

# Debricked

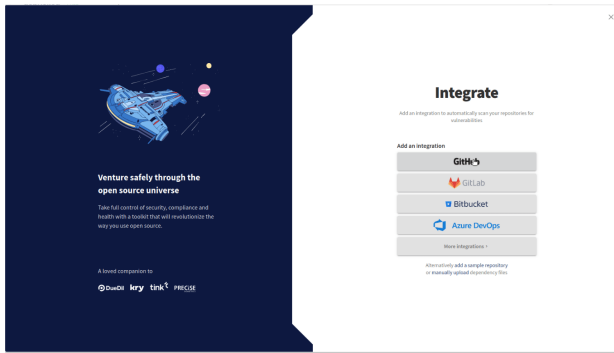
Created by 최혜성 hyesung.choi, last modified about 5 hours ago

## Debricked 개요

- **Debricked** (<https://debricked.com/>)
  - Open Source Security, Compliance, Community Process를 쉽게 자동화함
    - **Security vulnerabilities**
      - Open source dependency에서의 취약성을 지속적으로 자동으로 식별, 수정 및 위험을 방지함
      - Commit 할 때마다 Scan하고 새로운 취약점이 나타날 때 알림을 받을 수 있음
    - **License Compliance**
      - 자동화되고 시행가능한 pipeline rule로 Open Source Compliance를 보장하고 유지함
      - 용도에 따라 repository 위험 수준을 계산함
    - **Community Health**
      - 높은 품질을 보장하기 위해 도입하기 전에 Open Source Dependency를 평가하고 비교함
      - 시간이 지남에 따라 Project를 모니터링하고 community 통찰력을 얻고 잠재적인 위험을 식별함
  - Export a CycloneDX SBOM
- What can I do?
  - **Security example highlight**
    - 많은 보안 취약점이 있는 repository에서 이들 취약점을 각각 검토하는 것이 아니라, 'Open Pull Request'를 이용하여 한 번의 pull request로 가능한 한 많은 취약점 문제를 해결함
    - Open Pull Request를 클릭하면 Dependency를 업데이트하여 취약성을 해결하고 pull request를 생성할 수 있음
  - **License example highlight**
    - Dependency를 통해 가져온 License 종류를 알아야 함
    - 모든 License와 영향을 받는 repository가 있는 report가 생성되어 메일로 전송됨
  - **Automation example highlight**
    - 여러 가지 자동화 규칙을 통해 새로운 commit에 취약성이 존재하는 경우, pipeline을 실패시키고 이런 사건에 대한 알림을 받을 수 있음
- 사용 요금
  - [Click here to expand...](#)
    - **Free**
      - 제공 기능
        - Vulnerability Management
        - License Management
        - Project Health
      - 첫 달, 1000회 Scan 및 매달 100 Scan 무료
    - **Premium**
      - 제공 기능
        - Free 기능
        - License report
        - Chat and email support
        - API access (Rate limit : 5000)
        - Unlimited scans
      - 가격
        - 1개월, €25 /contributing developer(code contributor = someone who has made a commit to a repository within the last 30 days)
          - 환율 1350원 기준 33,750원
    - **Enterprise**
      - 제공 기능
        - Premium 기능
        - Enterprise level support
        - SBOM export
        - Start left policies
        - Increased compute
        - Unlimited API access
      - 가격
        - 1개월, €60 부터- /contributing developer(code contributor = someone who has made a commit to a repository within the last 30 days)
          - 환율 1350원 기준 81,000원

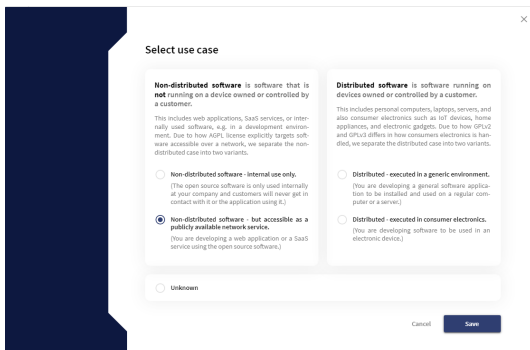
## Getting Started

- Setup an integration on first login
  - 자동으로 Vulnerability를 scan하기 위한 Repository integration을 추가함



- Set up a license use case
  - Repository에서 code 배포 방법 설정(Internal user only, Network service 등) 에 따라 License Risk가 달라질 수 있음
  - Repository Settings > Use case를 설정하면 License Risk(6단계)가 이에 따라 업데이트 됨

