18.2.14
angular	0.10.3	CVE-2026-22610	8.5	cpe:2.3:a:an…	2026-01-10	Unresolved	https://nvd.nist.gov/vuln/deta	https://github.com/angular/a https://github.com/angular/a	N/A	From (including) : 21.0.0 Up to (excluding) : 21.0.7 From (including) : 19.0.0 Up to (excluding) : 19.2.18 From (including) : 20.0.0 Up to (excluding) : 20.3.16 Up to (including) : 18.2.14
								https://github.com/angular/a		From (including) : 20.0.0 Up to (excluding) : 20.3.17

Project > Security

Full Discovered

Overview | Need to resolve | Full Discovered

Identification 단계의 SBOM 탭 기준 OSS 대상으로 검출된 전체 취약점 목록입니다.

OSS Name	OSS Version	Vulnerability ID	Score	CPE	Published Date	Vulnerability Resolution	Vulnerabilty Link	Official Security Patch Link	Security Patch Link for Internal	Affected SW Version Range	Security Comments
angular	0.10.3	CVE-2026-50…	8.6	cpe:2.3:a:an…	2026-06-22	Unresolved	https://nvd.nist.gov/vuln/deta	https://github.com/angular/dc	N/A	From (including) : 20.0.0 Up to (excluding) : 20.3.24 From (including) : 21.0.0 Up to (excluding) : 21.2.16	
angular	0.10.3	CVE-2026-50…	5.3	cpe:2.3:a:an…	2026-06-22	Unresolved	https://nvd.nist.gov/vuln/deta	https://github.com/angular/ar	N/A	From (including) : 19.0.0 Up to (excluding) : 19.2.22 From (including) : 20.0.0 Up to (excluding) : 20.3.22 Up to (including) : 18.2.14 From (including) : 21.0.0 Up to (excluding) : 21.2.15	
angular	0.10.3	CVE-2026-52…	5.3	cpe:2.3:a:an…	2026-06-22	Unresolved	https://nvd.nist.gov/vuln/deta	https://github.com/angular/ar	N/A	From (including) : 20.0.0 Up to (excluding) : 20.3.22 From (including) : 19.0.0 Up to (excluding) : 19.2.23 Up to (including) : 18.2.14 From (including) : 21.0.0 Up to (excluding) : 21.2.15	
										From (including) : 21.0.0 Up to (excluding) : 21.2.17	

Open Source / Open Source > Information > Vulnerability

OSS를 기준으로 취약점을 확인하는 두 단계의 분석 흐름 (OSS를 찾고 → 해당 OSS에 연결된 취약점을 상세 확인)

