

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

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



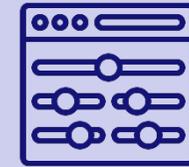
SBOM(SPDX, CycloneDX) 조회 및 다운로드, TTA 표준 규격을 준수한 변환 리포트 제공(리포트 커스터마이징 지원)

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

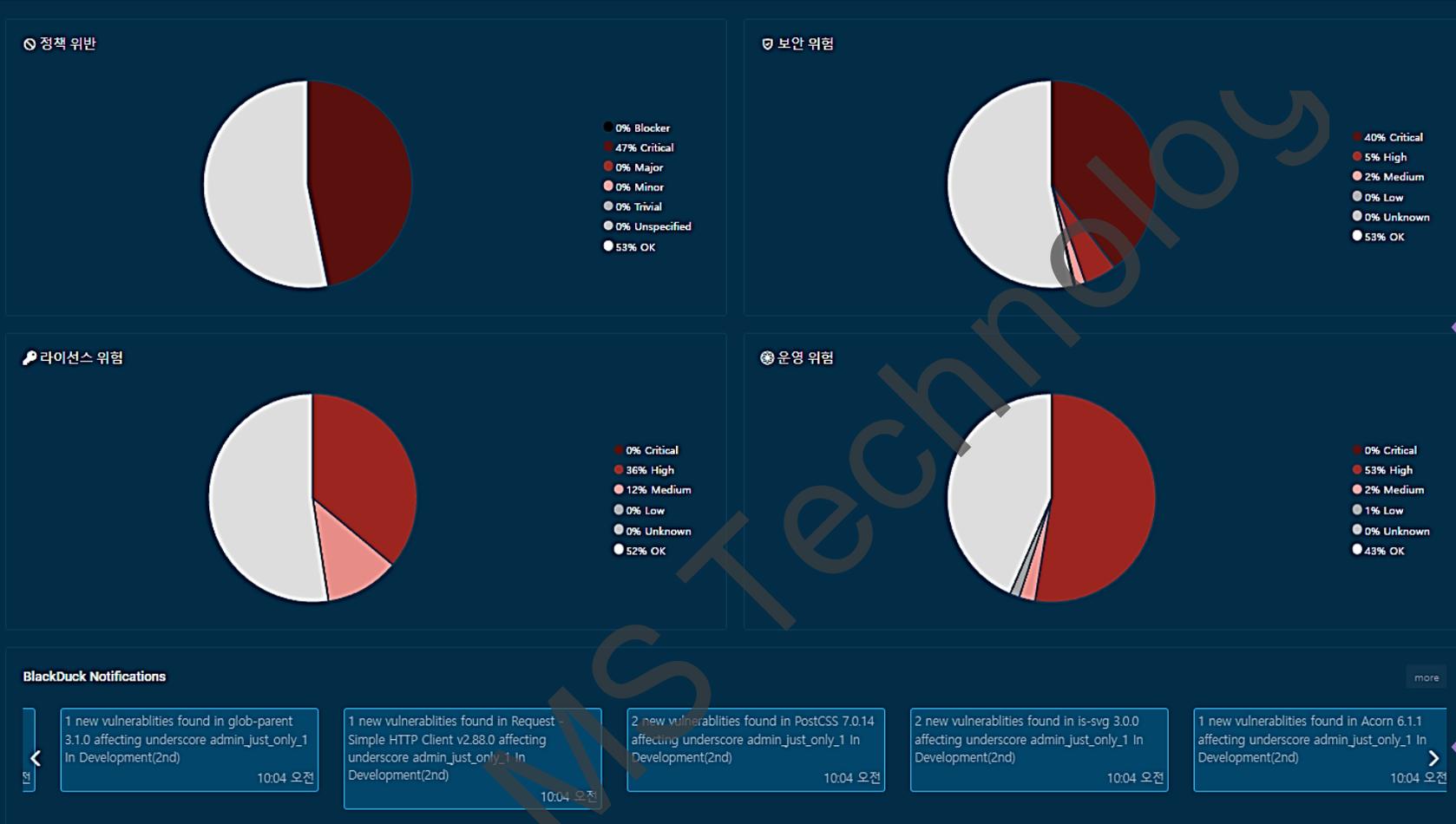
OSS Repository, CI/CD, Git ...