Name	License Risk	Affected repositories	Dependencies	License family
Apache-2.0	1 0 0 0 0 0	Pytho...	1	Permissive
BSD-2-Clause	Unknown	Pytho...	1	Permissive
BSD-3-Clause	1 0 0 0 0 0	Pytho...	1	Permissive
LGPL-2.1	1 0 0 0 0 0	Pytho...	1	Weak copyleft



- Setup automation
  - Automations engine을 사용하면 조건에 따라 규칙을 트리거 할 수 있음

- 기본적으로 원치 않는 License나 위험한 Vulnerability를 방지하기 위한 규칙을 설정할 수 있음
- 예) If a new dependency is added where the license risk is at least medium then notify all users in the group admins by email

Automation 알림 메일



### Automations Notification

A recent scan of the repository hyesung2/minio caused the following rule to trigger:

If a dependency contains a vulnerability which has not been marked as unaffected and which has not triggered this rule for this dependency before then notify all users in the group admins by email

[Manage rule](#)

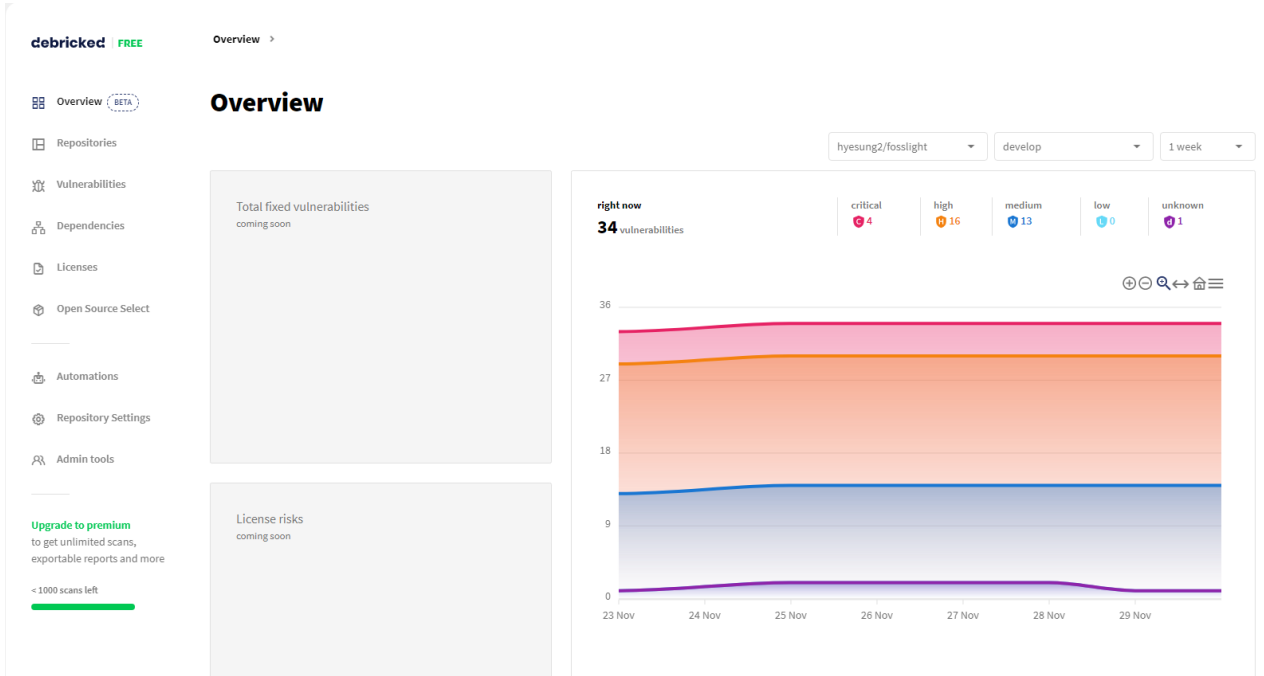
The rule was triggered for the following vulnerabilities:

Vulnerability	Dependencies	CVSS2	CVSS3
CVE-2022-32149	<a href="#">golang.org/x/text (Go)</a>	N/A	7.5
CVE-2021-38561	<a href="#">golang.org/x/text (Go)</a>	N/A	7.5
CVE-2022-21698	<a href="#">github.com/prometheus/client_golang (Go)</a>	5	7.5

