Google I/O Extended

패키지 취약성 관리

with Go and deps.dev API

@당근마켓 / 한국외국어대학교 이태현(Walter)

https://bit.ly/3Y1zb0y

Google I/O Extended

발표 소개

Introduction

Introduction

Build more secure apps with Go and Google

Introduction

01

패키지 취약성

- 소프트웨어 공급망
- 소프트웨어 공급망 공격
- 패키지 취약성

02

govulncheck

- Go 언어의 패키지 관리
- **govulncheck** 패키지 활용법

03

deps.dev API

- 오픈 소스 인사이트(Open Source Insight)
- deps.dev API

Google I/O Extended

패키지 취약성

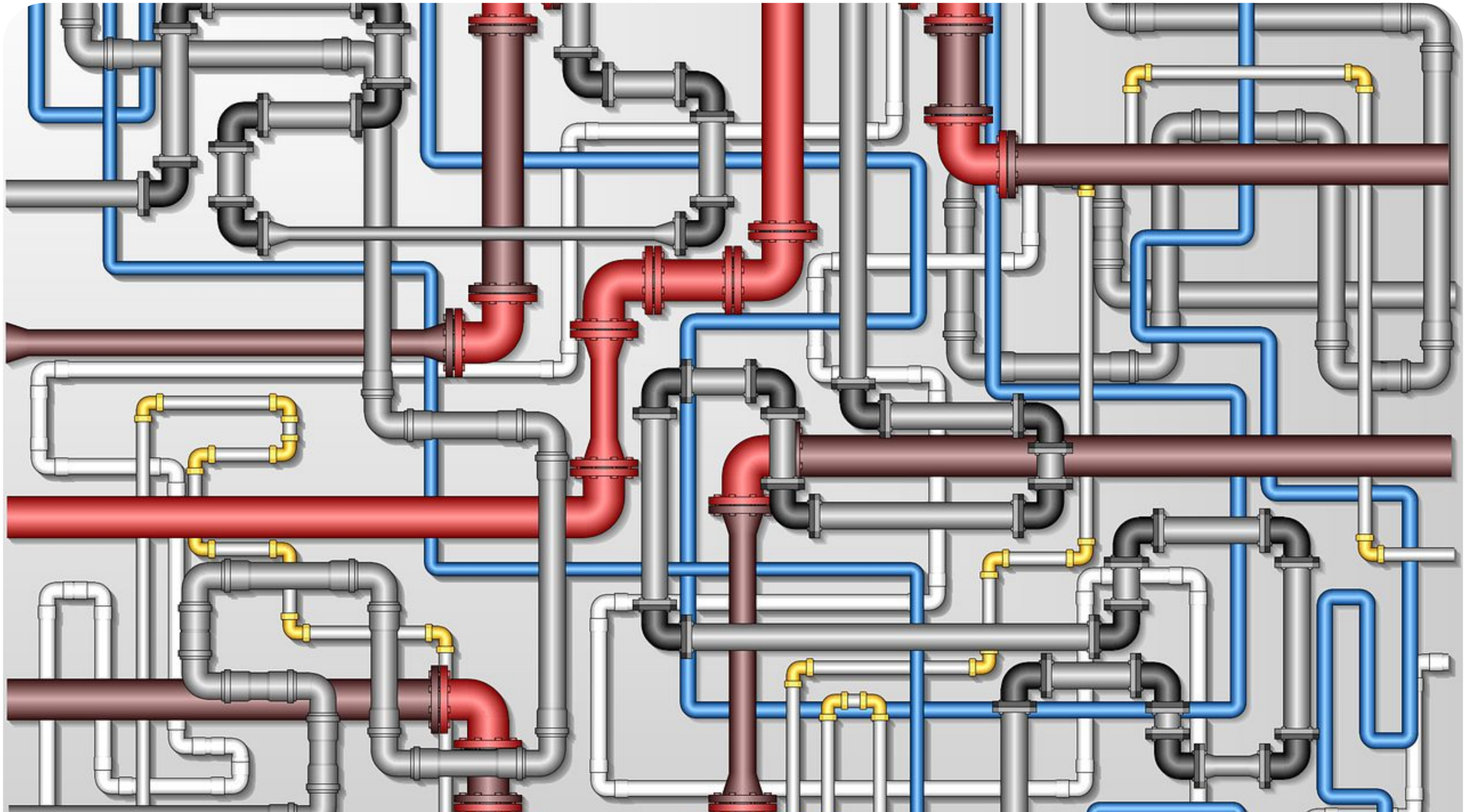
Package Vulnerability

Package Vulnerability

Software Supply Chain

소프트웨어 공급망
Software Supply Chain

파이프라인(Pipeline)



“ 애플리케이션 개발에서 배포까지
소프트웨어 개발 라이프 사이클에서
코드를 수정하는 모든 사용자와 요소 ”

Red Hat

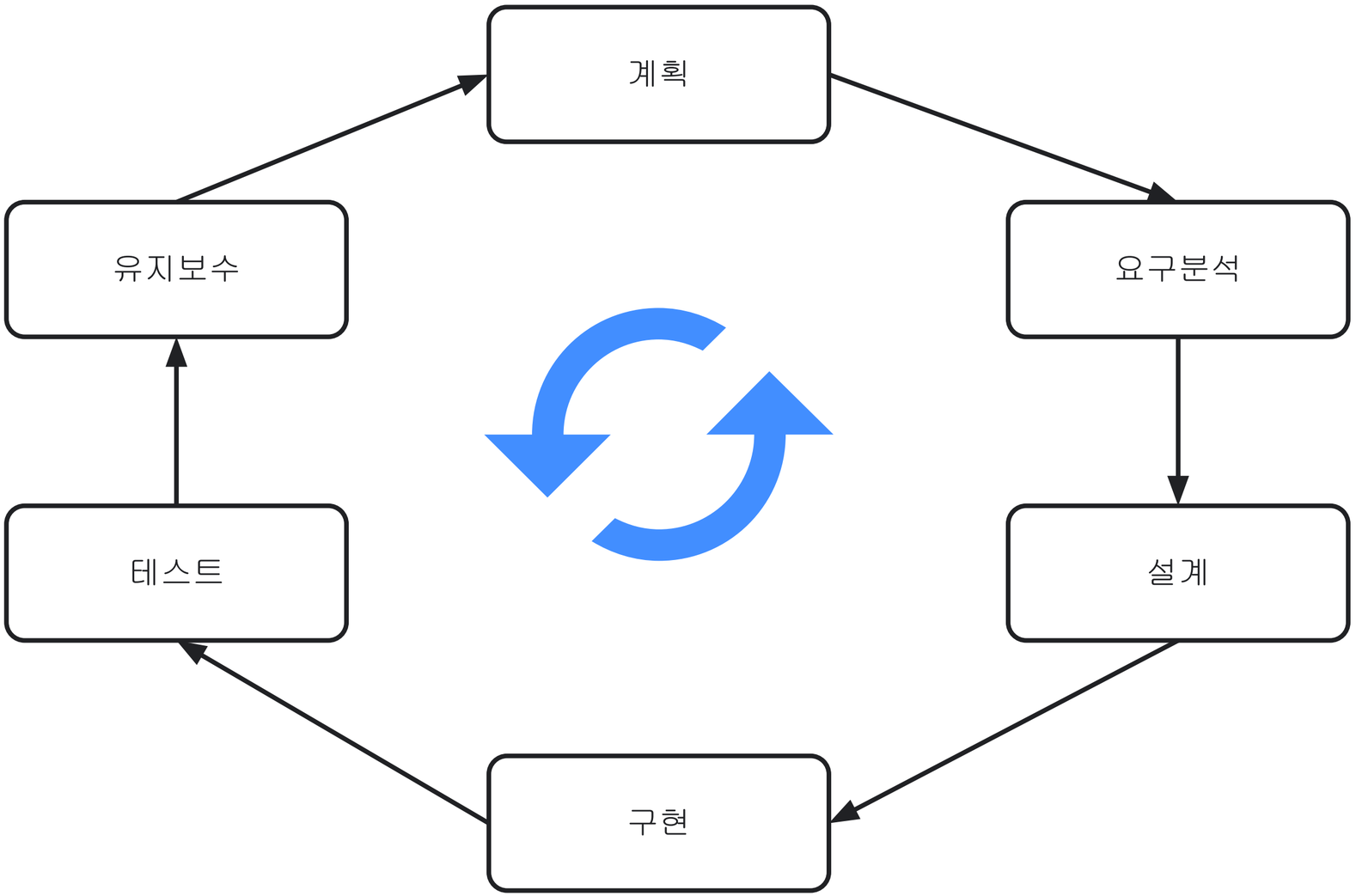
“ 애플리케이션 개발에서 배포까지
소프트웨어 개발 라이프 사이클에서
코드를 수정하는 모든 사용자와 요소 ”

