

Labrador 솔루션 소개

2023

㈜ 레브라도랩스



01

오픈소스 사용 현황

소프트웨어 보안취약점 자동분석 시스템
AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

1.1 오픈소스 동향

“ 많은 기업들이 오픈소스를 활용하여 혁신적인 신기술·신개념 서비스 개발

오픈소스(Open Source)의 의미

■ 누구나 자유롭게 확인·수정·배포할 수 있는 프로그램 소스코드

- 목적에 맞는 오픈소스를 자유롭게 다운로드 받아 구현 가능
- 오픈소스 활용을 통해 개발 효율 극대화 & 신속한 대응 가능
- 글로벌 개발자 커뮤니티와의 문제 공유 통해 완성도 향상

■ 오픈소스 활용 사례



글로벌 기업의 오픈소스 활용·확대



* 소프트웨어정책연구소, “오픈소스 수익화의 확산-오픈소스 기반 수익화 구조”

1.2 오픈소스 사용 위험 현황

“ 오픈소스 적극 활용 추세에 따라 보안 취약점, 라이선스 리스크 확대

보안 위험 현황

- ✓ 2~4년 전 배포된 리눅스 커널 기반으로 최신 기기가 운영되며, 평균 200~300개의 취약점을 내포하고 있음 (LABRADOR LABS 자체조사결과)
- ✓ 알려진 취약점인 CVE가 14만개 이상 공개 되었으며, 매일 50개 이상의 새로운 취약점이 발견 (www.cvedetails.com)
- ✓ 전세계 금융거래의 50%이상이 오픈소스를 통해 처리되고 있으며, 전체 오픈소스 75%에 한 개 이상의 취약점 보유 (코스콤 2021년)

오픈소스 취약점 발생 사례

오픈소스명	발생시기	내용
아파치 스트럿츠	'17.5월	· 미국의 신용평가기관인 에퀴팩스(Equifax)는 웹 애플리케이션 개발 오픈소스인 아파치 스트럿츠의 원격코드 실행 취약점 공격으로 약 1억 4천만 명의 개인정보 유출
MySQL	'19.5월	· 오픈소스 데이터베이스인 MySQL 서버의 기본 포트를 통해 암호화 되어있지 않은 서버를 확인하고 랜섬웨어 공격을 시도
쿠버네티스	'19.6월	· 쿠버네티스에서 파일 복사 시 경로 조작을 통해 악성 파일 실행이 가능한 취약점이 발견되어 디렉토리 탐색 공격 ^{*)} 발생

*CVE: Common Vulnerabilities and Exposures

라이선스 위반 현황

삼성전자, 한컴 등 오픈소스 라이선스 규정 위반으로 손해배상

- 삼성전자는 리눅스 커널의 코드 및 BusyBox 사용 시, 라이선스 위반으로 손해배상 판결
- 2018년 한컴오피스 듀얼라이선스 미인지로 인해 23억원 지불

금융권, OSS 리스크 관리 안되고 있어...법적 분쟁/보안사고 발생 우려 ↑

- 금융권이 대부분 애플리케이션 내 오픈소스에 대한 법적 고지의무 등 기본적인 라이선스 규정도 지키지 않는 상황 (데일리시큐 2020년 07월)

1.3 오픈소스 사용 리스크 대응

“ 오픈소스 적극 활용에 따른 취약점, 라이선스 이슈 증가로 이에 대한 효율적인 리스크 해결 방안 마련이 필요

조직 내부 Pain Point

- ✓ 오픈소스, 취약점 수동 관리에 따른 비효율성
- ✓ 취약점 발견 시 개발 담당자 확인 어려움
- ✓ 취약점 조치여부 확인 및 후속 관리 곤란
- ✓ 특정 취약점 발견 시 해당 프로젝트 확인 애로



취약점 수동 관리에 따른 비효율 및 애로사항 발생



자동화된 OSS
취약점 관리
시스템 필요

1.4 SBOM의 제도화 추세

“ SBOM은 S/W 구성요소의 정보 및 공급 관계 추적 가능하여 취약성을 탐지하고 문제 발생시 신속한 수정을 지원

SBOM (Software Bill of Materials) 동향

SBOM이란?

- 식품 성분 명세서와 같이, 개발 결과물의 모든 SW 구성 항목 정보 제공
- 취약점, 라이선스 이슈 정보 포함

SBOM의 제도화 추세



미 대통령 행정명령
(2021.05.12.)

Section 4
소프트웨어 공급망의 안전보장 향상

국가기관 납품 소프트웨어의
SBOM 제공 의무화 명시 (22.12)

SBOM의 시장 파급 효과

- 미국 관공서에 납품하는 모든 소프트웨어는 SBOM 의무 제공
- 미국 제조사 납품 국내 협력 회사에도 SBOM 제공 요구 중

Labrador SBOM 대응



Developer

SBOM
소프트웨어 목록관리
라이선스 점검
보안취약점 검증



User

- 오픈소스 소프트웨어 자동관리
- 안전한 소프트웨어 재사용 가능

- 높은 신뢰도의 소프트웨어 사용
- 이슈 발생시 대응 용이



- ✓ 분석 특허 알고리즘 활용, 정확한 SBOM 생성
- ✓ 국내 최초로 SBOM 표준 Export 기능 제공 (SPDX/CycloneDX)

사례
미국 Intuitive Surgical, SBOM 솔루션으로 Labrador 선정(2023)

02

래브라도랩스 소개

소프트웨어 보안취약점 자동분석 시스템
AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

2.1 LABRADOR LABS 소개

“ '18년 설립 이후 오픈소스 소프트웨어의 사용 리스크 자동 탐지 및 관리 솔루션 제공

기업 개요

LABRADOR LABS

“Find all bugs with Labrador”

【회사소개】

래브라도랩스는 소프트웨어 보안취약점을 찾아내는 자동화된 분석 시스템을 구축하기 위한 학술 연구 협력 프로젝트로 부터 시작했습니다. 연구실에서 발현된 참신하고 혁신적인 기술을 사용하여 국내외 소프트웨어 개발 환경에 기여하고자 회사를 설립하게 되었습니다

현재 보안취약점 자동분석 기술을 기반으로 소프트웨어 보안과 라이선스 분석 자동화 제품인 래브라도를 출시하여 국내외 다양한 사이트에 서비스를 제공하고 있습니다.

