Portal System
for Open Source Software

KossWise
with Black Duck

- 오픈소스 거버넌스 체계
- SBOM 생성 및 리포트
- 오픈소스 취약점 점검 내역
- 오픈소스 라이선스 식별 내역
- 오픈소스 공식 점검/승인
- 오픈소스 사용 계획 검토/승인
- 프로젝트 자가 검증/식별
- 컴포넌트/보안취약점 검색
- Repository 연동 및 점검
- 취약점 Notification

KMS Technology

KossWise 주요 기능

오픈소스 관리 프로세스

OSS 사용 계획 검토 부터 SBOM 승인, 프로젝트 배포 등 전체 과정을 모니터링 하고 관리

프로젝트 자가 검증

공식 점검 前, 소스코드 직접 스캔, OSS의 BOM 내역 확인, 조치 가이드 참고 및 조치 수행

OSS 사용 계획

자가 검증 後, 프로젝트에 사용할 OSS 내역을 계획하여 작성, 검토자에게 제출 및 승인을 득함

프로젝트 공식 점검

OSS 사용 계획 승인 後, 프로젝트 전체 소스코드를 등록 스캔하여 점검 담당자에게 공식 점검 요청을 진행

VCS/Repository 연동, 점검

VCS/Repository 연동 지원. OSS 반입 前 자동 점검, 반입 승인 및 OSS 내역 확인

프로젝트 점검 내역 확인

OSS 보안취약점 및 라이선스 현황 식별, 조치 가이드 및 점검자 의견 확인, SBOM 보고서 제공

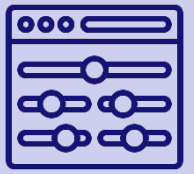
SBOM 제공, TTA 표준 리포팅

SBOM(SPDX, CycloneDX) 조회 및 다운로드, TTA 표준 규격을 준수한 변환 리포트 제공(리포트 커스터마이징 지원)

OSS 및 보안취약점 정보 검색

전체 프로젝트 내 사용중인 OSS 검색, NVD 및 블랙덕 자체 보유 DB를 통한 OSS/취약점 정보 검색 지원

커스터마이징 지원

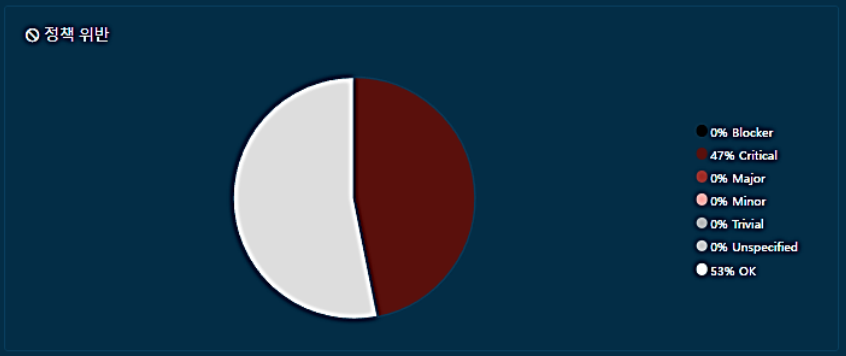


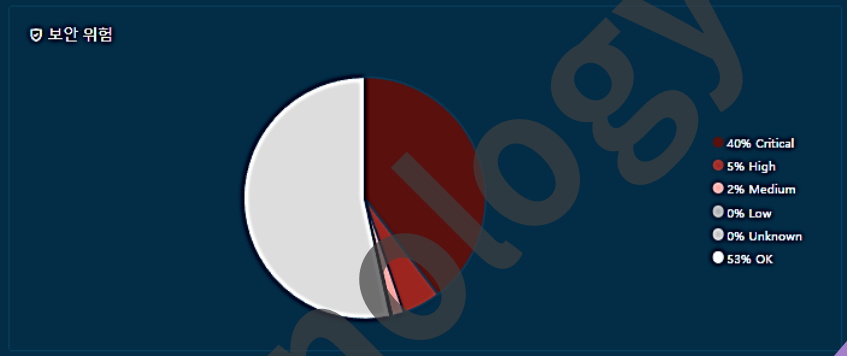
SSO, Email, SMS/메신저, 인사정보, SR System 등과 연동을 위한 커스터마이징 지원