소스코드 스캔, Dependency 분석

Tool

SBOM 생성, TTA 표준 리포팅, 고지문 ...

DashBoard (1/2)

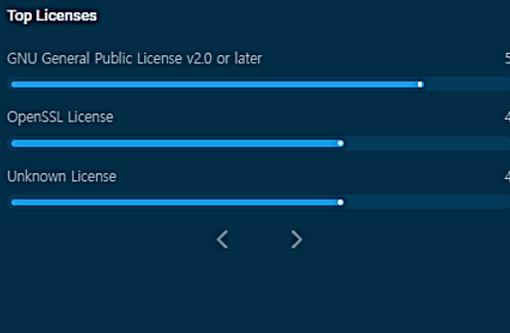


전체 프로젝트의 '정책위반/보안위험/라이선스위험/운영위험' 정보 집계

실시간 업데이트 되는 취약점 Notification

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

DashBoard (2/2)



스캔된 코드 총 용량 **117.44 GB**

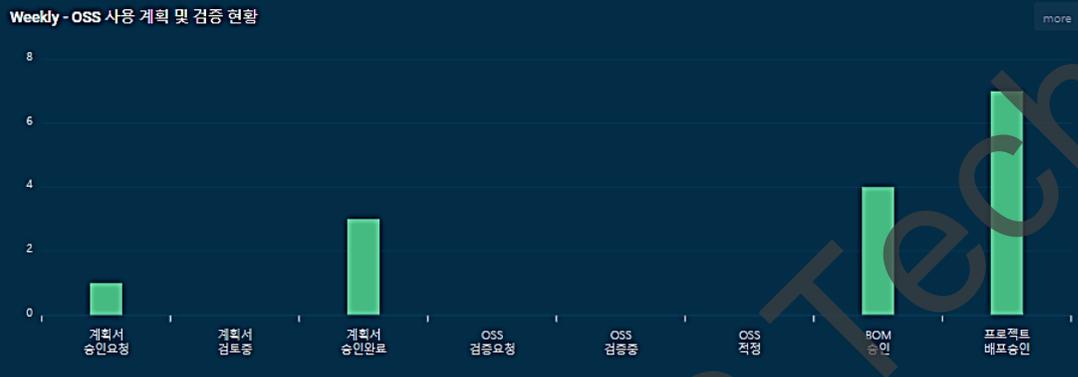
프로젝트 개수 **807**

버전 개수 **1,646**

취약점 개수 **19,107**

컴포넌트 개수 **43,351**

Top Components
Top Licenses



OSS 사용 계획 및 공식 검증 상태 별 현황

admin_just_only_1 (Ver. Integration-Test(1st)) 관리자 - OSS 스캔 완료	2023-08-07 10:04
admin_just_only_1 (Ver. In Development(2nd)) 관리자 - OSS 스캔 완료	2023-08-07 10:02
admin_just_only_1 (Ver. In Development(1st)) 관리자 - BOM 승인	2023-08-07 09:48
jake_test2 (Ver. Pre-Release(Alpha)) 관리자 - OSS 스캔 중	2023-08-04 15:00

OSS 사용 계획 및 공식
검증 상태 별 현황

작업 이력 이벤트 Log

공지사항

[결재] 결재 프로세스 내부 공유	2023-08-04
[취약점] 2023.07 기준 최신 취약점 공유	2023-08-04
[고지문] 고지문 양식 관련 기본 포맷 공유	2023-08-04
[정책] GPL 라이선스 내부 정책 변경합니다	2023-08-04
[정책] Apache 라이선스 내부 정책 변경합니다	2023-08-04