설립일	2018. 3월
위치	서초구 반포대로 20, 3, 4F
대표자	이희조, 김진석

LABRADOR 

사업화

연구지원

CSSA
Center for Software Security and Assurance

원천기술

기술/라이선스
이전

- 회사와 연구소간 공동 DB TF 운영

- 보안 및 오픈소스 거버넌스 컨설팅 TF 운영

- Chief Scientist 제도 운영

* CSSA

(Center for Software Security and Assurance)

고려대학교 컴퓨터학과 4개 연구실을 중심으로
미국 카네기멜론, 영국 옥스포드, 스위스 ETH 대학의 연구팀이 모여
2015년 설립한 연구센터



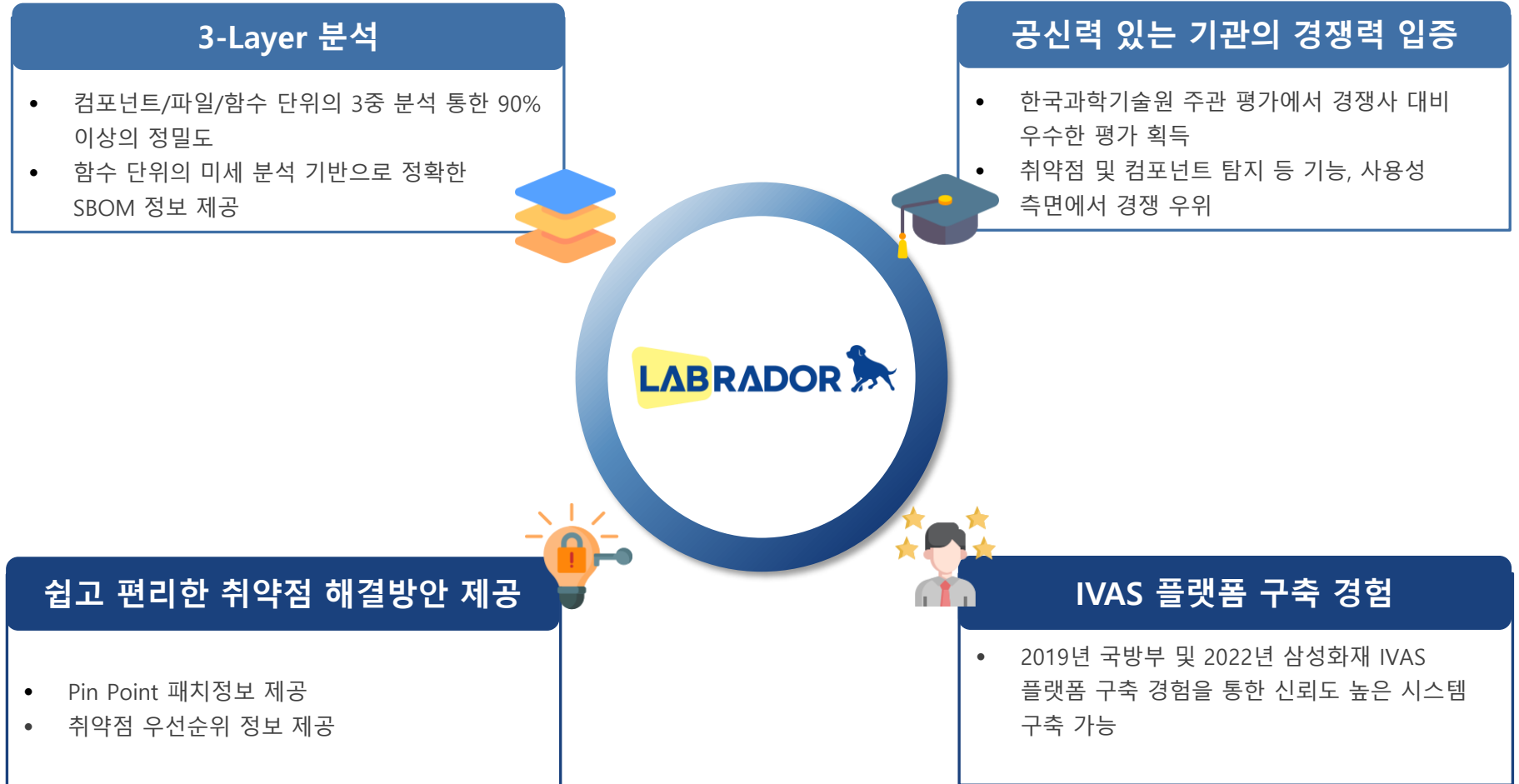
03

Labrador 소개

소프트웨어 보안취약점 자동분석 시스템
AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

3.1 Labrador 특징점

“ Labrador 솔루션은 3-Layer 취약점 분석과 같이 차별화 기술을 통해 높은 분석 정확도를 제공하며, 고객사의 사용 환경에 최적화된 솔루션 제공

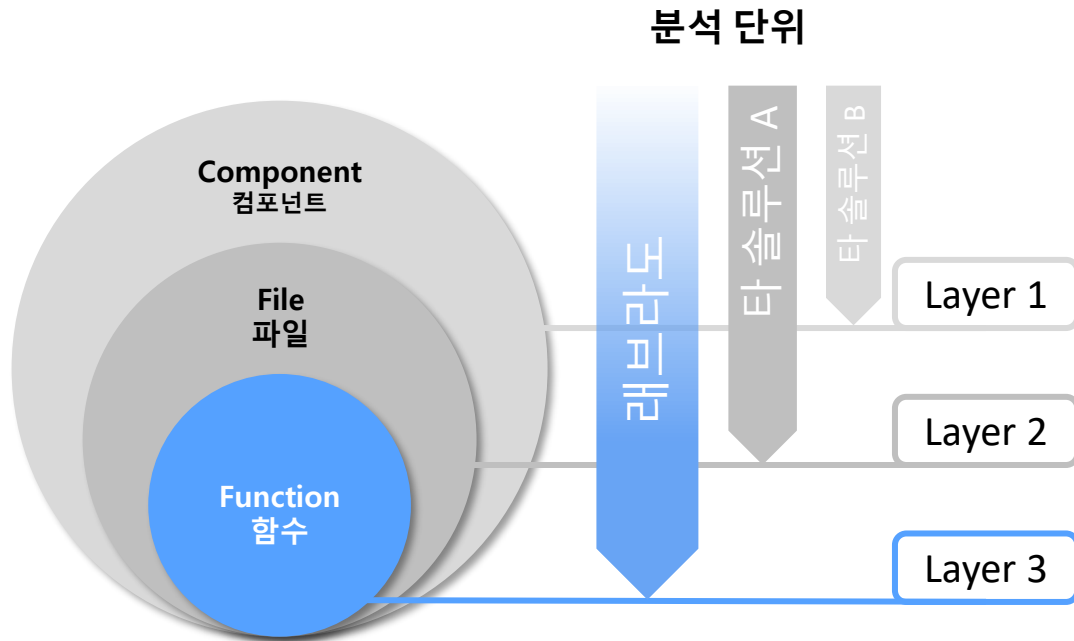


3.2 3-Layer 분석

“ 3-Layer 분석 개요

래브라도는 3-Layer 취약점 분석을 근간으로 오픈소스 소프트웨어의 구성요소(SBOM)를 정확히 탐지하고, 이를 기준으로 쉽고 편리한 취약점 분석 및 해결 방법을 제공

OSS 소스코드 구성



함수 단위 분석 VUDDY
컴포넌트 분석 CENTRIS

미국 특허: US 10146532.B2
국내 특허: 제 10-1568224 호

3-Layer Analysis, Only 래브라도 !!