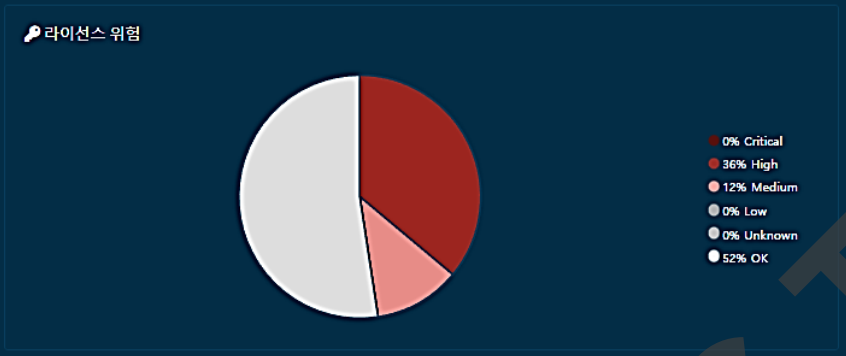
Open Source Software Governance

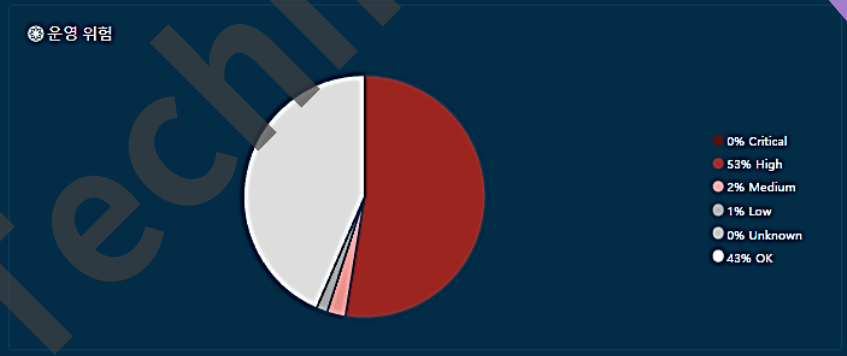
프로젝트 담당자와 OSS 검토자 간 협업	Team	담당자 정보, 역할 및 권한 관리 및 통제
OSS 라이선스 정책 설정 및 점검	Policy	OSS 보안취약점 등급 별 위험 식별
OSS 사용 계획, 점검, 조치, 승인, 배포	Process	OSS Repository, CI/CD, Git …
소스코드 스캔, Dependency 분석	Tool	SBOM 생성, TTA 표준 리포팅, 고지문 …

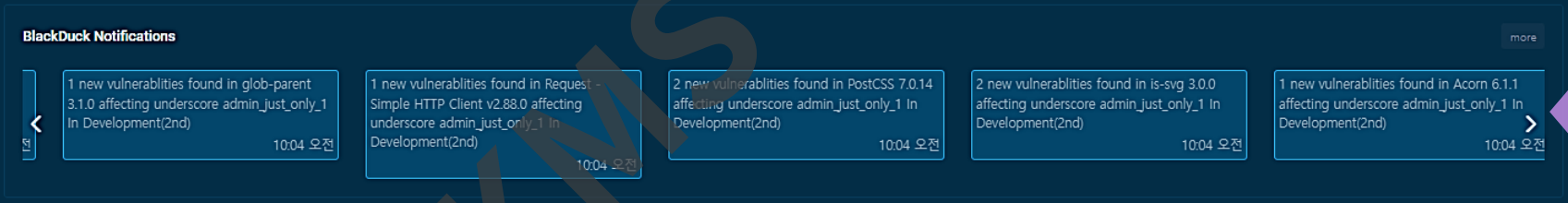
DashBoard (1/2)











전체 프로젝트의 '정책위반/보안위험/라이선스위험/운영위험 ' 정보 집계

실시간 업데이트 되는 취약점 Notification

- 최신 취약점 식별 정보
- 등록된 프로젝트 내 실시간 식별된 취약점 정보 포함

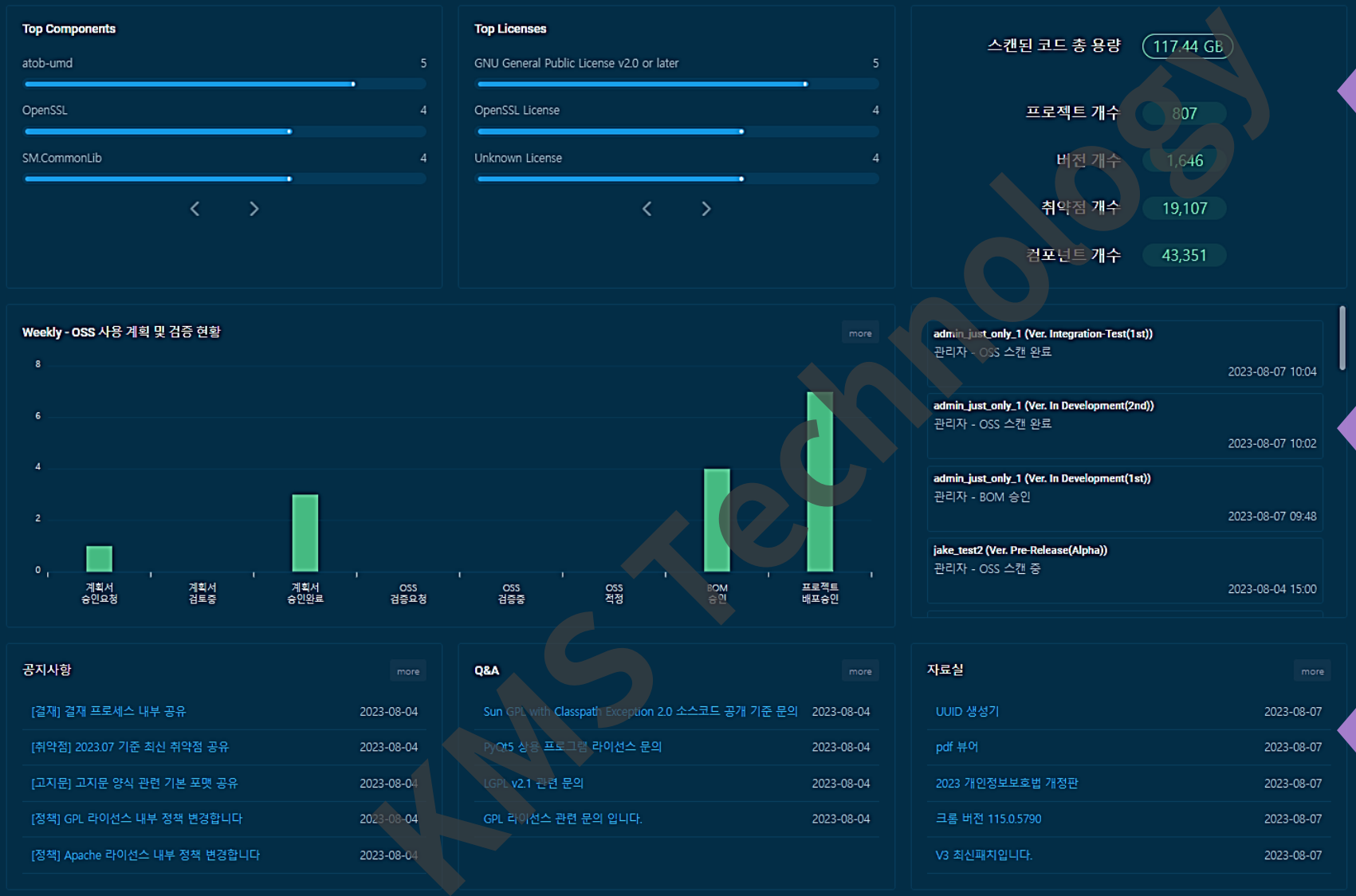
DashBoard (2/2)