### Dashboard

- 특정 repository 또는 모든 repository의 vulnerability 수에 대한 기록 데이터를 그래프 형식으로 볼 수 있음 (확인할 시간, 간격 등을 선택)
- 사용자 Repository 상태의 snapshot(unknown-, low-, high- 등의 vulnerability 정보 포함)을 주기적으로 생성함 (Repository를 성공적으로 Scan 할 때마다 업데이트됨)
- CVSS 점수를 기반으로 하며 CVSS3가 항상 CVSS2보다 우선함

Overview



## Repository View

### Repository main

[repository](#)

Generate report

Repositories

# Repositories

Scanning

+ Invite users

All

Search by name

15 entries

+ New

Name	Total vulnerabilities	Vulnerability priority	Review status	Total vulnerabilities with exploits
hyesung2/fosslight	34	4 Critical, 16 High	0 Unexamined, 34 Unaffected	1
hyesung2/fosslight_scanner	1	0 Critical, 1 High	0 Unexamined, 1 Unaffected	0
hyesung2/scancode-toolkit	0	0 Critical, 0 High	0 Unexamined, 0 Unaffected	0

< 1 >

- **Vulnerability priority:** CVSS score를 기반으로 한 vulnerability 분포
- **Review status:** How many vulnerabilities that are *vulnerable*, *unexamined*, and *unaffected*.
- **Total vulnerabilities with exploits:** The total amount of vulnerabilities that have at least one known exploit.

## Vulnerabilities in a repo

[Click here to expand...](#)

Repositories > **hyesung2/fosslight**

Automate

Generate report

# hyesung2/fosslight

Repository All branches

Fix vulnerability

The pull request will include the updates needed to fix as many vulnerabilities as possible

Open pull request

+ Invite users

Vulnerabilities Dependencies Licenses Commits

Search by name or dependency

6 Filter 15 entries

Name	Discovered	CVSS	debAI	Dependencies	Uses vulnerable functionality	Review status	Fixes and exploits
CVE-2022-31692	2022-11-23	9.8 Critical	74	spring-security-core (Ma...	Unknown	Unexamined	2
CVE-2022-26520	2022-11-23	9.8 Critical	71	org.postgresql:postgresq...	Unknown	Unexamined	2
CVE-2022-21724	2022-11-23	9.8 Critical	70	org.postgresql:postgresq...	Unknown	Unexamined	2
CVE-2020-10683	2022-11-23	9.8 Critical	70	dom4j:dom4j (Maven)	Unknown	Unexamined	2
CVE-2020-13936	2022-11-23	8.8 High	70	org.apache.velocity:velo...	Unknown	Unexamined	3

- Repository 별 Vulnerabilities, Dependencies, Licenses, Commits 정보를 보여줌
- **debAI:** Debricked의 지능형 시가 다른 metrics와 함께 자신의 보안 기본 설정을 기반으로 취약점 순위를 매김
- **Vulnerable functionality usage :** Vulnerable functionality가 실제로 사용되었는지를 표시함 (Yes, No, Unknown)
- **Fixes and exploits :** ???

## Vulnerability details

[Click here to expand...](#)

# CVE-2022-26520

Vulnerability 2 Manual fix

Discovered 8 days ago

in dependency postgresql (Maven)

## CWE

No information - CVE-2022-26520 is not listed with a CWE-ID number

## NVD

**\*\* DISPUTED \*\*** In pgjdbc before 42.3.3, an attacker (who controls the jdbc URL or properties) can call java.util.logging.FileHandler to write to arbitrary files through the loggerFile and loggerLevel connection properties. An example situation is that an attacker could create an executable JSP file ... [Read more](#)

## GitHub

Path traversal in org.postgresql:postgresql **\*\* DISPUTED \*\*** In pgjdbc before 42.3.3, an attacker (who controls the jdbc URL or properties) can call java.util.logging.FileHandler to write to arbitrary files through the loggerFile and loggerLevel connection properties. An example situation is that an ... [Read more](#)

9.8

CVSS3 Critical

7.5

CVSS2 High

## Actions

Set review status for fosslight

Mark as unaffected
  Flag as vulnerable
  Pause rule triggering

Fix vulnerability

**1** direct dependency to update [Open pull request](#)

[Full fix details >](#)

Introduced through **1** direct dependency to update

build.gradle 1 file

`org.postgresql:postgresql` ✖ 42.2.19 > ✔ 42.3.3 [View in file](#)