Q&A

Sun GPL with Classpath Exception 2.0 소스코드 공개 기준 문의	2023-08-04
PyQt5 상용 프로그램 라이선스 문의	2023-08-04
GPL v2.1 관련 문의	2023-08-04
GPL 라이선스 관련 문의입니다.	2023-08-04

자료실

UUID 생성기	2023-08-07
pdf 뷰어	2023-08-07
2023 개인정보보호법 개정판	2023-08-07
크롬 버전 115.0.5790	2023-08-07
V3 최신패치입니다.	2023-08-07

공지사항/O&A/자료실

공식 프로젝트 스캔 내역 조회

프로젝트 계획서 **프로젝트 내역** + 프로젝트 등록

★ 북마크 (0) 전체 (17) OSS 스캔 완료 (0) OSS 검증 요청 (0) OSS 검증 중 (0) OSS 조치 요청 (0) OSS 조치 중 (0) OSS 적정 (0) BOM 승인 요청 (0) BOM 승인 (3) 배포 승인 요청 (0) 배포 승인 (7) OSS 검증 취소 (1)

선택 키워드 입력 2023-07-28 ~ 2023-08-04 1주 1개월 1년 조회 프로젝트명

<p>☆ admin_just_only_1 (Ver. In Planning)</p> <p>정책 위반 0 0 0 보안 위험 0 0 0 라이선스 위험 0 0 0 운영 위험 3 0 0</p> <p>BD Group: 8e509884-1091-4e46-b159-d3f177b16081 마지막 스캔일: 2023-08-04 마지막 경신일: 2023-08-04</p> <p>담당자: 관리자(개발부서) 등록일: 2023-08-04</p>	<p>배포 승인</p> <p>배포 승인</p> <p>적용</p>
<p>☆ choi_test_1 (Ver. Integration-Test(1st))</p> <p>정책 위반 0 0 0 보안 위험 0 0 0 라이선스 위험 0 0 0 운영 위험 3 0 0</p> <p>BD Group: 8e509884-1091-4e46-b159-d3f177b16081 마지막 스캔일: 2023-08-03 마지막 경신일: 2023-08-04</p> <p>담당자: choi(개발부) 등록일: 2023-08-03</p>	<p>BOM 승인</p> <p>BOM 승인</p> <p>적용</p>
<p>☆ choi_test_1 (Ver. Integration-Test(2nd))</p> <p>정책 위반 0 0 0 보안 위험 0 0 0 라이선스 위험 0 0 0 운영 위험 0 0 0</p> <p>BD Group: 8e509884-1091-4e46-b159-d3f177b16081 마지막 스캔일: 2023-08-03 마지막 경신일: 2023-08-03</p> <p>담당자: choi(개발부) 등록일: 2023-08-03</p>	<p>스캔 오류</p> <p>로그 다운로드</p>

프로젝트 점검 상태 별 정렬 탭

프로젝트 내 식별된 위험 표출, 상태 변경 옵션

<p>정책 위반 25 0 0</p>	<p>보안 위험 25 38 17</p>
<p>라이선스 위험 0 0 0</p>	<p>운영 위험 1 0 0</p>

- BOM 승인
- 상태 선택
- OSS 스캔 중
- OSS 스캔 완료
- OSS 검증 요청
- OSS 검증 중
- OSS 조치 요청
- OSS 조치 중
- OSS 적정
- BOM 승인 요청
- BOM 승인**
- 배포 승인 요청
- 배포 승인
- OSS 검증 취소

프로젝트 상태 변경 옵션

프로젝트 스캔 후, BOM 확인



식별된 전체 컴포넌트의 '보안위험/라이선스위험/운영위험/ 정보 집계

☆ jake_test2 (Ver. In Development(1st)) 마지막 스캔일 : 2023-08-04 [컴포넌트](#) [보고서](#)