Top Components
Top Licenses

OSS 사용 계획 및 공식 검증 상태 별 현황

작업 이력 이벤트 Log

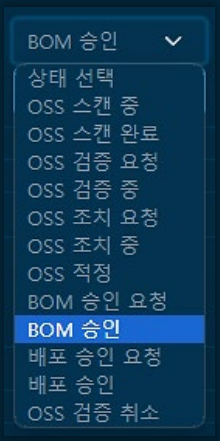
공지사항/Q&A/자료실



공식 프로젝트 스캔 내역 조회

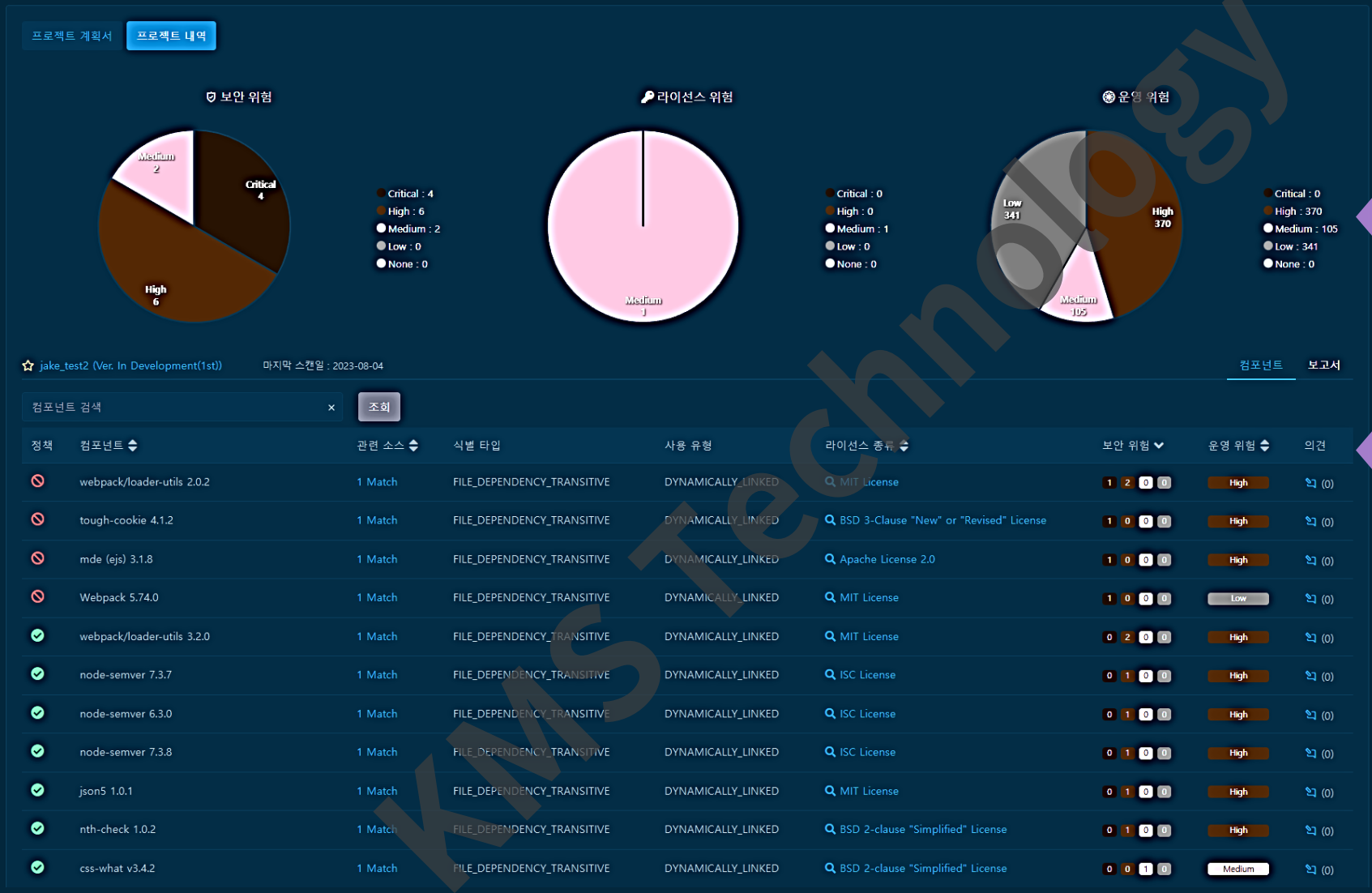
프로젝트 점검 상태 별 정렬 탭

프로젝트 내 식별된 위험 표출, 상태 변경 옵션