1 정확한 SBOM 제공

✓ 다양한 디펜던시 분석으로 정확한 소프트웨어 구성 요소 탐지

2 획기적인 취약점 탐색 정확도 제공

✓ 함수 단위 미세분석으로 오탐 및 과탐 발생을 제로 수준

3 취약점만 해결 가능한 백포팅 해법 제공

✓ 문제되는 취약점 부분만 해결 가능한 검증된 패치정보 제공

4 사용자 정의 취약점 등록 및 관리 가능

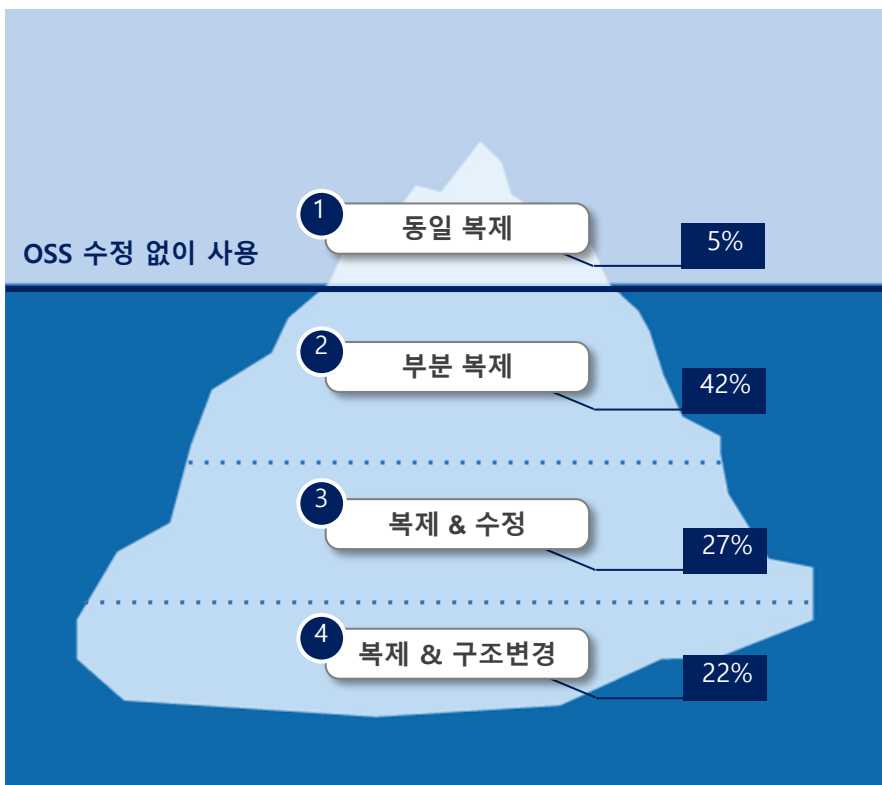
✓ 컴포넌트 단위 포함, 함수단위의 자체 취약코드 등록 및 탐지 기능으로 자체취약점 관리

3.3 3-Layer 분석의 필요성

“ 3-Layer 분석 특성

오픈소스 소프트웨어 활용 시, *95%의 오픈소스 소프트웨어가 부분 복제되거나, 수정 및 변경되어 재사용되고 있습니다. 3-Layer 취약점 분석 방식은 컴포넌트, 파일 및 함수 단위까지의 취약점 분석을 실행하기 때문에 다양한 활용 형태에 대응 가능하여 오탐 및 과탐을 최소화합니다.

분석 대상 사용자 S/W 활용 형태



3-Layer 분석 방식

OSS 활용 형태	컴포넌트 단위 취약점 매칭 (Layer 1)	파일 단위 취약점 매칭 (Layer 2)	함수 단위 취약점 매칭 (Layer 3)
1 동일 복제	○	○	○
2 부분 복제	△ 일부 탐지 가능	○	○
3 복제 & 수정	X	X	△ 일부 탐지 가능
4 복제 & 구조변경	X	△ 일부 탐지 가능	△ 일부 탐지 가능

"CENTRIS: A Precise and Scalable Approach for Identifying Modified Open-Source Software Reuse"
 IEEE/ACM Int'l Conf. on Software Engineering (ICSE), May 2021.
<https://ccs.korea.ac.kr/pds/ICSE21.pdf>

3.4 함수 취약점 탐지

“ 함수 취약점 탐지 및 수정 예시

- logging-log4j2 컴포넌트 분석 진행
- 5개의 함수 취약점 탐지
(CVE-2021-44228, CVE-2021-44832)
- 함수 취약점이 탐지된 파일 코드 수정
- DataSourceConnectionSource.java
파일의 취약한 함수 2건 수정
- 컴포넌트 재분석 수행
- 컴포넌트 코드 수정본 분석 수행
- 해당 CVE 취약점 제거 확인
- 취약점 수 변화 확인(5개->3개)
- CVE-2021-44832 취약점 제거

함수 취약점(5) 🛡️ 화이트리스트 (0)

번호	정책	함수 이름	파일 이름	점수	CVE ID	CWE ID	라인	컴포넌트	패치 안내
1	🛡️	createManager	JndiManager.java	10	CVE-2021-44228	CWE-20 🔗 CWE-400 🔗 CWE-502 🔗	178 ~ 185	logging-log4j2	View
2	🛡️	JndiManager	JndiManager.java	10	CVE-2021-44228	CWE-20 🔗 CWE-400 🔗 CWE-502 🔗	42 ~ 45	logging-log4j2	View
3	🛡️	lookup	JndiManager.java	10	CVE-2021-44228	CWE-20 🔗 CWE-400 🔗 CWE-502 🔗	171 ~ 173	logging-log4j2	View
4	🛡️	createConnectionSource	DataSourceConnectionSource.java	6.6	CVE-2021-44832	CWE-20 🔗	67 ~ 86	logging-log4j2	View
5	🛡️	DataSourceConnectionSource	DataSourceConnectionSource.java	6.6	CVE-2021-44832	CWE-20 🔗	44 ~ 47	logging-log4j2	View



함수 취약점 패치 안내

취약점 ID CVE-2021-44832 [🔗](#)

CVSS V2 6.5 CVSS V3 6.5

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.13.2.

번호	파일 이름	함수 이름	라인
1	log4j-core/src/main/java/org/apache/logging/log4j/core/appender/dbjdbbc/DataSourceConnectionSource	DataSourceConnectionSource	44-47

다음은 참조하여 코드를 수정해주세요.

취약 함수

1	- DataSourceConnectionSource.java_OLD	1	+ DataSourceConnectionSource.java_NEW
..

함수 취약점 패치 안내

취약점 ID CVE-2021-44832 [🔗](#)

CVSS V2 6.5 CVSS V3 6.5

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.13.2.

번호	파일 이름	함수 이름	라인
1	log4j-core/src/main/java/org/apache/logging/log4j/core/appender/dbjdbbc/DataSourceConnectionSource	createConnectionSource	67-86

다음은 참조하여 코드를 수정해주세요.

취약 함수

1	- DataSourceConnectionSource.java_OLD	1	+ DataSourceConnectionSource.java_NEW
..