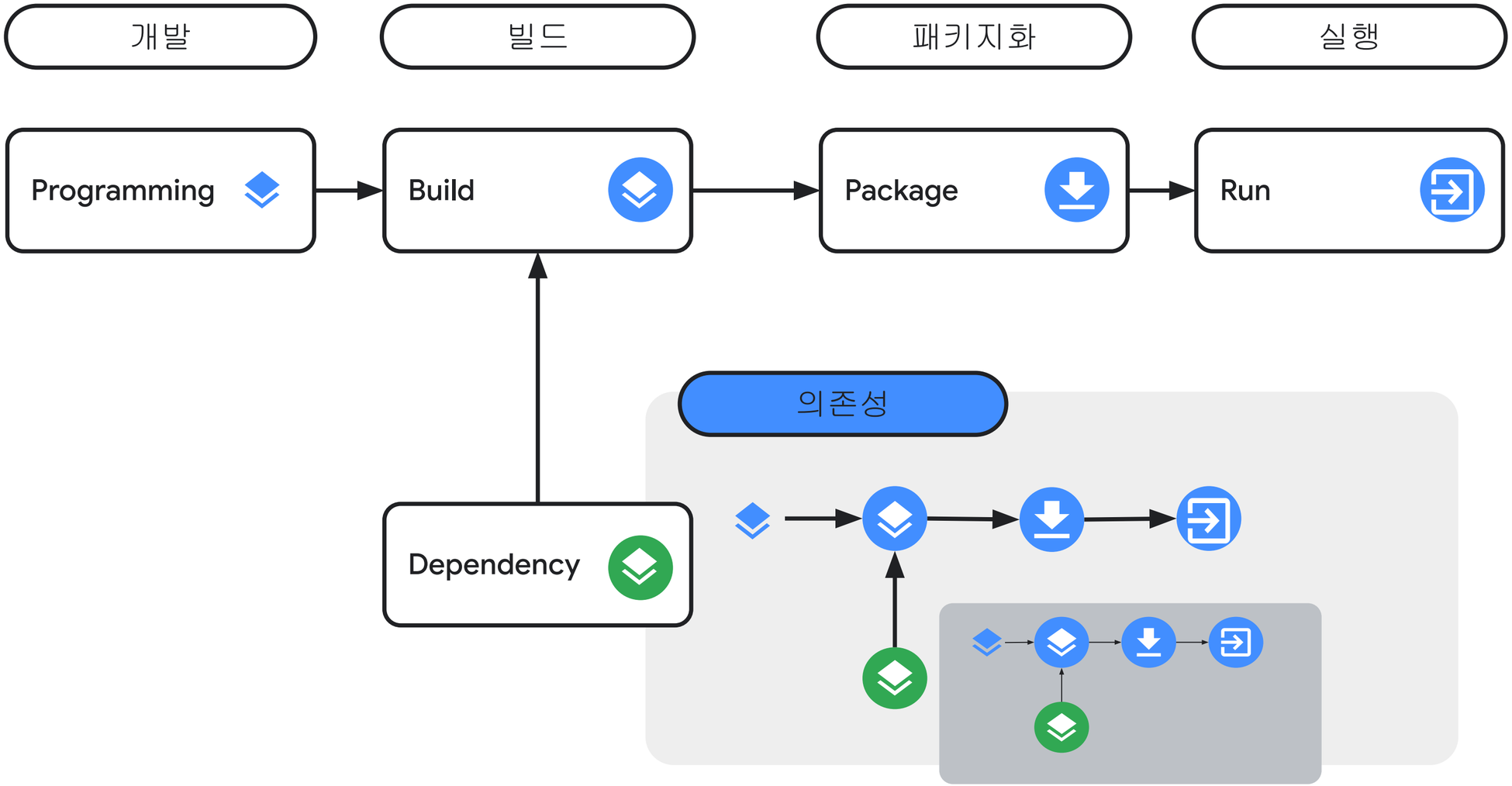
Red Hat

Software Development Life Cycle

소프트웨어 개발 생명 주기

SDLC: Software Development Life Cycle

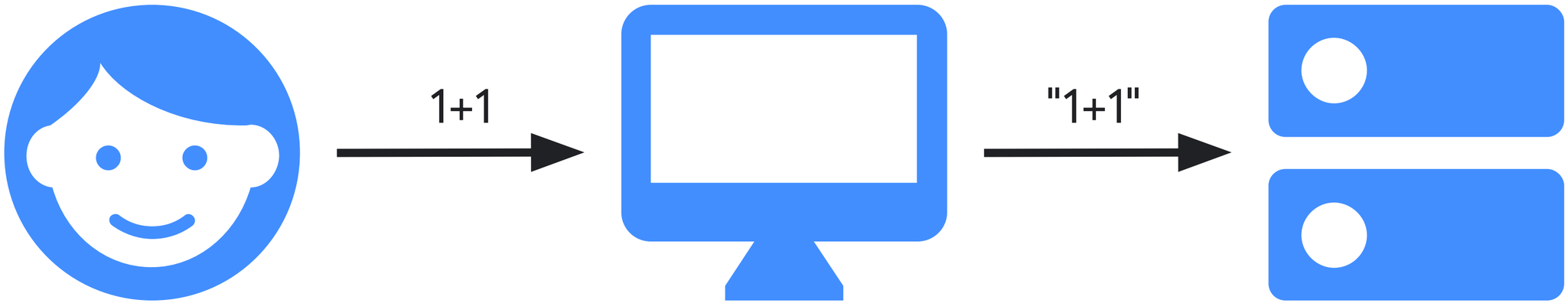

계획
요구분석
설계
구현
테스트
유지보수


개발
빌드
패키지화
실행
Programming
Build
Package
Run
Dependency
의존성

Software Supply Chain

소프트웨어 공급망 공격
Software Supply Chain Attack

2021년 12월 9일 Log4j 보안 취약점 사태


1+1
"1+1"

LOG4J

35,000

“ More than 35,000 Java packages impacted by Log4j Vulnerabilities ”