Vulnerable dependency postgresql (Maven)



**3** Get Started

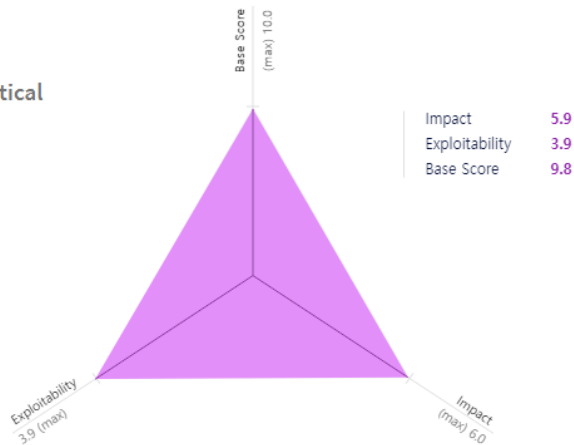
## CVSS Details [About CVSS](#)

**CVSS2** **7.5** High

Attack Vector	Network
Attack Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity	Partial
Availability	Partial

**CVSS3** **9.8** Critical

Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High



References 📄 About references

Path traversal in org.postgresql:postgresql · CVE-2022-26520 🔗  
· GitHub Advisory Database · GitHub

[Source](#) [Manual fix](#) [Github.com](#)

NVD - CVE-2022-26520 🔗

[Source](#) [Manual fix](#) [Nvd.nist.gov](#)

Arbitrary File Write Vulnerability · Advisory · pgjdbc/pgjdbc · 🔗  
GitHub

[Github.com](#)

Tomcat setup 🔗

[Jdbc.postgresqlOrg](#)

PostgreSQL JDBC Changelog 🔗

[Jdbc.postgresqlOrg](#)

fix javadocs by davecramer · Pull Request #2454 · 🔗  
pgjdbc/pgjdbc · GitHub

[Github.com](#)

[Show more](#) ▼

- Vulnerability ID를 클릭하면 특정 vulnerability에 대한 상세 정보를 얻을 수 있음
- 심각도에 대한 요약과 함께 NVD, Github와 같은 권고 사항에 대한 링크를 제공함
- Vulnerability가 도입된 위치가 나와 있음. Vulnerability가 발견된 파일과 Vulnerability가 도입된 Dependency를 보여줌
- Vulnerable dependency에서 취약성이 발견될 경우 안전한 버전을 표시함
- CVSS 점수 내역이 표시되고 가능한 경우 CVSS2 및 CVSS3 점수를 모두 표시하지만 CVSS3가 선호되어야 함
- Issue tracker의 문서 뿐만 아니라 문제 해결, 패치, 실제 exploit에 대한 정보를 찾을 수 있는 외부 참조 목록을 제공함

### Vulnerabilities view

모든 스캔된 repository에서 발견된 vulnerability 정보를 볼 수 있음

[Click here to expand...](#)