함수 취약점(3) 🛡️ 화이트리스트 (0)

번호	정책	함수 이름	파일 이름	점수	CVE ID	CWE ID	라인	컴포넌트	패치 안내
1	🛡️	createManager	JndiManager.java	10	CVE-2021-44228	CWE-20 🔗 CWE-400 🔗 CWE-502 🔗	178 ~ 185	logging-log4j2	View
2	🛡️	JndiManager	JndiManager.java	10	CVE-2021-44228	CWE-20 🔗 CWE-400 🔗 CWE-502 🔗	42 ~ 45	logging-log4j2	View
3	🛡️	lookup	JndiManager.java	10	CVE-2021-44228	CWE-20 🔗 CWE-400 🔗 CWE-502 🔗	171 ~ 173	logging-log4j2	View

3.5 공신력 있는 기관의 경쟁력 입증

“ 한국과학기술원(KAIST) 사이버보안연구센터 주관 ‘오픈소스 취약점 분석 도구 평가’ 래브라도는 경쟁사 대비 최우수 평가 획득

연구 범위 및 내용

CSRC Weblog

[일:] 2022년 03월 04일



2021년 12월 일명 “Log4j 보안 취약점 사태”가 발생함에 따라 오픈소스인 “Log4j”를 활용한 정보시스템을 운영하는 정부기관 및 기업들은 비상 상황에 맞닥뜨리게 되었습니다. 오픈소스는 여러 장점에도 불구하고 현재의 개발 패러다임으로 인해 소프트웨어 보안 취약점이 손쉽게 확산 될 수 있다는 문제점이 많아 오픈소스의 안전성 및 신뢰성 확보하기 위한 대응책 마련이 필요한 시점입니다. 이번 포스팅에서 오픈소스 취약점 분석 도구 소개와 오픈소스 취약점 분석 도구에 대한 평가를 작성하였습니다.

• 카이스트 블로그 : <https://csrc.kaist.ac.kr/blog/2022/03/04/>

- 평가 지표** : 소프트웨어진흥법 제49조 제2항 “소프트웨어 기술성 평가 기준 지침” 평가 기준에 따른 상용소프트웨어 평가항목 및 배점 참고(제3조 제2항 관련)
- 평가 방법** : GitHub 최상위 랭크된 오픈소스 중 자주 사용되는 7개 언어로부터 생성된 프로젝트 10개 선정 후, 보안 취약점 분석 도구인 Labrador와 해외 도구 3종에 대해 컴포넌트 탐지와 취약점 분석 결과 비교
- 평가 결과** : 종합 분석 결과, 37개 항목 중 25개 항목에서 “우수” 평가를 받아 최우수 도구로 선정됨.
- 종합 평가 결과표**

		A	B	C	Labrador
기능성	우수	4	2	1	8
	보통	1	2	3	1
	나쁨	3	4	5	0
사용성	우수	7	10	9	14
	보통	4	1	5	4
	나쁨	6	6	7	3
유지 관리성	우수	3	2	2	3
	보통	0	0	2	1
	나쁨	2	2	3	3

04

Labrador 주요 기능

소프트웨어 보안취약점 자동분석 시스템
AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

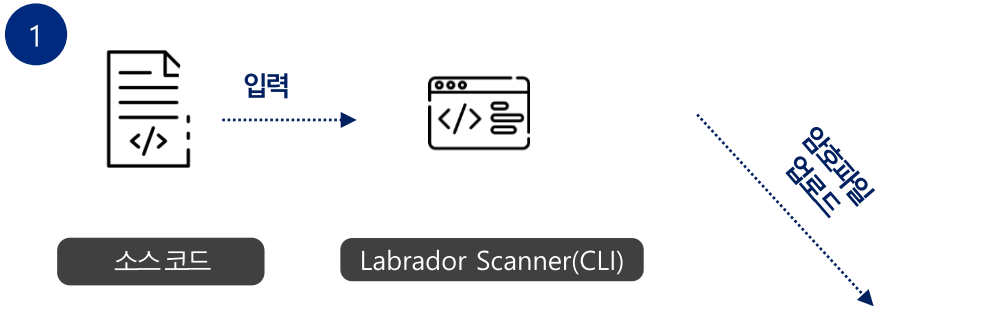
4.1 다양한 Scan Mode 제공

“ 사용자의 환경을 고려하여 다양한 소스코드 스캔 방식 제공

Option 1

CLI

사용자 시스템의 Command Line에서 소스코드 스캔 후 결과 확인
(코드 프라이버시가 보장되는 Hashed 암호파일 업로드)



Option 2

Git URL

Public/Private 저장소의 소스코드 URL을 입력하면
자동 스캔 및 분석



Option 3

ZIP Upload

분석대상 소스코드를 압축해서 업로드 후
자동 스캔 및 분석



4.2 오픈소스 라이선스 컴플라이언스 관리

“ 소스코드 심층 분석 통해 오픈소스 라이선스 정보 수집 및 컴플라이언스 이슈에 대한 사전 대응

라이선스 컴플라이언스 관리

- 오픈소스 라이선스 이슈 정보 제공 통해 컴플라이언스 리스크 제거
- 검출된 라이선스의 고지문 예제 자동 생성

License Term	Status
Permits copying, distributing and modifying	YES
Must attach a copy of the license at distribution	YES
Must retain all copyright or attribution notices	Allowing distribution by changing to another license after creating a combined work (can be combined with exclusive software)
The scope of the reciprocity obligation	-
May convey a Combined Work and distribution of other licenses is allowed	CONDITIONAL
Must mention if software is modified	-
Grants explicit patent license	-
License terminates upon patent lawsuit filing	-
Restrictions on use of names, trademarks, and trade names	-
Disclaimer of Warranty	YES
Limitation of liability	YES

No.	Policy	Type	License	URL	Actions
1	MIT License	MIT License	MIT License	https://opensource.org/licenses/MIT	View

License Name	URL
Apache License 2.0	https://www.apache.org/licenses/LICENSE-2.0
Apache License 2.0	https://www.apache.org/licenses/LICENSE-2.0
Apache License 2.0	https://www.apache.org/licenses/LICENSE-2.0
Apache License 2.0	https://www.apache.org/licenses/LICENSE-2.0
Apache License 2.0	https://www.apache.org/licenses/LICENSE-2.0
Apache License 2.0	https://www.apache.org/licenses/LICENSE-2.0
Apache License 2.0	https://www.apache.org/licenses/LICENSE-2.0
Apache License 2.0	https://www.apache.org/licenses/LICENSE-2.0
Apache License 2.0	https://www.apache.org/licenses/LICENSE-2.0
Apache License 2.0	https://www.apache.org/licenses/LICENSE-2.0