프로젝트 상태 변경 옵션

프로젝트 스캔 후, BOM 확인

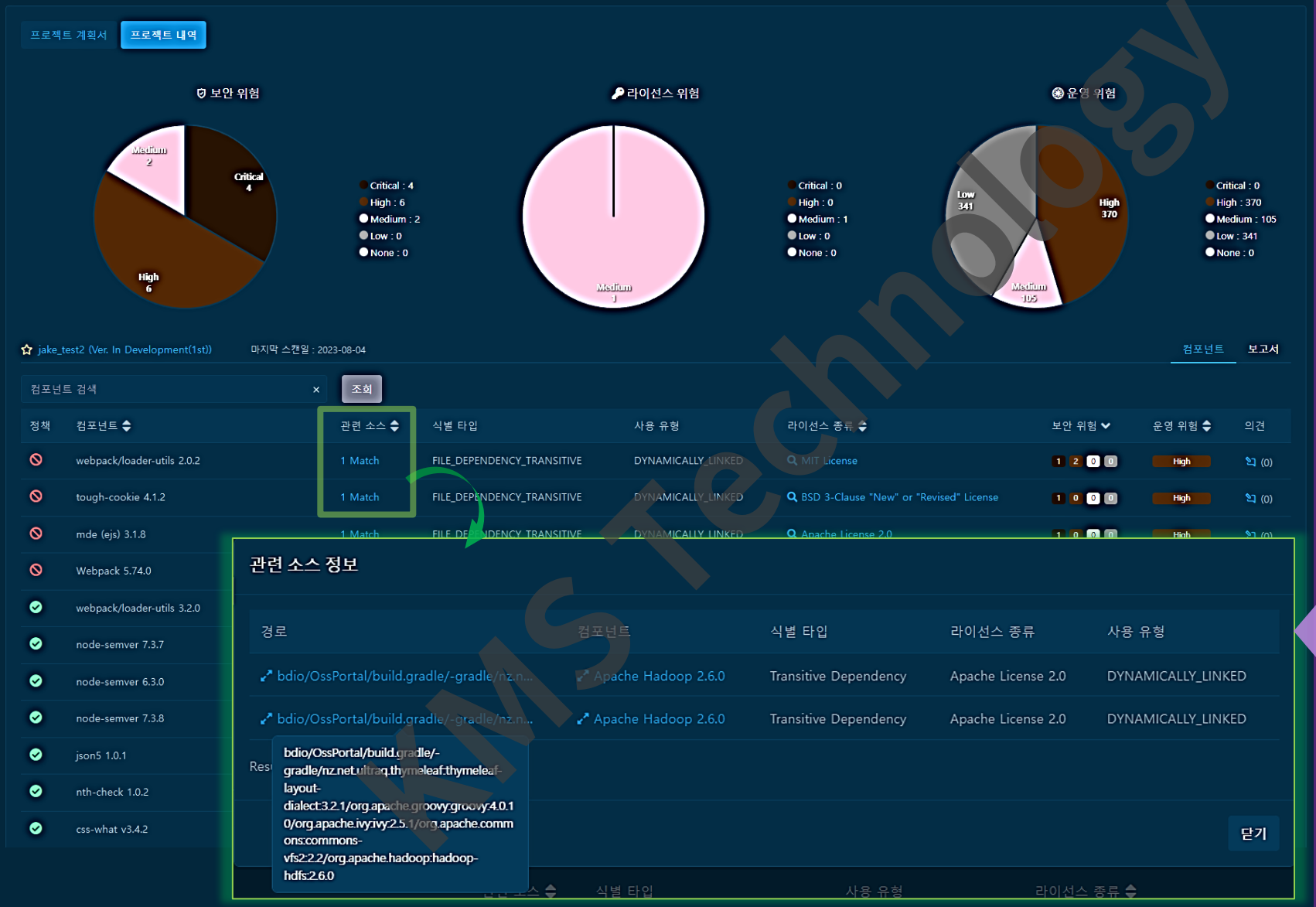


식별된 전체 컴포넌트의 '보안위험/라이선스위험/ 운영위험/ 정보 집계

식별된 전체 컴포넌트의 BOM 내역 확인

- 정책 위반 여부
- 컴포넌트 명칭
- 검출된 관련 소스
- 식별 타입
- 사용 유형
- 라이선스 종류
- 보안위험
- 운영위험
- 검토자 코멘트