컴포넌트 검색

정책	컴포넌트	관련 소스	식별 타입	사용 유형	라이선스 종류	보안 위험	운영 위험	의견
🚫	webpack/loader-utils 2.0.2	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	🔍 MIT License	1 2 0 0	High	👤 (0)
🚫	tough-cookie 4.1.2	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	🔍 BSD 3-Clause "New" or "Revised" License	1 0 0 0	High	👤 (0)
🚫	mde (ejs) 3.1.8	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	🔍 Apache License 2.0	1 0 0 0	High	👤 (0)
🚫	Webpack 5.74.0	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	🔍 MIT License	1 0 0 0	Low	👤 (0)
✅	webpack/loader-utils 3.2.0	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	🔍 MIT License	0 2 0 0	High	👤 (0)
✅	node-semver 7.3.7	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	🔍 ISC License	0 1 0 0	High	👤 (0)
✅	node-semver 6.3.0	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	🔍 ISC License	0 1 0 0	High	👤 (0)
✅	node-semver 7.3.8	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	🔍 ISC License	0 1 0 0	High	👤 (0)
✅	json5 1.0.1	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	🔍 MIT License	0 1 0 0	High	👤 (0)
✅	nth-check 1.0.2	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	🔍 BSD 2-clause "Simplified" License	0 1 0 0	High	👤 (0)
✅	css-what v3.4.2	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	🔍 BSD 2-clause "Simplified" License	0 0 1 0	Medium	👤 (0)

식별된 전체 컴포넌트의 BOM 내역 확인

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

식별된 관련 소스 정보

프로젝트 계획서 | 프로젝트 내역

보안 위험

Critical : 4
High : 6
Medium : 2
Low : 0
None : 0

라이선스 위험

Critical : 0
High : 0
Medium : 1
Low : 0
None : 0

운영 위험

Critical : 0
High : 370
Medium : 105
Low : 341
None : 0

☆ jake_test2 (Ver. In Development(1st)) 마지막 스캔일 : 2023-08-04 컴포넌트 보고서

컴포넌트 검색 [x] [조회]

정책	컴포넌트	관련 소스	식별 타입	사용 유형	라이선스 종류	보안 위험	운영 위험	의견
🚫	webpack/loader-utils 2.0.2	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	MIT License	1 2 0 0	High	(0)
🚫	tough-cookie 4.1.2	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	BSD 3-Clause "New" or "Revised" License	1 0 0 0	High	(0)
🚫	mde (ejs) 3.1.8	1 Match	FILE_DEPENDENCY_TRANSITIVE	DYNAMICALLY_LINKED	Apache License 2.0	1 0 0 0	High	(0)
🚫	Webpack 5.74.0							
✅	webpack/loader-utils 3.2.0							
✅	node-semver 7.3.7							
✅	node-semver 6.3.0							
✅	node-semver 7.3.8							
✅	json5 1.0.1							
✅	nth-check 1.0.2							
✅	css-what v3.4.2							

관련 소스 정보

경로	컴포넌트	식별 타입	라이선스 종류	사용 유형
bdio/OssPortal/build.gradle/-gradle/nz.net.ultraq.thymeleaf.thymeleaf-layout-dialect:3.2.1/org.apache.groovy:groovy:4.0.10/org.apache.ivy:ivy:2.5.1/org.apache.commons:commons-ifs:2.2.2/org.apache.hadoop:hadoop-hdfs:2.6.0	Apache Hadoop 2.6.0	Transitive Dependency	Apache License 2.0	DYNAMICALLY_LINKED
bdio/OssPortal/build.gradle/-gradle/nz.net.ultraq.thymeleaf.thymeleaf-layout-dialect:3.2.1/org.apache.groovy:groovy:4.0.10/org.apache.ivy:ivy:2.5.1/org.apache.commons:commons-ifs:2.2.2/org.apache.hadoop:hadoop-hdfs:2.6.0	Apache Hadoop 2.6.0	Transitive Dependency	Apache License 2.0	DYNAMICALLY_LINKED