4.3 오픈소스 취약점 관리

“ 오픈소스 취약점 정보 제공 기능

01 정확한 취약점 정보 제공

- 취약점에 대한 3-Layer 분석 기반 90% 이상의 정밀도
- 변경된 소스코드에 대해서도 정확한 분석 가능

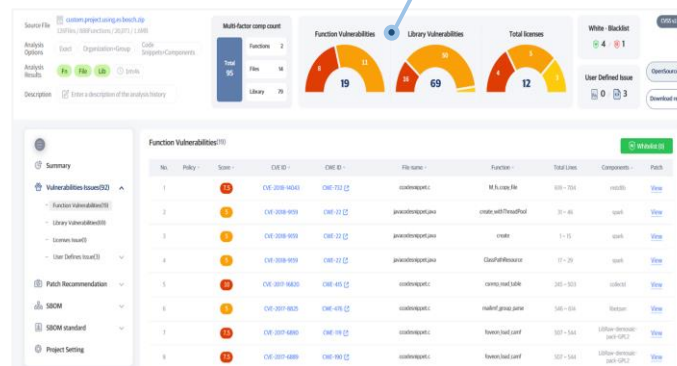
02 Pinpoint 패치정보 제공

- 취약한 부분의 코드만 수정하여 개발 효율 극대화
- 단순 버전 업그레이드와 달리, 부작용 사전 방지 가능

03 취약점 우선순위 정보 제공

- CVSS 기준 위험 스코어 정보 제공
- CWE Top 25별 추천 패치 우선 순위 정보 제공

정확한 취약점 정보 제공



취약 부분 패치 제공

```
getCookie

Vulnerable Function
1 @@ -1,5 +1,11 @@
2
3 public static String getCookie(HttpServletRequest req,String
4 Cookie c = getCookie(req, name);
5 if(c==null || c.getValue()==null) return defaultValu;
6 return c.getValue();
7
8
9
10
11
12

Patch Function
1 +++ Functions.java_31_NEW.vul 2021-12-04 17:44:50.01016901
2 @@ -1,5 +1,11 @@
3 public static Cookie getCookie(HttpServletRequest req,String
4 Cookie[] cookies = req.getCookies();
5 if(cookies==null)
6 for (Cookie cookie : cookies) {
7 if(cookie.getName().equals(name)) {
8 return cookie;
9 }
10 }
11 }
12 return null;
```

4.4 사용자 운영 지원

“ 오픈소스 프로젝트의 분석 이력 자동 관리

01 회사 내 그룹별 사용 지원

- 그룹 및 프로젝트 별 독립된 사용환경 및 이력 관리 제공
- 최상위 관리자의 통합 관리 기능 제공

02 분석 이력 관리

- 프로젝트 취약점, 라이선스 이슈 및 조치 이력 확인
- 프로젝트 버전 별 비교 분석 기능 제공

03 다양한 보고서 제공

- PDF 형식의 요약 보고서 제공
- 엑셀 형식의 상세 보고서 제공

분석 이력 관리

Labrador Analysis Detail Report

Report Generated At: [Date]

Project Summary

Project Name	Labrador 001
Started At	2022-02-07 14:15:33
Ended At	2022-02-07 14:15:55
Analysed By	Labrador
Elapsed	32s

Analysis

Analysis Method	Source Maps Labrador Scanner v2.0.0
Repo URL	https://github.com/LabradorLabs/Labrador
Target Branch	main
Target Commit	sha256:1234567

Source

Project Size	1.23MB
Scanner Result	Function: Pass, File: Pass, Count: 254, Function: 874, Lines: 17,309

Analysis Option

Mode	Exact
Applied Policy	Organization, Group
Applied Fuzz-Oracles	Functions, Components
Working Rule ID	Function: 0%, File: 0%

Result Summary

Vulnerabilities - Issues (CVE)	Total: 6
Code Level Vulnerabilities	Function Level: 3, File Level: 3
Library Vulnerabilities	Total: 37
User Defined Issues	Total: 0, Functions: 0, Components: 0
BOM (Software Bill of Materials)	Total: 41
Comp.	Function Components: 8, File Components: 0
Library Components	73
License	74

Overview

Code Level Vulnerabilities: CVESS v2 (6), CVESS v1 (6), License (6)

Library Vulnerabilities: CVESS v2 (37), CVESS v1 (21), White-Blacklist (0), User Defined Issues (0)

Vulnerabilities - Issues (CVE): Critical (6), High (0), Medium (0), Low (0), Unknown (0)

White-Blacklist: Potential (0), Pressure (0), Unknown (0)

User Defined Issues: 0

다양한 보고서 제공

4.5 조직 내 소프트웨어 거버넌스 정책 자동 관리

“ 소프트웨어 거버넌스에 대한 다양한 정책 및 자동화 지원

01 자체 취약점 및 컴포넌트 관리

- 자체 개발한 소스코드의 취약점 자동 관리 기능 제공
- 조직 내 사용금지 된 컴포넌트 자동 필터링 기능 제공

02 Whitelist / Blacklist 관리

- 특정 CVE/CWE/컴포넌트/라이선스에 대한 조직내 정책 자동 관리 기능 제공

03 미등록된 취약점 관리

- CVE에 미등록된 취약점 등록 및 관리 기능 제공

The screenshot displays three overlapping windows from a software governance tool:

- Code Snippet:** A Java code snippet for a function named `void AP_Param-set_defaults_from_table`. It shows logic for setting default values for parameters based on table names and IDs.
- Group Policy:** A table titled "licenses[14] - Whitelist - Blacklist" showing a list of licenses. The table has columns for "No.", "Policy", and "License". Several entries are marked with a red 'B' icon, indicating a specific policy status. The table content is as follows:

No.	Policy	License
14	B	GNU General Public License v2.0 only
13	B	GNU General Public License v3.0 only
12	B	Affero General Public License v1.0 only
11	B	GNU Affero General Public License v3.0 only
10	B	GNU Free Documentation License v1.1 only - invariants
- SecurityContext Dialog:** A configuration window for a component named "SecurityContext". It shows the component name, description ("User defined component #1"), and a list of files. The files listed are:

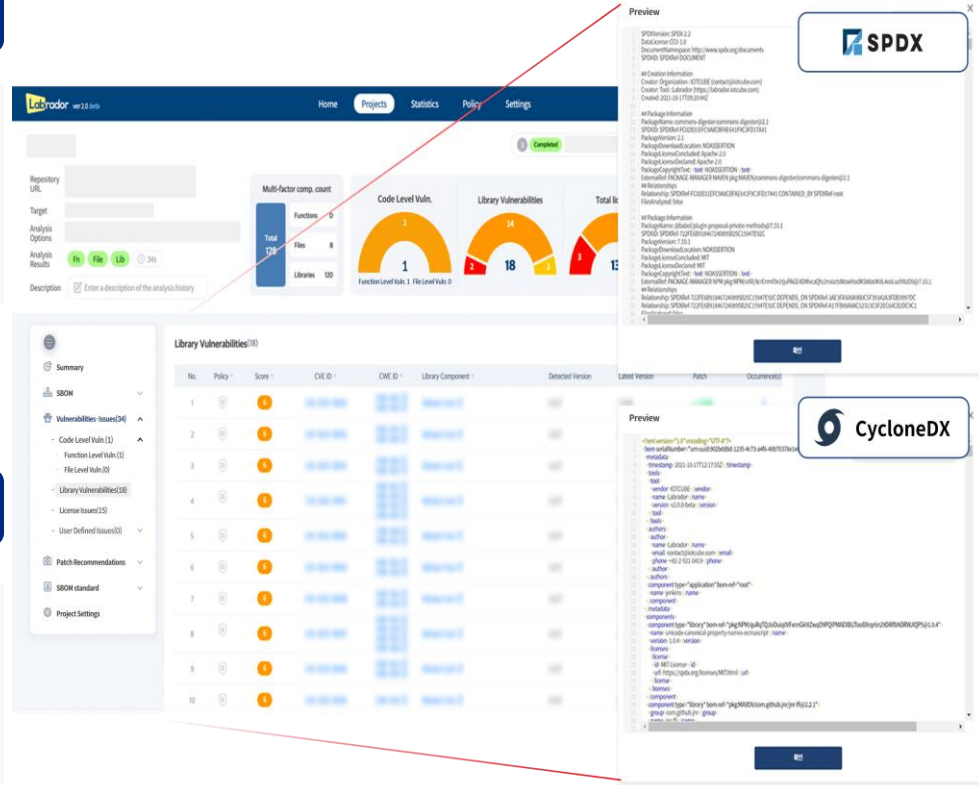
번호	파일 이름
1	...SecurityContext.java
2	...SecurityContextHolder.java
3	...SecurityContextImpl.java
4	SecurityContext.java
5	SecurityContextHolder.java
6	SecurityContextImpl.java

4.6 SBOM 국제 표준 포맷 제공

SPDX & CycloneDX 국제 표준 포맷 제공

01 국제 표준 포맷 지원

- 안전하고 투명한 소프트웨어 공급망 관리를 위해 SBOM 국제 표준인 SPDX, CycloneDX 지원



02 SW 공급망 관리 지원

- SDLC 전 단계에서 SW 구성요소 추적관리
- 협력업체를 포함한 3rd party SW 구성요소 관리
- 구성요소 관리를 통한 SW 공급망 공격 예방

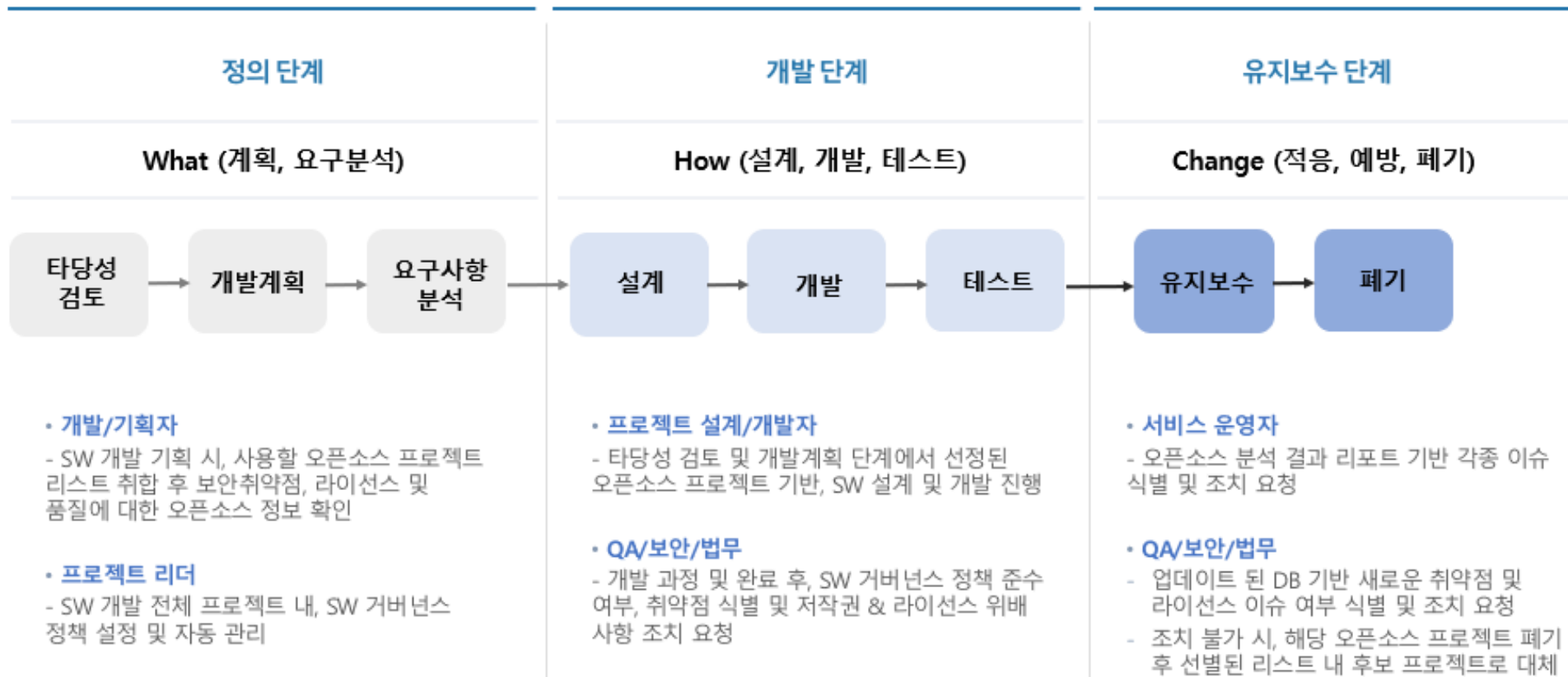
05

Labrador 운영 환경

소프트웨어 보안취약점 자동분석 시스템
AUTOMATED SW VULNERABILITY ANALYSIS SYSTEM

5.1 SDLC 단계별 오픈소스 관리 운영 방안

“ SDLC의 정의 단계, 개발 단계 및 유지보수 전 단계에 걸쳐 오픈소스 관리 지원



5.1 SDLC 단계별 오픈소스 관리 운영 방안

“ SDLC의 정의 단계, 개발 단계 및 유지보수 전 단계에 걸쳐 오픈소스 관리 지원



정의 단계

- ✓ 사전 기능 점검 및 보안성 테스트를 위해 DB 검색 기능 제공
- ✓ DB 검색으로 찾은 컴포넌트의 취약점 및 라이선스 이슈 파악

컴포넌트/취약점 DB 검색

컴포넌트, 취약점 검색

컴포넌트/취약점 DB 검색 가이드

- 라이브러리 컴포넌트 검색
 - java maven 또는 gradle을 이용한 프로젝트 개발 시, 사용하고자 하는 라이브러리를 검색해서 안전한 버전인지 확인 후 사용해 주세요.
 - 키워드로 검색이 가능하며 groupid:artifactid 형태로 검색하면 정확한 검색이 가능

'log4j' 검색결과

전체 656 | 취약점 25 | 파일/함수 컴포넌트 2 | 라이브러리 컴포넌트 429

취약점(25)

번호	ID	CVSS v2	CVSS v3	설명
1	CVE-2008-7261	7.5	8.1	The Workplace (aka WP) component in IBM FileNet P8 Application Engine (P8AE) 3.5.1 before 3.5.1-010 reco...
2	CVE-2012-5616	5.5	6.5	Apache CloudStack 4.0.0-incubating and Citrix CloudPlatform (formerly Citrix CloudStack) before 3.0.6 stor...
3	CVE-2014-0722	5.0	6.1	The log4jnet web application in Cisco Unified Communications Manager (UCM) does not properly validate...
4	CVE-2017-5645	7.5	9.0	In Apache Log4j 2.x before 2.8.2, when using the TCP socket server or UDP socket server to receive seriali...