debricked
FREE

Overview
82%

Repositories

Vulnerabilities

Dependencies

Licenses

Open Source Select

Automations

Repository Settings

Admin tools

Upgrade to premium

to get unlimited scans, exportable reports and more

1000 scans left

Vulnerabilities
>

Generate report

Vulnerabilities

Latest scan 18 hours ago

+ Invite users

All

Filter 15 entries

Filter 15 entries

Name	Discovered	CVSS	Dependencies	Review status
CVE-2021-32671	18 hours ago	10 <span style="color: red;">🔴</span>	core (npm)	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2018-14721	18 hours ago	10 <span style="color: red;">🔴</span>	com.fasterxml.Jackson.core:jackson-databind (Maven)	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-39382	18 hours ago	9.8 <span style="color: red;">🔴</span>	core (npm)	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-31692	2022-11-23	9.8 <span style="color: red;">🔴</span>	org.springframework.security:spring-security-core (Maven)	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-2421	18 hours ago	9.8 <span style="color: red;">🔴</span>	socket.io-parser (npm)	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-41711	18 hours ago	9.8 <span style="color: red;">🔴</span>	core (npm)	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-39322	18 hours ago	9.8 <span style="color: red;">🔴</span>	core (npm)	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-37601	18 hours ago	9.8 <span style="color: red;">🔴</span>	loader-utils (npm)	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-38352	18 hours ago	9.8 <span style="color: red;">🔴</span>	framework (Composer)	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-33107	18 hours ago	9.8 <span style="color: red;">🔴</span>	framework (Composer)	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-21829	18 hours ago	9.8 <span style="color: red;">🔴</span>	core (npm) <span style="border: 1px solid #ccc; padding: 2px 5px; font-size: 0.7em;">+2</span>	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-29777	18 hours ago	9.8 <span style="color: red;">🔴</span>	core (npm) <span style="border: 1px solid #ccc; padding: 2px 5px; font-size: 0.7em;">+1</span>	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-29776	18 hours ago	9.8 <span style="color: red;">🔴</span>	core (npm) <span style="border: 1px solid #ccc; padding: 2px 5px; font-size: 0.7em;">+1</span>	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0
CVE-2022-21831	18 hours ago	9.8 <span style="color: red;">🔴</span>	activestorage (RubyGems)	<span style="color: red;">🔴</span> 0 <span style="color: orange;">🟡</span> 1 <span style="color: green;">🟢</span> 0 <span style="color: gray;">⊖</span> 0

- Debricked에서 사용되는 Security관련 상세 내용은 <https://debricked.com/docs/security/security-about.html> 참조

collab.lge.com/main/display/OSC/Debricked

6/11

## Dependency view

Indirect dependency를 포함하여 import 된 모든 dependency에 대한 개요를 볼 수 있음

[Click here to expand...](#)

debricked FREE
+ Invite users

- Overview BETA
- Repositories
- Vulnerabilities
- Dependencies
- Licenses
- Open Source Select
- Automations
- Repository Settings
- Admin tools

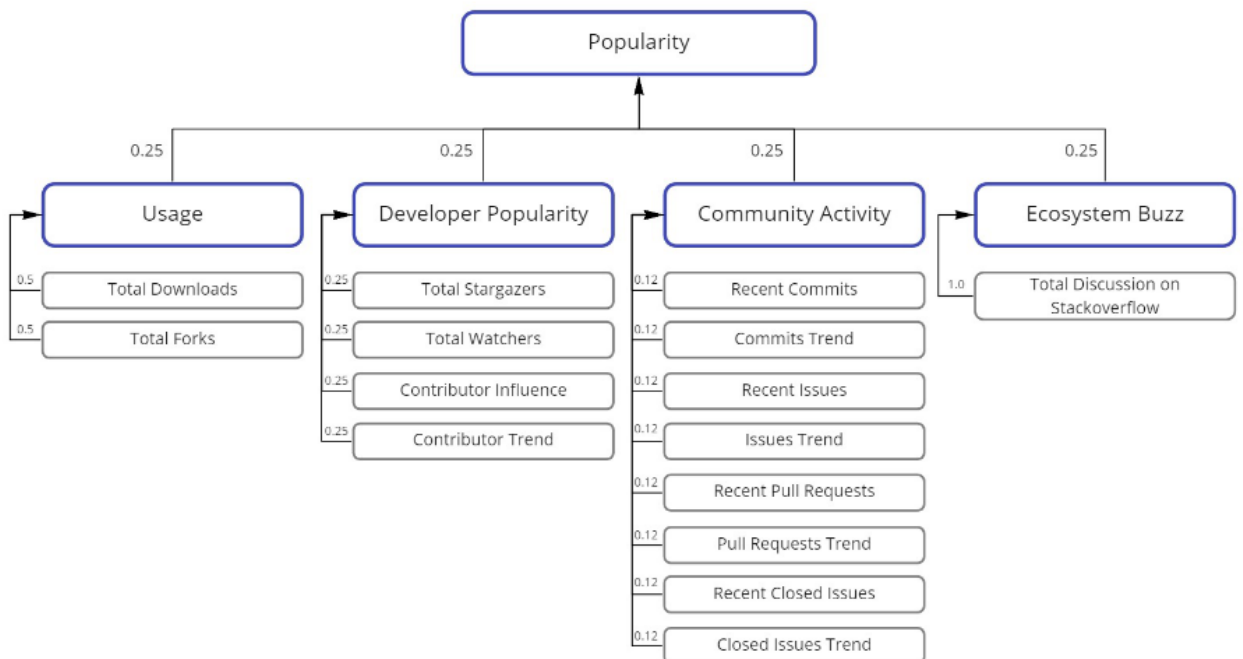
Upgrade to premium  
to get unlimited scans,  
exportable reports and more