닫기

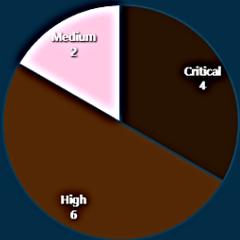
식별된 컴포넌트의
관련 소스 위치 정보

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

컴포넌트의 라이선스 정책

프로젝트 계획서 프로젝트 내역

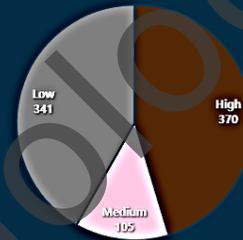
보안 위험



라이선스 위험



운영 위험



☆ jake_test2 (Ver. In Development(1st)) 마지막 스캔일 : 2023-08-04

컴포넌트 보고서

컴포넌트 검색 x 조회

정책 컴포넌트 관련 소스 식별 타입 사용 유형 라이선스 종류 보안 위험 운영 위험 의견

webpack/loader-utils 2.0.2 1 Match FILE_DEPENDENCY_TRANSITIVE DYNAMICALLY_LINKED

MIT License High (0)

라이선스 정책

BSD 3-Clause "New" or "Revised" License High (0)

Apache License 2.0

Apache License 2.0
Status: UNREVIEWED | Family: Permissive

Required	Forbidden	Permitted
<ul style="list-style-type: none"> State Changes: Any changes you make to the code must be documented and distributed along with the code Include Notice Include Copyright Compensate Damages Include License 	<ul style="list-style-type: none"> Hold Liabile: A disclaimer of warranty prevents you from holding the original owner and/or contributors liable for any damages due to the use of this software Use Trademarks Patent Retaliation 	<ul style="list-style-type: none"> Use Patent Claims Private Use Modify Commercial Use Sub-license Disclose Source Distribute Place Warranty Place Additional Restrictions

MIT License	1	2	0	0	High	(0)
BSD 3-Clause "New" or "Revised" License	1	0	0	0	High	(0)
Apache License 2.0	1	0	0	0	High	(0)
MIT License	1	0	0	0	Low	(0)
MIT License	0	2	0	0	High	(0)
ISC License	0	1	0	0	High	(0)
ISC License	0	1	0	0	High	(0)
ISC License	0	1	0	0	High	(0)
MIT License	0	1	0	0	High	(0)
BSD 2-clause "Simplified" License	0	1	0	0	High	(0)
BSD 2-clause "Simplified" License	0	0	1	0	Medium	(0)

식별된 컴포넌트의 라이선스 정책 정보

- 필수/금지/허용 정책
- 라이선스 Copyright

컴포넌트의 보안 권고 정보

프로젝트 계획서 프로젝트 내역

Apache Commons Collections (maven:commons-collections:commons-collections:3.2.1)

1

4 Known Vulnerabilities

취약점 Critical : 1 High : 3 Medium : 0 Low : 0

업그레이드 권장사항

취약점이 해결된 가장 **근접한 버전** 정보입니다

3.2.2.redhat-2

Has no known vulnerabilities

취약점이 해결된 가장 **최신 버전** 정보입니다

20040616

Has no known vulnerabilities

프로젝트 목록으로

식별자

전체 점수

CWE

> NVD CVE-2015-6420

7.5 HIGH

CWE-502

▼ BDSA BDSA-2017-2285

8.5 HIGH

CWE-20, CWE-502

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.

[View BDSA record](#)

게시일 2017년 12월 14일 | 마지막 수정 2020년 03월 27일 | 시스템 관리자 업데이트 2023년 08월 04일

해당 컴포넌트의
Origin 목록 확인

대체 가능한 패치 정보
제공

CVE, CWE 정보,
권고 가이드

컴포넌트의 보안 권고 정보

How to fix it
Workaround

CVSS v3.xx

CVSS v2.x

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

프로젝트 계획서

프로젝트 내역

Apache Commons Collections (maven:commons-collections:commons-collections:3.2.2)

4 Known Vulnerabilities

업그레이드 권장사항

취약점이 해결된 가장 **근접한 버전** 정보입니다

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 allows for remote code execution (RCE) via crafted specialized objects. Failed attempts will cause a denial of service (DoS) attack.