컴포넌트 현황 파악

Apache Log4j Core 2.14.1 Release Date: 2021.03.07

부안 README

CVSS v2: 2, 3, 4, 5, 6, 7, 8, 9, 10

CVSS v3: 2, 3, 4, 5, 6, 7, 8, 9, 10

취약점 (4)

번호	ID	CVSS v2	CVSS v3	설명
1	CVE-2021-44228	9.3	10	Apache Log4j 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12...
2	CVE-2021-44832	8.5	6.6	Apache Log4j versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2...
3	CVE-2021-45046	6.1	8	It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was in...
4	CVE-2021-45105	4.3	6.0	Apache Log4j versions 2.0.alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1) di...

보안 동향

최근 30일 | 모든 버전

라이선스 현황 파악

Information

Language: Java

Age: 10 years old

License: Apache-2.0

Keyword: apache, api, java, library, log4j, log4j2, logging

Popularity

Monthly commits

Downloads by version

라이브러리 일반 정보 및 기능 파악

Repository: https://github.com/apache/log4j...

Contributors: 30 (G, R, J, M) ...

Stars: 2,895 | Watchers: 112 | Forks: 1,404

Tags: 136 | Last Commit: 2022.08.27

5.1 SDLC 단계별 오픈소스 관리 운영 방안

“ SDLC의 정의 단계, 개발 단계 및 유지보수 전 단계에 걸쳐 오픈소스 관리 지원



개발 단계

Patch 1

Vulnerabilities ID CVE-2014-2065 CVSS v2 CVSS v3

Cross-site scripting (XSS) vulnerability in Jenkins before 1.551 and LTS before 1.532.2 allows remote attackers to inject arbitrary web script or HTML via the iconSize cookie.

Function backporting	Vulnerability Type	File	Function	Line
1	Function Level Vuln.	Functions.java		

Modify your code based on the following recommendation.

취약 부분 패치 제공

```

1 Functions.java_31_OLD.vul 2021-12-04 17:44:50.01016907
2 @@ -1.5 +1.11 @@
3 public static String getCookie(HttpServletRequest req, String
4 cookie c = req.getCookies(), name);
5 if(c==null || c.getValue()==null) return defaultValues;
6 return c.getValue();
7 }
8
9
10
11
12
13
14
15 return null;
    
```

+++ Functions.java_31_NEW.vul 2021-12-04 17:44:50.01016907
 @@ -1.5 +1.11 @@
 + public static String getCookie(HttpServletRequest req, String
 + cookie[] cookies = req.getCookies();
 + if(cookies==null) {
 + for (Cookie cookie : cookies) {
 + if(cookie.getName().equals(name)) {
 + return cookie;
 + }
 + }
 + return null;

취약점이 없는 종속 라이브러리를 사용하는 상위 라이브러리의 버전 정보 제공 가능

1.7.0 로 업그레이드 시 하위 취약점 제거

라이브러리	버전	라이선스	상태
org.json:json	20180813	JSON License	20230217
org.apache.commons:commons-collections4	4.4	Apache License 2.0	no release
org.apache.commons:commons-lang3	3.12.0	Apache License 2.0	no release
org.apache.commons:commons-text	1.11.0	Apache License 2.0	no release
org.apache.commons:commons-io	2.14.0	Apache License 2.0	no release
org.apache.commons:commons-math3	3.6.1	Apache License 2.0	no release
org.apache.commons:commons-compress	1.22	Apache License 2.0	no release
org.apache.commons:commons-csv	1.10.0	Apache License 2.0	no release
org.apache.commons:commons-jcs-core	3.2	Apache License 2.0	no release
org.apache.commons:commons-jcs-memcached	3.2	Apache License 2.0	no release
org.apache.commons:commons-jcs2-core	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-memcached	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-spring3	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-shiro	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-tran	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp3	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp4	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp5	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp6	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp7	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp8	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp9	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp10	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp11	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp12	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp13	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp14	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp15	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp16	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp17	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp18	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp19	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp20	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp21	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp22	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp23	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp24	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp25	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp26	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp27	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp28	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp29	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp30	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp31	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp32	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp33	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp34	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp35	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp36	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp37	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp38	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp39	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp40	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp41	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp42	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp43	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp44	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp45	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp46	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp47	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp48	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp49	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp50	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp51	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp52	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp53	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp54	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp55	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp56	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp57	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp58	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp59	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp60	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp61	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp62	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp63	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp64	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp65	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp66	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp67	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp68	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp69	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp70	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp71	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp72	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp73	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp74	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp75	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp76	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp77	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp78	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp79	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp80	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp81	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp82	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp83	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp84	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp85	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp86	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp87	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp88	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp89	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp90	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp91	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp92	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp93	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp94	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp95	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp96	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp97	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp98	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp99	2.13.0	Apache License 2.0	no release
org.apache.commons:commons-jcs2-xmpp100	2.13.0	Apache License 2.0	no release

- ✓ 통합 포털과 연동하여 주기적인 취약점 자동 분석 기능 제공
- ✓ 취약한 코드를 대체할 패치 코드 및 취약한 버전에 대한 대체 버전 제공
- ✓ 고려대 CSSA와의 긴밀한 협력관계 통해 전문 대응 인력 확보

LABRADOR

사업화

연구지원
기술/라이선스이전

CSSA

원천기술

'23.10 현재 총 7개 특허 관련 기술 이관

- 취약점 DB TF 운영 중
- 공동 보안 세미나 시행
- Chief Scientist 현장 지원

CSSA와 기술이전 및 교류로 긴밀한 협력관계 유지



5.1 SDLC 단계별 오픈소스 관리 운영 방안

“ SDLC의 정의 단계, 개발 단계 및 유지보수 전 단계에 걸쳐 오픈소스 관리 지원



유지보수 단계

- ✓ 통합 포털의 통합 점검 기능으로 개발한 소프트웨어의 기능 및 보안성 이슈 검증
- ✓ 소프트웨어의 직/간접 종속성 파악
- ✓ 조치 관리 기능 통해 운영중인 소프트웨어 지속적으로 모니터
- ✓ 취약한 코드를 대체할 패치 코드 및 취약한 버전에 대한 대체 버전 제공

통합 점검
통합 점검 기능으로 '분석한 레퍼지토리에에서 발견된 요소들'을 검색할 수 있습니다.