Open Source

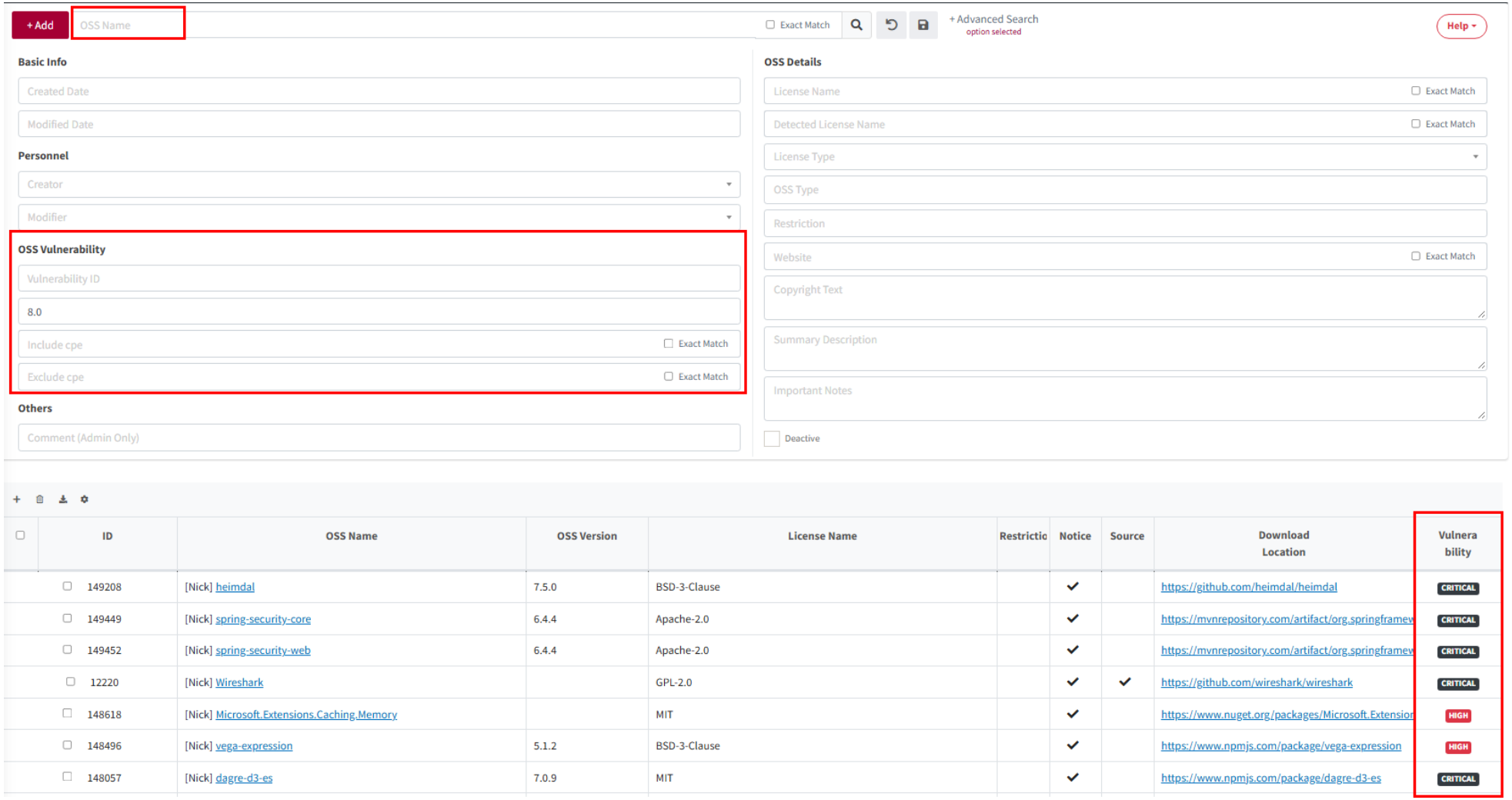
- OSS Name / Version별 취약점 아이콘으로 취약점 존재 여부와 심각도 확인
- 등록된 OSS 정보와 취약점을 조건별로 검색·확인

Open Source > Information > Vulnerability

선택한 OSS와 버전에 연결된 취약점 목록을 확인
- 취약점 ID 및 데이터 출처 확인(NVD ID, OSV Alias ID)
- 취약점 Score 확인
- Modified Date 확인

Open Source / Open Source > Information > Vulnerability

Open Source



Open Source / Open Source > Information > Vulnerability

Open Source > Information > Vulnerability

Open Source Information (curl 8.6.0)

Compliance | Vulnerability

취약점 C 6 H 13 M 20 L 4 ? 12

Search:

ID	Alias ID	Score	Modified Date
CVE-2026-10536 NVD	CURL-CVE-2026-10536 OSV	9.8	2026-09-15
CVE-2026-11856 NVD	CURL-CVE-2026-11856 OSV	9.8	2026-09-15
CVE-2026-19931 NVD	CURL-CVE-2026-19931 OSV	9.8	2026-09-15
CVE-2026-18924 NVD	CURL-CVE-2026-18924 OSV	9.1	2026-09-15
CVE-2026-8924 NVD	CURL-CVE-2026-8924 OSV	9.1	2026-09-15
CVE-2026-8927 NVD	CURL-CVE-2026-8927 OSV	9.1	2026-09-15
CVE-2024-2398 NVD	CURL-CVE-2024-2398 OSV	8.6	2026-10-15
CVE-2026-82209 NVD	CURL-CVE-2026-82209 OSV	8.2	2026-09-15
CVE-2026-8286 NVD	CURL-CVE-2026-8286 OSV	8.1	2026-09-15