[View BDSA record](#)

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

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_0957... 	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

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

log4j x 조회 정렬

Apache Extras Companion for log4j 1.2. > 1.2.17 사용된 프로젝트: 2	보안 위험 0 0 0	라이선스 위험 0 0 0	운영 위험 2 0 0
Apache Log4j > 1.0.1 사용된 프로젝트: 1	보안 위험 1 2 1	라이선스 위험 0 0 0	운영 위험 1 0 0
Apache Log4j > 1.2.12 사용된 프로젝트: 12	보안 위험 3 4 1	라이선스 위험 0 0 0	운영 위험 12 0 0
Apache Log4j > 1.2.13 사용된 프로젝트: 1			
Apache Log4j > 1.2.14 사용된 프로젝트: 5			
Apache Log4j > 1.2.15 사용된 프로젝트: 2			
Apache Log4j > 1.2.16 사용된 프로젝트: 2			

사용중인 프로젝트

Apache Log4j

프로젝트 명칭

- BJ_AOSP_External - 1
- BJ_spring-boot - 2023-07
- HQ_Java_Test - daq_batch
- admin_only_test_1 - Self-Test
- mike_test_1 - In Development(1st)

닫기

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

×
조회

※ 검색어 예시) CVE-2019-6592

식별자	전체 점수	게시일	마지막 경신일	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	

CVE 코드 검색어 입력

NVD/BDSA에서 검색된 취약점 정보 확인

보안 권고 사항 확인

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/001aada7dab82c3c09cde3f8e14245dc9d8b454) 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 (&t**2.16.0**) by removing

[사용중인 컴포넌트](#)
[보안 취약점 DB 검색](#)
[오픈소스 컴포넌트 검색](#)
[BD Notifications](#)
[컴포넌트 정책 보기](#)

2 new vulnerabilities found in Apache Kafka 2.8.1-rc1 affecting choi_scan_test_20230808_3 Default Detect Version

New
 CVE-2022-34917 (BDSA-2022-2610), BDSA-2023-0235

2023-08-08

1 vulnerability updated for Apache Tomcat 8.5.11 affecting jake_cmd_test1 version2_my_board_master

Updated
 BDSA-2023-0357

2023-08-08

1 new vulnerabilities found in JSch 0.1.50 affecting jake_cmd_test1 version2_my_board_master

New
 CVE-2016-5725 (BDSA-2016-1723)

2023-08-08

4 new vulnerabilities found in Apache HttpClient 3.0 affecting jake_cmd_test1 version2_my_board_master