1000 scans left

All
Expand all  15 entries ⚙️

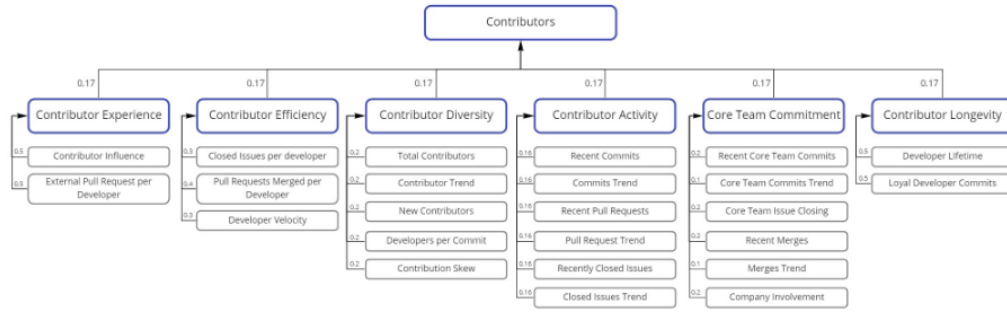
Name	Total vulnerabilities	Vulnerability priority	Review status	Licenses	Health Scores
@actions/core (npm)	0 / 109 of 109	C: 19 H: 25	0 109 0 0		P:69 C:60
org.activitiactiviti-bpmn-model...	4 / 0 of 64	C: 0 H: 0	0 0 0 0	Apache-2.0	P:0.0 C:0.0
grunt-assemble (npm)	84 / 0 of 48	C: 0 H: 0	0 0 0 0	MIT	P:32 C:27
npm2arch (npm)	172 / 0 of 37	C: 0 H: 0	0 0 0 0	MIT	P:16 C:19
@angular/core (npm)	1 / 34 of 34	C: 5 H: 5	0 34 0 0	MIT	P:74 C:72
grunt-contrib-imagemin (npm)	357 / 0 of 29	C: 0 H: 0	0 0 0 0	MIT	P:41 C:29
grunt-critical (npm)	349 / 0 of 27	C: 0 H: 0	0 0 0 0	MIT	P:55 C:47
karma (npm)	219 / 2 of 24	C: 0 H: 0	0 2 0 0	MIT	P:78 C:57
grunt-google-cdn (npm)	124 / 0 of 24	C: 0 H: 0	0 0 0 0	Debricked Unknown License	P:39 C:29
actionpack (RubyGems)	0 / 24	C: 0 H: 4	0 24 0 0	MIT	P:78 C:71
django (pip)	0 / 23	C: 2 H: 5	0 23 0 0	Debricked Unknown License	P:81 C:72
grunt-contrib-nodeunit (npm)	389 / 0 of 23	C: 0 H: 0	0 0 0 0	MIT	P:36 C:45
npm (npm)	128 / 7 of 20	C: 0 H: 3	0 7 0 0	BSD-2-Clause, ISC	P:73 C:73
grunt (npm)	102 / 3 of 19	C: 0 H: 2	0 3 0 0	MIT	P:68 C:47
tap (npm)	150 / 1 of 19	C: 0 H: 1	0 1 0 0	ISC	P:61 C:43

- Vulnerability priority:** dependency의 CVSS score 분포를 보여줌
  - Review status:** *vulnerable, unexamined, unaffected.*
  - Licenses:** dependency의 License
  - Popularity:** dependency의 popularity score
    - popularity score는 개발자와 사용자 모두의 관심을 나타내며, 생존 가능성과 지속적인 개발을 가리킴
- [Click here to expand...](#)



- Contributors:** dependency의 contributor score
  - contributor score는 , Software에 적용할 Open Source를 결정할 때 프로젝트 기여자를 검사하고 분석한 결과를 점수화함

[Click here to expand...](#)



## License view

Debricked와 integration 된 repository의 모든 License를 보여줌

[Click here to expand...](#)

debricked FREE
Licenses >
Generate report

- Overview
- Repositories
- Vulnerabilities
- Dependencies
- Licenses
- Open Source Select
- Automations
- Repository Settings
- Admin tools