레퍼지토리: [선택] 검색어: 검색

검색 결과(1) [목록 다운로드](#)

번호	발견 항목	참조 위치	시스템명	레퍼지토리명
1	r/logging-log4j2-rel-2.14.0.git logging-log4j2-rel-2.14.0	레퍼지토리	운영System	r/logging-log4j2-rel-2.14.0.git

컴포넌트 | 파일 매칭(2) | 라이브러리 매칭(526) | 소스 트리

라이브러리 매칭 컴포넌트(526) [목록](#) [트리](#)

직/간접 종속성 파악

Direct Transitive

조치 현황/이력 관리

Python 프로젝트 설명e

취약점 조치 현황 ! 발견된 취약점을 조치해 주세요.

	조치 필요	조치 계획 미등록	조치 예정	조치일 경과	예외 처리	조치 유예 /불필요
컴포넌트 (파일매칭)	0	31	0	0	0	9
컴포넌트 (라이브러리 매칭)	0	0	0	0	0	0
파일	0	1	0	0	0	1
합수	0	62	0	0	0	69

조치 이력

김희상님이 조치 예정 상태로 변경하였습니다.
조치 예정일 : 2023.07.03
조치 계획:
2023.07.03 10:43:45

취약점이 발견되었습니다.
2023.07.03 10:43:33

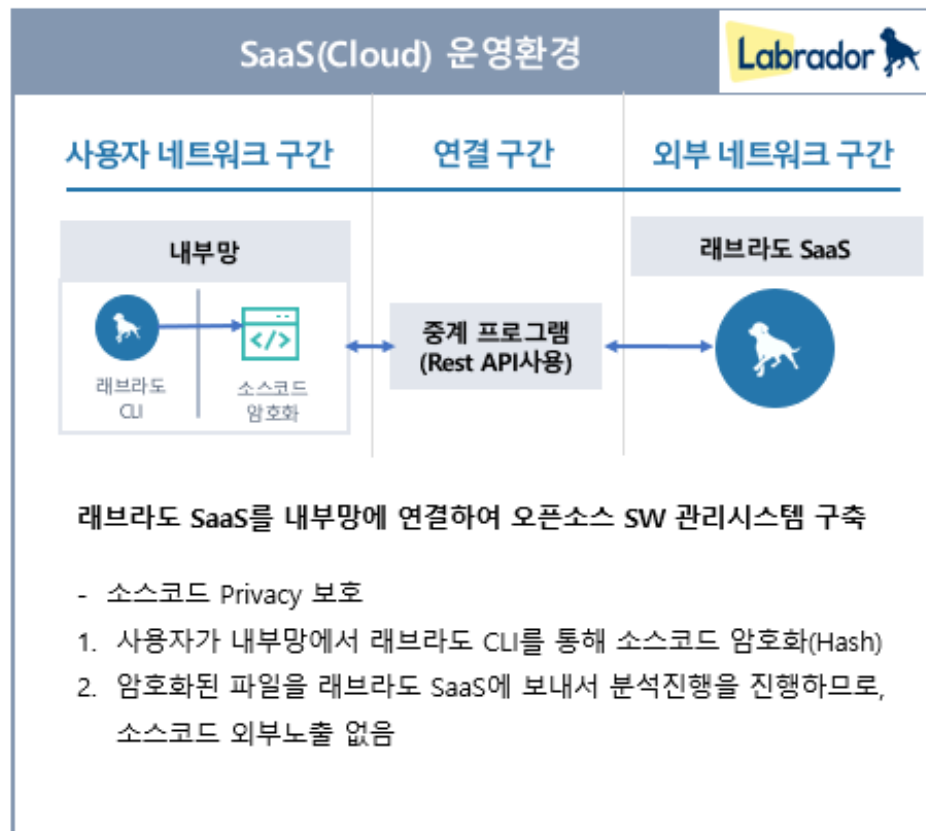
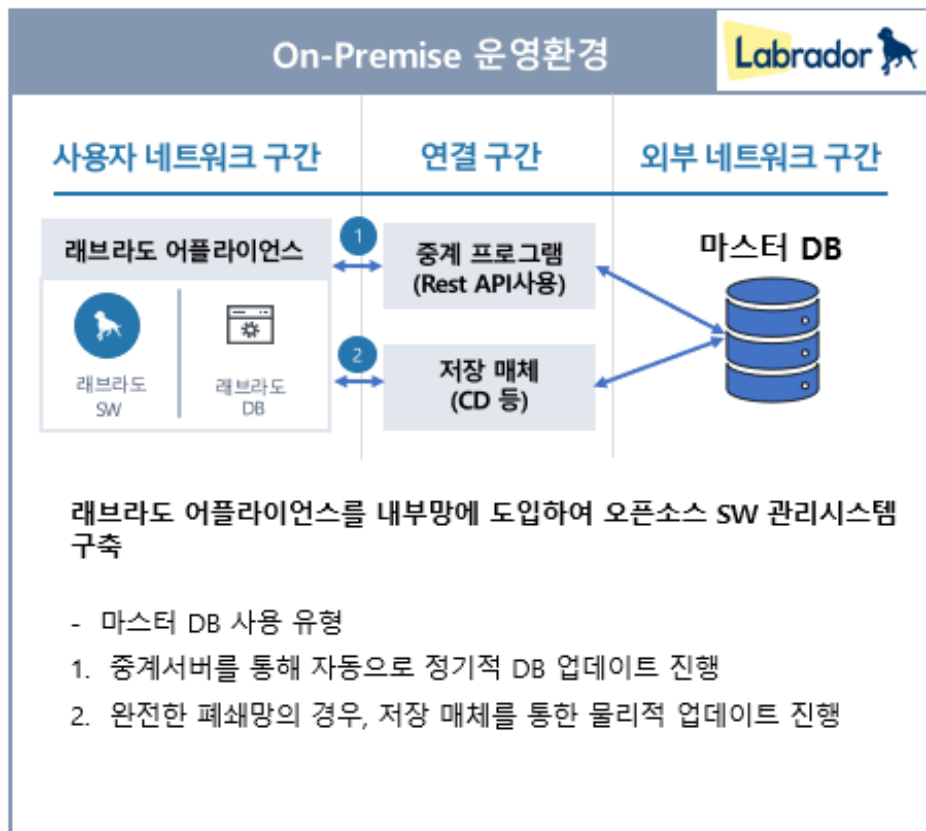
김희상님이 조치 예정 상태로 변경하였습니다.
조치 예정일 : 2023.07.18
조치 계획:
2023.07.03 10:43:28

김희상님이 예외 처리 상태로 변경하였습니다.
예외 사유: 파일, 함수 취약점 패치 완료 후에도 컴포넌트 취약점이 남은 경우 예외 처리합니다.
2023.07.03 10:43:14

김희상님이 조치 예정 상태로 변경하였습니다.
조치 예정일 : 2023.07.03

5.2 래브라도 구축 환경

“ On-Premise 및 SaaS 방식의 운영환경 제공



감사합니다



(주)래브라도랩스 <http://www.labradorlabs.ai>

📍 서울특별시 서초구 반포대로 20 3, 4층

☎ 02-921-0419