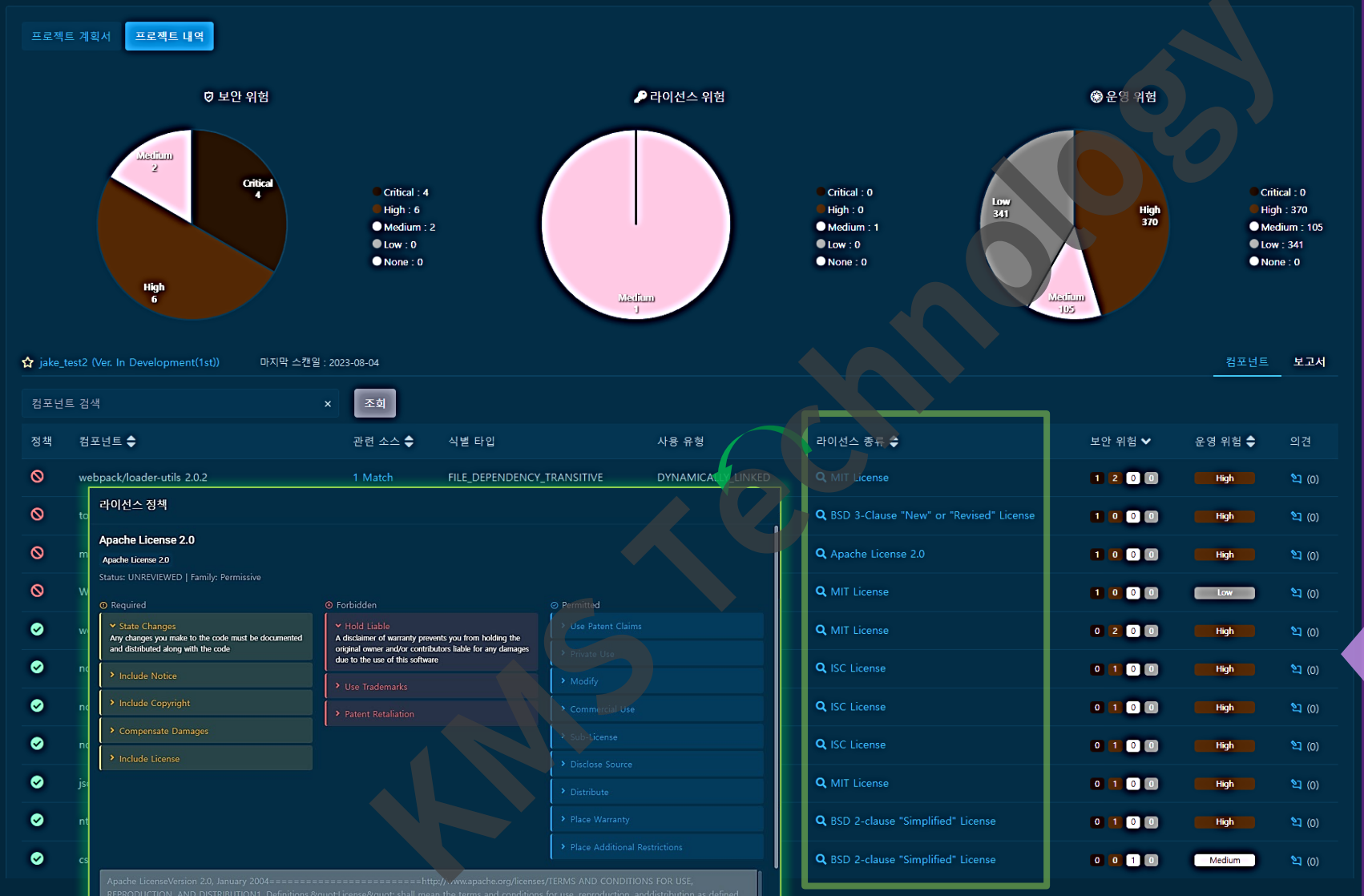
식별 된
관련 소스 정보



식별된 컴포넌트의
관련 소스 위치 정보

- 발견된 전체 파일 경로
- 컴포넌트 명칭
- 식별된 타입 정보
- 라이선스 종류
- 사용 유형 정보

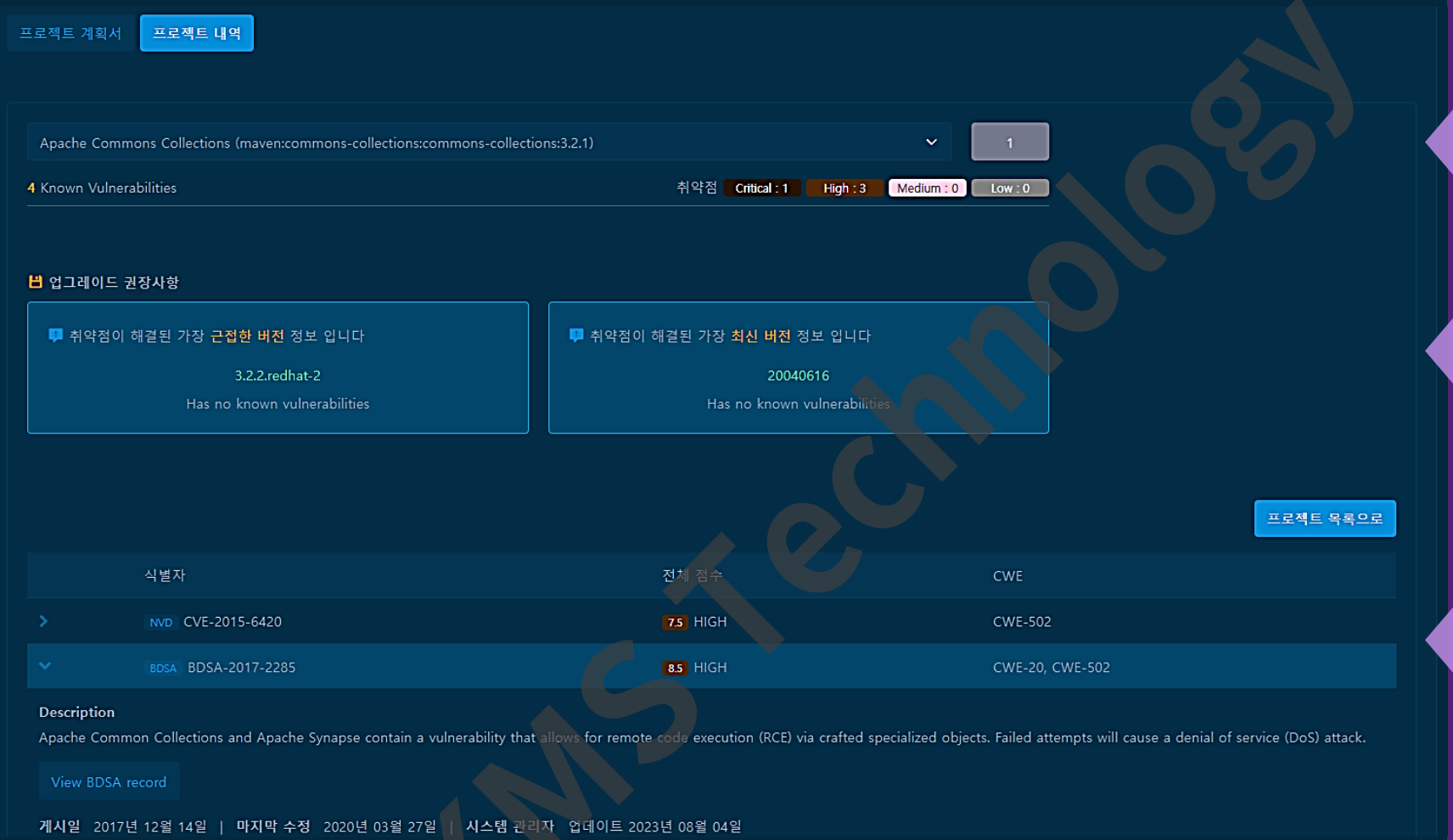
컴포넌트의 라이선스 정책



식별된 컴포넌트의 라이선스 정책 정보

- 필수/금지/허용 정책
- 라이선스 Copyright

컴포넌트의 보안 권고 정보



해당 컴포넌트의 Origin 목록 확인

대체 가능한 패치 정보 제공

CVE, CWE 정보, 권고 가이드

컴포넌트의 보안 권고 정보

프로젝트 계획서 | 프로젝트 내역

Apache Commons Collections (maven:commons-collections:commons-collections:

4 Known Vulnerabilities

업그레이드 권장사항

취약점이 해결된 가장 근접한 버전 정보 입니다

3.2.2.redhat-2

Has no known vulnerabilities

식별자	
NVD	CVE-2015-6420
BDSA	BDSA-2017-2285

Description

Apache Common Collections and Apache Synapse contain a vulnerability that allo

View BDSA record

게시일 2017년 12월 14일 | 마지막 수정 2020년 03월 27일 | 시스템 관리자

Black Duck Security Advisory

Apache Synapse and Apache Commons Collection Vulnerable to Remote Code Execution (RCE) During Object De-serialization

게시일: 2017-12-14 | 업데이트: 2020-03-27

- **Description**

Apache Common Collections and Apache Synapse contain a vulnerability that allows for remote code execution (RCE) via crafted specialized objects. Failed attempts will cause a denial of service (DoS) attack.

- **How to fit it**

Fix Available

Fixed in Apache Synapse version 3.0.1 by this commit.

Fixed in In Apache Commons Collections version 3.2.2 by this commit and this commit.

Fixed in In Apache Commons Collections 4.1-r1 by the following commits:

- Commit 1
- Commit 2
- Commit 3
- Commit 4
- Commit 5

The latest stable release are available here.

No Workaround

- **Scores**

CVSS v3.x

BDSA-2017-2285

Overall	8.5	HIGH
Overall(Temporal)	8.5	
Base	9.8	
Exploitability	3.9	
Impact	5.9	

CVSS v2

BDSA-2017-2285

Overall	8.5	HIGH
Overall(Temporal)	8.5	
Base	7.5	
Exploitability	10	
Impact	6.4	

닫기

How to fix it
Workaround

CVSS v3.xx

CVSS v2.x

SBOM & 변환 리포트 생성/다운로드

보고서

프로젝트 > 프로젝트 내역

프로젝트 계획서 | 프로젝트 내역

choi_test_1 (Ver. Pre-Release(Alpha)) 마지막 스캔일 : 2023-08-03

컴포넌트 | 보고서

보고서 생성하기 | 목록 다시 조회

OSS 컴플라이언스 보고서

OSS 컴플라이언스 보고서 파일	BD 원본 파일명	BD 파일 형식	보고서 타입	BD 마지막 생성일	BD 상태
choi_test_1-Pre-Release(Alpha)-202308080959.xlsx 완료	choi_test_1-Pre-Release(Alpha)_2023-08-08_095756.zip	CSV	VERSION	2023-08-08T00:57:56.359Z	완료

OSS 컴플라이언스 보고서 변환 생성 파일

Notices / SBOM / Vulnerability

BD 원본 파일명	BD 파일 형식	보고서 타입	BD 마지막 생성일	BD 상태
choi_test_1-Pre-Release(Alpha)_CYCLONEDX_14_2023-08-08_095904.zip	JSON	SBOM	2023-08-08T00:59:04.591Z	완료
vulnerability-update-report-choi_test_1-Pre-Release(Alpha)_2023-08-08_095...	CSV	VERSION_VULNERABILITY_UPDATE	2023-08-08T00:57:56.989Z	완료
vulnerability-status-report-choi_test_1-Pre-Release(Alpha)_2023-08-08_0957...	CSV	VERSION_VULNERABILITY_STATUS	2023-08-08T00:57:56.867Z	완료
vulnerability-remediation-report-choi_test_1-Pre-Release(Alpha)_2023-08-08...	CSV	VERSION_VULNERABILITY_REMEDIATION	2023-08-08T00:57:56.516Z	완료
choi_test_1-Pre-Release(Alpha)_2023-08-08_095756.zip	JSON	VERSION_LICENSE	2023-08-08T00:57:56.142Z	완료
choi_test_1-Pre-Release(Alpha)_SPDX_22_2023-08-08_095756.zip	JSON	SBOM	2023-08-08T00:57:56.141Z	완료

Notices, SBOM, Vulnerability

사용중인 컴포넌트 검색

검색된 컴포넌트 정보
위험 정보 확인

검색된 컴포넌트가
사용된 프로젝트 목록

보안취약점 DB 검색

사용중인 컴포넌트 | **보안 취약점 DB 검색** | 오픈소스 컴포넌트 검색 | BD Notifications | 컴포넌트 정책 보기

CVE-2021-44228 × 조회

※ 검색어 예시) CVE-2019-6592

식별자	전체 점수	게시일	마지막 갱신일	CWE
BDSA BDSA-2021-3731	9.4 CRITICAL	2021-12-10	2023-01-20	CWE-502
NVD CVE-2021-44228	10 CRITICAL	2021-12-10	2023-04-04	CWE-400, CWE-502, CWE-20, CWE-917
NVD CVE-2022-23848	9.8 CRITICAL	2022-02-21	2022-03-01	
NVD CVE-2021-4125	8.1 HIGH	2022-08-25	2023-03-29	CWE-400, CWE-502, CWE-20
NVD CVE-2022-33915	7 HIGH	2022-06-17	2022-07-06	
NVD CVE-2021-4104	7.5 HIGH	2021-12-14	2022-10-06	
NVD CVE-2021-45046	9 CRITICAL	2021-12-15	2023-06-27	
BDSA BDSA-2021-3779	7.5 HIGH	2021-12-15	2023-08-07	