New
 BDSA-2012-0025, CVE-2020-13956 (BDSA-2020-2701), BDSA-2014-0126, BDSA-2014-0112

2023-08-08

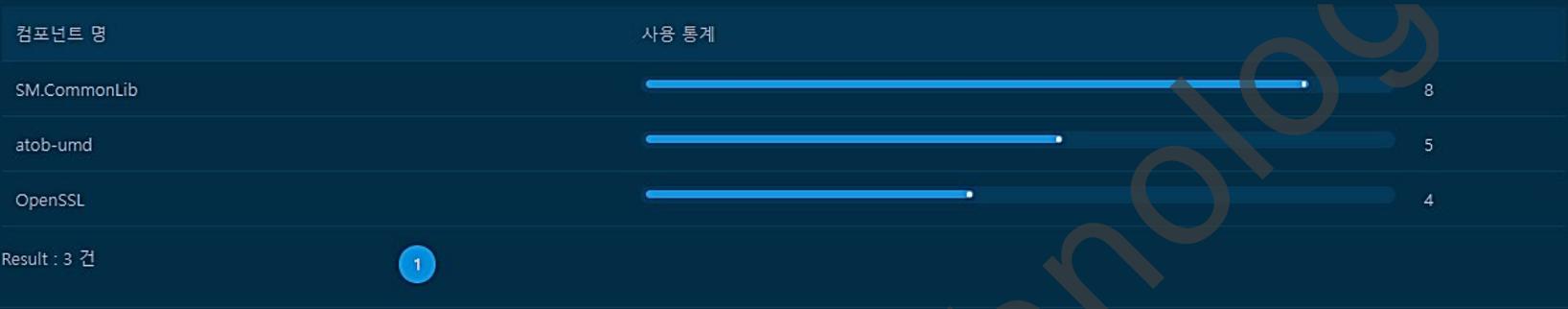
취약점 관련 Notification 내용

- <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

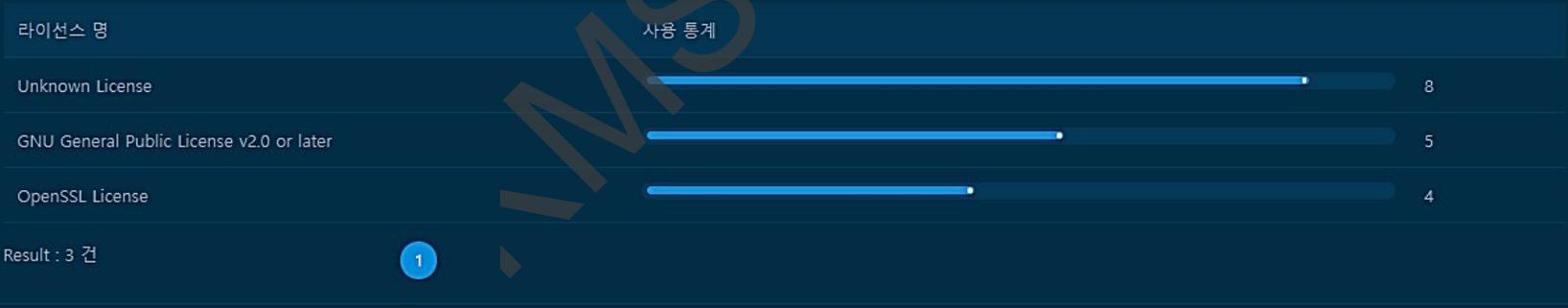
2023-08-01 ~ 2023-08-08 1주 1개월 1년 조회



Top Components

Top Components Top Licenses

2023-08-01 ~ 2023-08-08 1주 1개월 1년 조회



Top Licenses

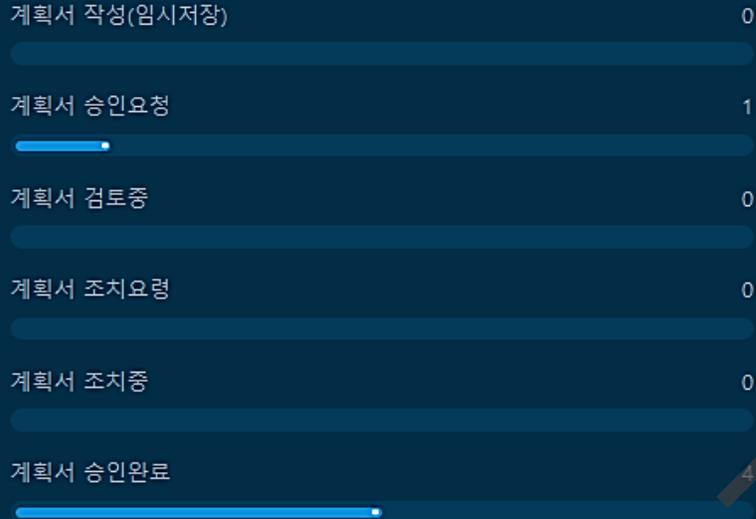
공식 프로젝트 현황 통계

2023-07-08 ~ 2023-08-08

1주 1개월 1년

조회

계획서 상태



컴포넌트 검증 상태



프로젝트 계획서 현황
프로젝트 소스 검증 현황

Contact

솔루션 문의하기



KMS 테크놀로지

www.kmstech.co.kr/Contact

솔루션 구축 실적



KMS 테크놀로지

www.kmstech.co.kr/business_report

홈 페이지 www.kmstech.co.kr

연락처 02-6925-0803

문의 info@kmstech.co.kr

KMS
Technology