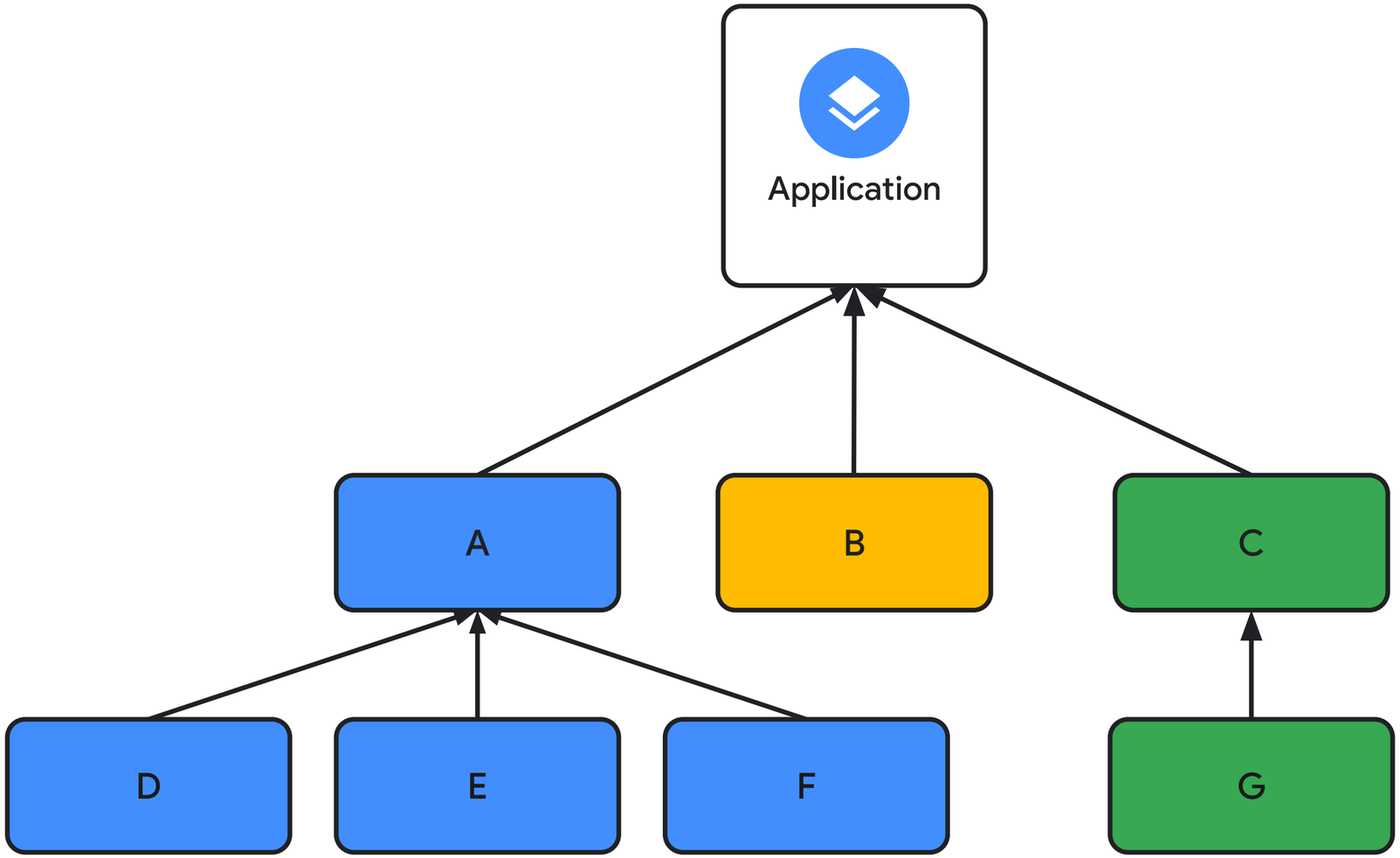
Google

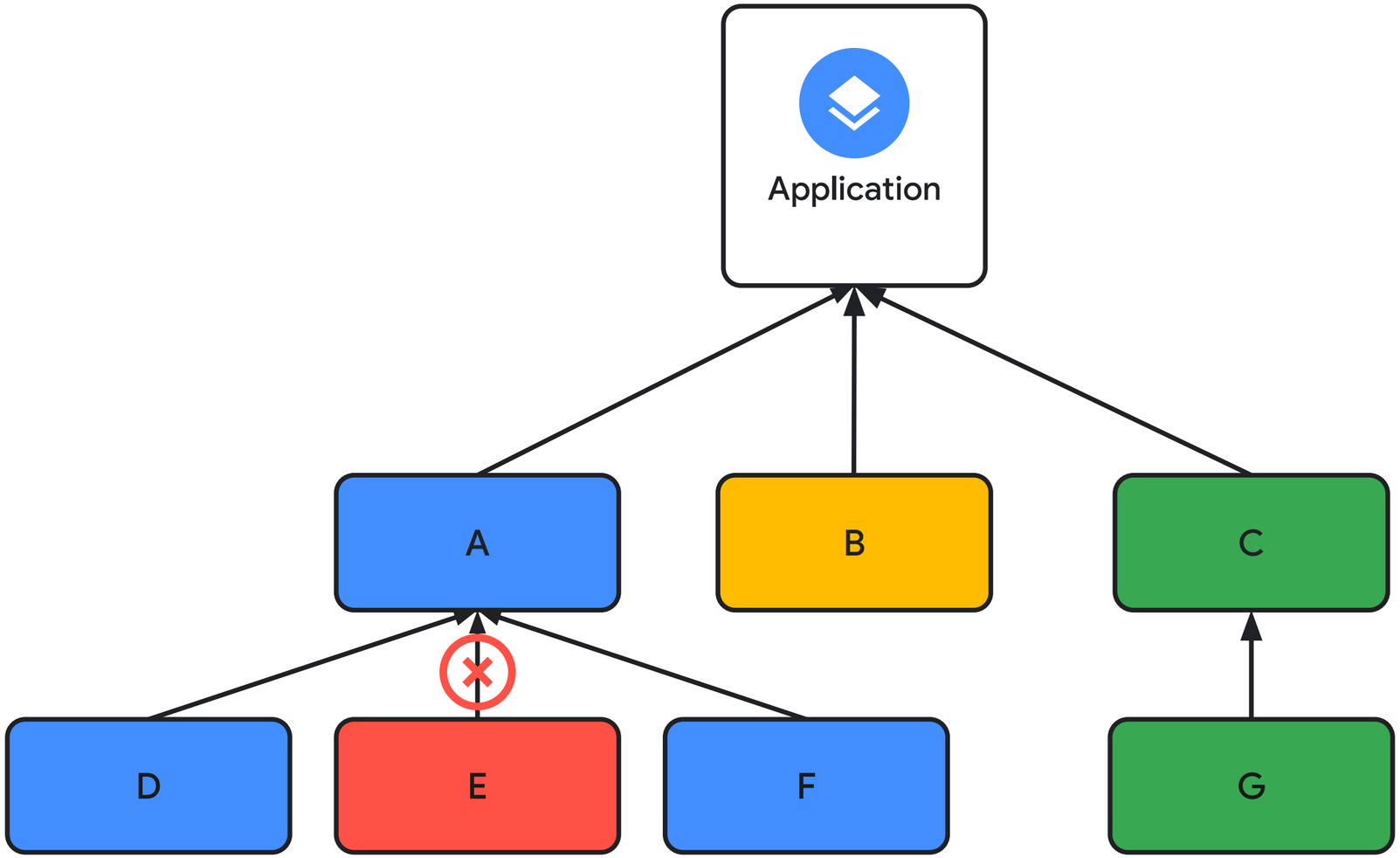
Package Vulnerability

패키지 취약성
Package Vulnerability

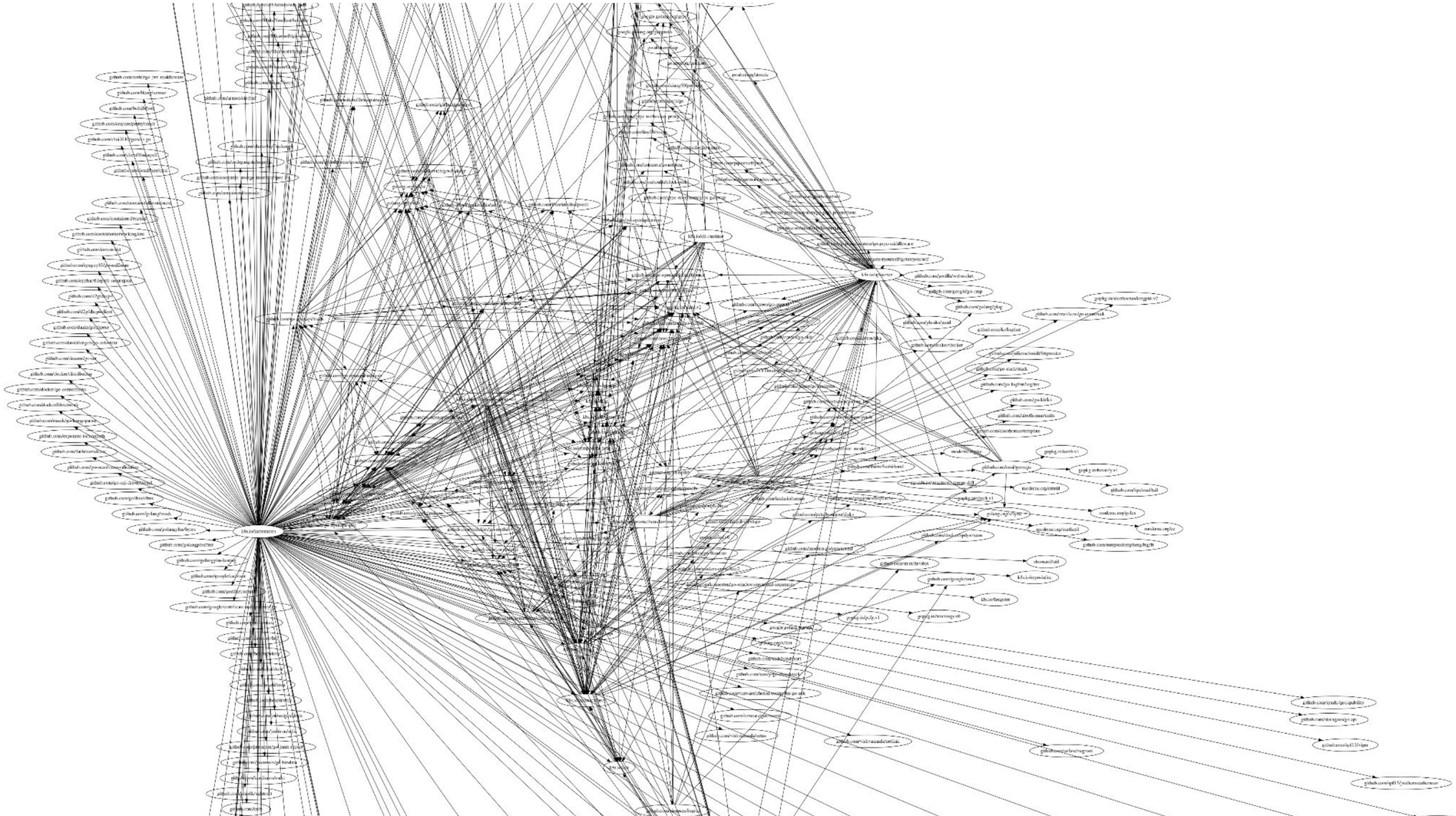
“ 바퀴를 다시 발명하지 마라 ”

“ Do not reinvent the wheel ”


Application
A
B
C
D
E
F
G


Application
A
B
C
D
E
F
G

Kubernetes Dependency Graph



Google I/O Extended

Go 언어의 패키지 관리

Package Management in Go

Package Management in Go

go.mod 파일과 go.sum 파일

Package Management in Go

패키지 해시값 관리

go.mod 파일과 **go.sum** 파일

패키지 리스트 관리

go.mod

```
require (
  github.com/gin-gonic/gin v1.1.4 //  indirect
  github.com/golang/protobuf v1.5.3 //  indirect
  github.com/mattn/go-isatty v0.0.19 //  indirect
  golang.org/x/net v0.12.0 //  indirect
  golang.org/x/sys v0.10.0 //  indirect
  google.golang.org/protobuf v1.31.0 //  indirect
  gopkg.in/go-playground/validator.v8 v8.18.2 //  indirect
  gopkg.in/yaml.v2 v2.4.0 //  indirect
)
```