### Licenses

Latest scan 19 hours ago

All

Search by license name or repository 15 entries

Name	License Risk	Affected repositories	Dependencies	License family
0BSD	●1 ●0 ●0 ●0 ●0 ●0 ●0	scancode-toolkit	1	Permissive
Apache-1.1	●0 ●0 ●0 ●0 ●0 ●1 ●0	fosslight	1	Permissive
Apache-2.0	●1 ●0 ●0 ●0 ●0 ●2 ●0	scancode-toolkit +2	351	Permissive
Artistic-2.0	●1 ●0 ●0 ●0 ●0 ●0 ●0	scancode-toolkit	2	Weak copyleft
BSD-2-Clause	●1 ●0 ●0 ●0 ●0 ●2 ●0	scancode-toolkit +2	82	Permissive
BSD-3-Clause	●1 ●0 ●0 ●0 ●0 ●2 ●0	scancode-toolkit +2	131	Permissive
CC-BY-3.0	●1 ●0 ●0 ●0 ●0 ●0 ●0	scancode-toolkit	1	Permissive
CC-BY-4.0	●1 ●0 ●0 ●0 ●0 ●0 ●0	scancode-toolkit	2	Permissive
CC0-1.0	●1 ●0 ●0 ●0 ●0 ●1 ●0	scancode-toolkit +1	17	Permissive
CDDL-1.0	●1 ●0 ●0 ●0 ●0 ●1 ●0	scancode-toolkit +1	3	Weak copyleft
CDDL-1.1	●1 ●0 ●0 ●0 ●0 ●1 ●0	scancode-toolkit +1	2	Weak copyleft
Debricked Unknown License	●2 ●0 ●0 ●0 ●0 ●0 ●0	scancode-toolkit +1	76	Unknown
EPL-1.0	●1 ●0 ●0 ●0 ●0 ●1 ●0	scancode-toolkit +1	5	Weak copyleft
EPL-2.0	●1 ●0 ●0 ●0 ●0 ●1 ●0	fosslight +1	8	Weak copyleft

- **Risk**- 위험 수준에 따라 색상으로 6단계 구분 (repository 설정에 따라 동일한 License도 위험도가 다름)
- **Affected repositories** : License가 발견된 repository
- **Dependencies** : License의 영향을 받는 Dependency 수
- **License family** : License가 속한 type

### Risk details

- License와 관련된 잠재적인 규정 준수 위험을 평가하기 위해 신호등 등급 시스템을 사용함.
- 색깔은 일부 License가 다른 License 보다 더 위험하다는 것이 아닌 컴플라이언스 준수 문제의 예상 양과 복잡성을 나타냄

<b>RED</b>	Banned license High compliance risk not allowed Unknown license	<ul style="list-style-type: none"> <li>• 사용이 허용 되지 않은 License 임 ( 예- 가전에서 GPL-3.0 사용)</li> <li>• License 조건을 위반할 가능성이 높으므로 법적 문제에 노출될 수 있음</li> </ul>
------------	--	---