Black Duck Security Advisory

Apache Log4j Vulnerable to Remote Code Execution (RCE) Through LDAP Access via JNDI and Specially Crafted Log Messages

게시일: 2021-12-10 | 업데이트: 2023-01-20

- Description

Apache Log4j, as used in many popular services, is vulnerable to improperly allowing lightweight directory access protocol (LDAP) access via Java naming and directory interface (JNDI). A remote attacker able to supply the end application with specially crafted input that is then processed by the Log4j subcomponent could cause the execution of arbitrary Java code. **Note** - log4j-api packages by themselves do not contain the vulnerable functionality and are therefore unaffected. log4j-core packages and the upstream overarching source repository are affected. - A previously suggested mitigation of setting environment variable `LOG4J_FORMAT_MSG_NO_LOOKUPS=true` is not recommended. This mitigation has been proven inadequate against this vulnerability. - This vulnerability is partially fixed in [**2.15.0-rc2**](https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2) by [this](https://github.com/apache/logging-log4j2/commit/001aaada7dab82c3c09cde5f8e14245dc9d8b454) commit and [this](https://github.com/apache/logging-log4j2/commit/bac0d8a35c7e354a0d3f706569116dff6c6bd658) commit. These fixes were deemed incomplete. See BDSA-2021-3779 (CVE-2021-45046) for more details. This vulnerability is listed as exploitable by the Cybersecurity & Infrastructure Security Agency in their [Known Exploited Vulnerabilities Catalog](https://www.cisa.gov/known-exploited-vulnerabilities-catalog).

- How to fix it

Fix Available

Fixed in versions:

- **2.16.0-rc1** by this commit.
- **2.12.2-rc1** by this commit and this commit.
- **2.3.1-rc1** by this commit and this commit.

The latest releases can be found here.

NOTE: It is recommended to upgrade to version **2.17.0**. This recommendation is due to related vulnerabilities (BDSA-2021-3779, CVE-2021-45046) affecting the version that this vulnerability is fixed in.

Workaround

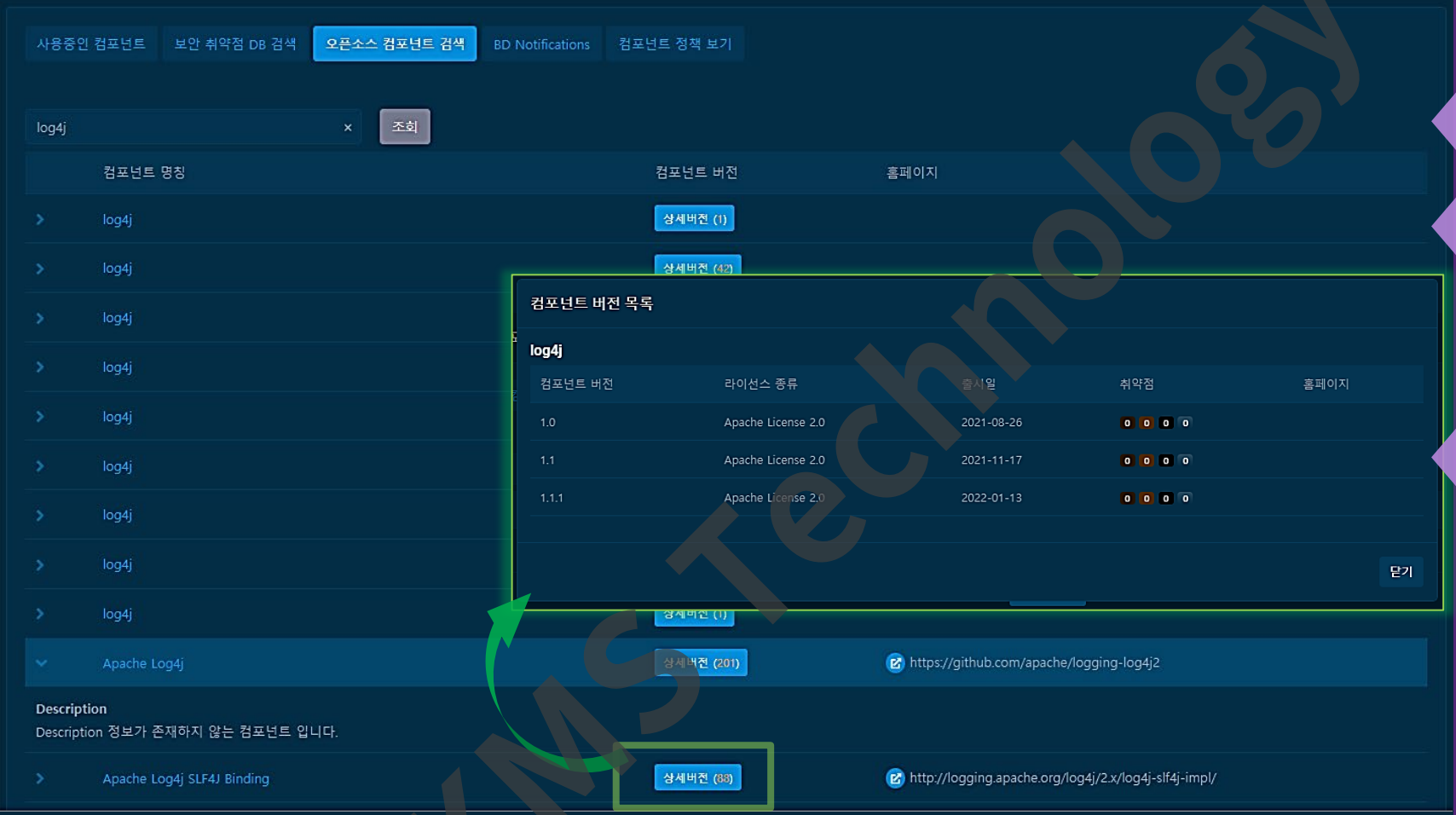
The vendor states that: > This issue can be mitigated in prior releases (<**2.16.0**) by removing