Showing 1 to 10 of 55 entries

Previous 1 2 3 4 5 6 Next

Vulnerability

NVD·OSV 취약점 정보를 직접 검색·확인하는 독립 메뉴

검색 조건

- Vulnerability ID
- Source: NVD / OSV
- Component (Name)

결과 필드

- Vulnerability ID
- Source
- Component (Name)
- Affected versions
- Severity (score)

추가 기능

- ID 클릭시 취약점 생세 페이지 이동
- 검색 결과 Excel Export

※ Vulnerability 메뉴는 조치 상태 분석 화면이 아니라 취약점 데이터·영향 범위 검색 화면입니다.

Vulnerability

Vulnerability ID | Exact Match | Source | libTomMath | Exact Match

	Vulnerability ID	Source	Component(name)	Affected versions	Severity(score)
1	AZL-28639	OSV	Azure Linux:2:libtommath	[0, 1.1.0-5)	9.8 (CVSS_V3)
2	AZL-36959	OSV	Azure Linux:3:libtommath	[0, 1.1.0-5)	9.8 (CVSS_V3)
3	AZL-65547	OSV	Azure Linux:3:libtommath	[0, 1.3.1~rc1-3]	
4	CVE-2023-36328	NVD	libtom:libtommath	1.2.1)	9.8 (CVSS_V3)
5	CVE-2023-36328	OSV	https://github.com/libtom/libtommath	0.01,0.02,0.03,0.04,0.05,0.06,0.07,0.08,0.09,0.10,0.11,0.12,0.13,0.1…	9.8 (CVSS_V3)
6	CVE-2025-40913	OSV	https://github.com/libtom/libtommath	0.01,0.02,0.03,0.04,0.05,0.06,0.07,0.08,0.09,0.10,0.11,0.12,0.13,0.1…	6.5 (CVSS_V3)
7	CVE-2025-40914	OSV	https://github.com/dcit/perl-cryptx	v0.022,v0.023,v0.024,v0.025,v0.026,v0.029,v0.030,v0.031,v0.032,v…	9.8 (CVSS_V3)
8	DEBIAN-CVE-2023-36328	OSV	Debian:12:libtommath	[0, 1.2.0-6+deb12u1)	9.8 (CVSS_V3)
9	DEBIAN-CVE-2023-36328	OSV	Debian:13:libtommath	[0, 1.2.1-1)	9.8 (CVSS_V3)
1…	DEBIAN-CVE-2023-36328	OSV	Debian:14:libtommath	[0, 1.2.1-1)	9.8 (CVSS_V3)

LG Electronics Open Source Program Office

기대 효과와 확인 메뉴

OSS 취약점 커버리지 확대	OSV DB 추가 및 패키지 생태계별 Advisory·영향 범위 보완	Project > Identification > SBOM Open Source > Information > Vulnerability Vulnerability
CVE가 없는 취약점 식별	OSV 고유 Vulnerability ID	Open Source > Information > Vulnerability Vulnerability
취약점 출처 및 상세 정보 추적	Source(NVD,OSV) 구분 및 원문 링크 확인	Open Source > Information > Vulnerability Vulnerability
조치 대상 및 해결 상태 관리	CVSS 기준 조치 대상과 Need to resolve 상태 확인	Project > Security
SBOM 기반 프로젝트 취약점 관리	SBOM 컴포넌트와 프로젝트 취약점·조치 상태 연계	Project > Identification > SBOM Project > Security

향후 지원 예정: VEX

탐지 결과에 해결 상태를 연결하여 대응 현황 관리 범위를 확장

VEX란?

- Vulnerability Exploitability eXchange의 약자로,특정 제품 또는 구성에 알려진 취약점이 실제로 영향을 주는지 여부를 표현하는 보안 정보

왜 필요한가?

- NVD·OSV에서 확인된 취약점에 해결 상태를 연결하여 조치 현황을 명확하게 관리

FOSSLight Hub 방향

- Vulnerability Resolution을 기반으로 취약점 해결 상태를 VEX 정보로 제공 예정