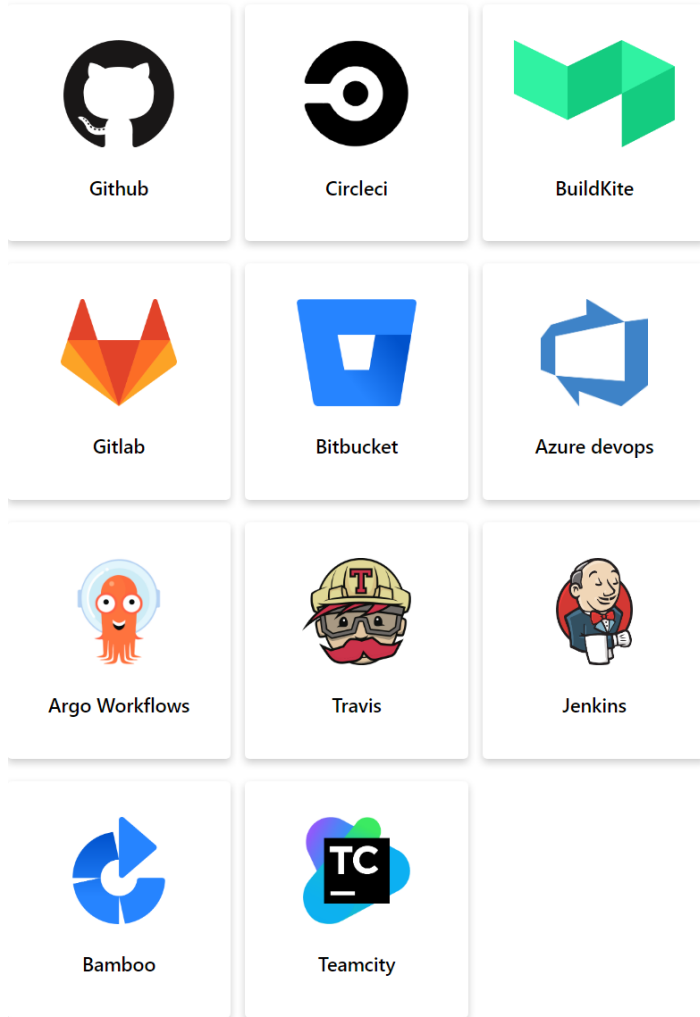
ORANGE	Restricted license	<ul style="list-style-type: none"> <li>• 상당한 위험성이 있는 제한된 License</li> <li>• 컴플라이언스 고려 사항은 일반적으로 완전히 준수하기 어렵기 때문에 법적 지침을 얻을 후 프로젝트 또는 사례별로 허용됨</li> </ul>
YELLOW	Approved license	<ul style="list-style-type: none"> <li>• Source Code 공개와 같이 상당한 컴플라이언스 준수 고려 사항이 있는 승인된 license는 공개적으로 사용 가능해야 하며, Copyleft license 제품군의 license와 마찬가지로 다른 license에 다른 코드와 결합하는데 제한이 있음</li> </ul>
GREEN	Approved license	<ul style="list-style-type: none"> <li>• 저작권 및 고지(permission notice)와 같은 준수 고려 사항이 거의 없는 승인된 license로 permissive license 제품이며 대부분의 license와 마찬가지로 코드 배포에서 유지되어야 함</li> </ul>
Blue	Non-OSS Commercial Proprietary license	

## Integration

### CI/build systems

- Debricked는 workflow에서 서비스를 쉽게 사용할 수 있도록 다양한 도구에 대한 여러 가지 Integration을 제공함
- 지원되는 CI/build systems

[Click here to expand...](#)



### CLI

- Common Line Tool (CLI)를 제공함
- 상세 내용은 <https://debricked.com/docs/integrations/cli.html> 참고

### Manual upload

- Repository 설정 뿐만 아니라, 파일을 별도로 업로드하여 분석할 수 있음

[Click here to expand...](#)

debricked **FREE** Repository Settings >

Overview BETA

Repositories

Vulnerabilities

Dependencies

Licenses

Open Source Select

Automations

**Repository Settings**

Admin tools

Upgrade to premium to get unlimited scans, exportable reports and more

1000 scans left

## Repository Settings

Latest scan 2 days ago

Repositories Commits

Search by name or commit

15 entries


Manual scan

New


Name	Automations	Use case	Integrations	GitHub App scanning
hyesung2/fossflight	4 rules	Non-distributed, network service	GitHub	<input type="checkbox"/>
hyesung2/fossflight_scanner	4 rules	Distributed, electronics	GitHub	<input type="checkbox"/>
hyesung2/scancode-toolkit	4 rules	Unknown	GitHub	<input type="checkbox"/>

### Language support


Language




C#




Go




Java & Kotlin




JavaScript




Objective-C & Swift




PHP




Python



Ruby



Rust



Linux package managers

## Dependency level of support

[Level of support](#)

\*Level of support:

1. Supports finding root dependencies only
2. Supports finding transitive/indirect dependencies
3. Supports finding all relations between dependencies (and visualizing as a dependency tree)

Language	Package Manager	File Format	Level of Support*
C#	NuGet	.csproj	3
		package.lock.json	3
packages.config		1	
	Paket	paket.lock	2
Go	Bazel	WORKSPACE	3
	Go Modules	go.mod	3
	Go Dep	gopkg.lock	1
Java	Bazel	WORKSPACE	3
	Gradle	build.gradle	3
		build.gradle.kts	3
	Maven	pom.xml	3
JavaScript	Bower	bower.json	3
	npm	package.json	3
		package-lock.json	3
	Yarn	package.json	3
		yarn.lock	3
Objective-C	Cocoapods	podfile.lock	2
PHP	Composer	composer.json	2
		composer.lock	2
Python	pip	requirements.txt	2
	Pipenv	Pipfile	2
		Pipfile.lock	2
Ruby	RubyGems	Gemfile.lock	2
Rust	Cargo	Cargo.lock	2
Swift	Cocoapods	podfile.lock	2