CVE 코드 검색어 입력

NVD/BDSA에서 검색된 취약점 정보 확인

보안 권고 사항 확인

오픈소스 컴포넌트 검색

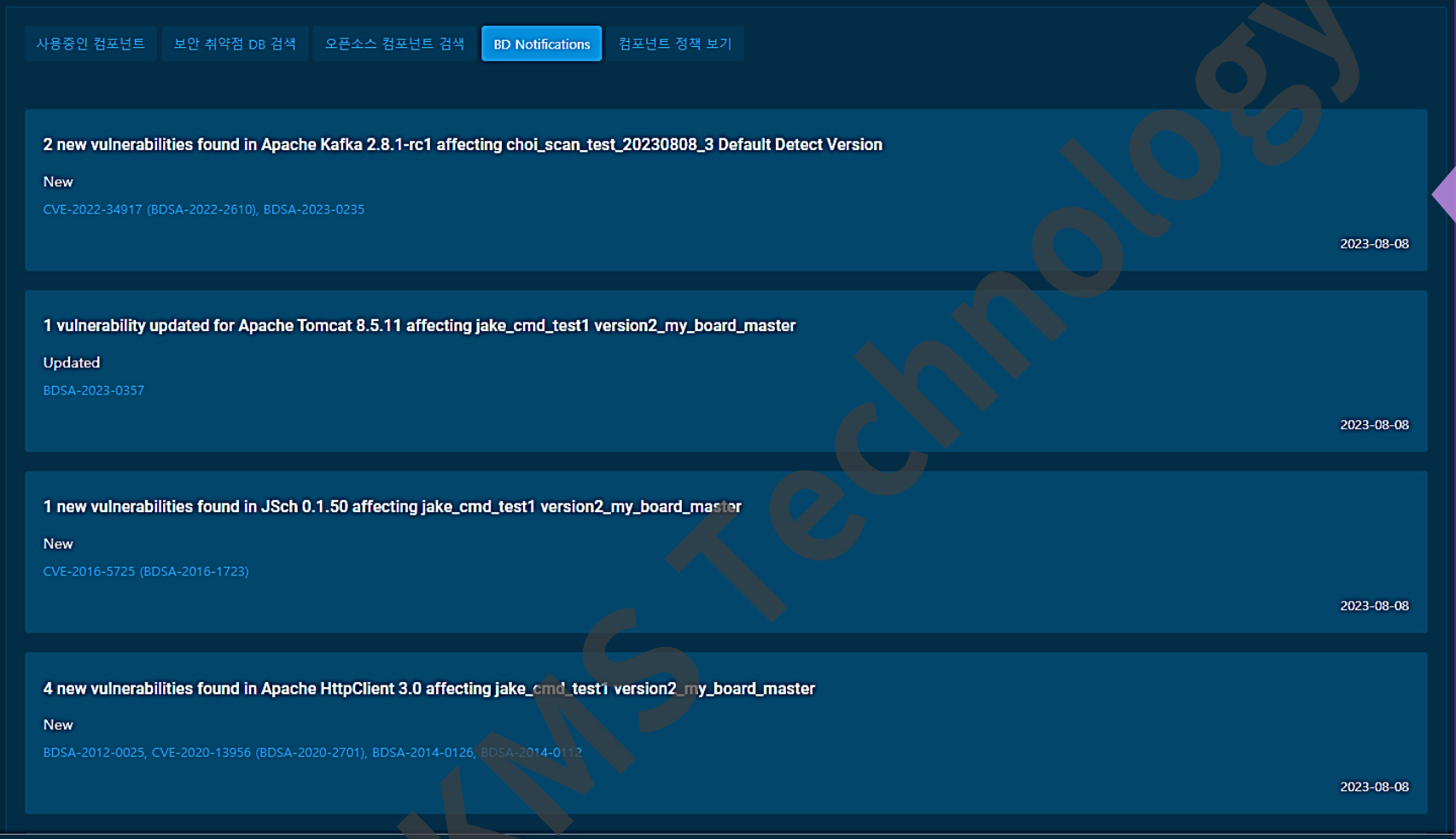


컴포넌트 명칭 입력

검색된 컴포넌트 목록,
상세 버전 개수 표출

검색된 컴포넌트의
상세 버전 목록

실시간 취약점 Notifications



취약점 관련 Notification 내용

<옵션>

- POLICY_OVERRIDE
- RULE_VIOLATION
- VULNERABILITY
- LICENSE_LIMIT
- RULE_VIOLATION_CLEARED
- PROJECT
- PROJECT_VERSION
- BOM_EDIT
- VERSION_BOM_CODE_LOCATION_BOM_COMPUTED
- COMPONENT_UNKNOWN_VERSION

오픈소스 사용 현황 통계

Top Components

Top Licenses

공식 프로젝트 현황 통계

2023-07-08 ~ 2023-08-08 ○ 1주 ◉ 1개월 ○ 1년 조회

프로젝트 계획서 현황
프로젝트 소스 검증 현황

계획서 상태

계획서 작성(임시저장)	0
계획서 승인요청	1
계획서 검토중	0
계획서 조치요령	0
계획서 조치중	0
계획서 승인완료	4

컴포넌트 검증 상태

스캔완료	5
검증요청	0
검증중	0
조치요령	0
조치중	0
적정	0
BOM 승인요청	0
BOM 승인	6
배포 승인요청	0
배포 승인	7

Contact

솔루션 문의하기

KMS 테크놀로지

www.kmstech.co.kr/Contact

솔루션 구축 실적

KMS 테크놀로지

www.kmstech.co.kr/business_report

홈 페 이 지	www.kmstech.co.kr
연 락 처	02-6925-0803
문 의	info@kmstech.co.kr

KMS Technology