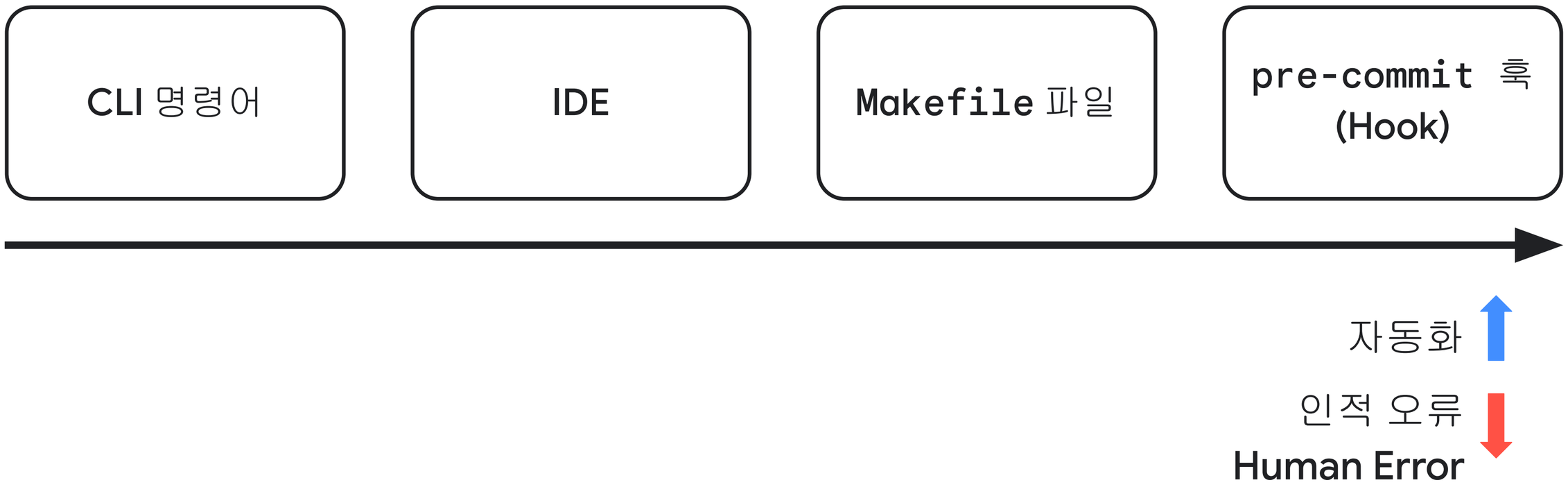
go.sum

```
github.com/gin-gonic/gin v1.1.4 h1:XLaCFbU39SSGRQr...
github.com/gin-gonic/gin v1.1.4/go.mod h1:7cKuhb...
github.com/golang/protobuf v1.5.0/go.mod h1:FsONVRA...
github.com/golang/protobuf v1.5.3 h1:KhyjKVUg...
github.com/golang/protobuf v1.5.3/go.mod h1:XVQd3VN...
```

govulncheck

govulncheck 패키지 활용

Package Management in Go



Package Management in Go

CLI 명령어

Command Line Interface

```
$ govulncheck .

Vulnerability #2: GO-2021-0052
  Inconsistent interpretation of HTTP Requests in github.com/gin-gonic/gin
More info: https://pkg.go.dev/vuln/GO-2021-0052
Module: github.com/gin-gonic/gin
  Found in: github.com/gin-gonic/gin@v1.1.4
  Fixed in: github.com/gin-gonic/gin@v1.7.7
  Example traces found:
    #1: main.go:16:7: govulncheck.main calls gin.Engine.Run
```

```
$ govulncheck .

Vulnerability #2: GO-2021-0052
  Inconsistent interpretation of HTTP Requests in github.com/gin-gonic/gin
More info: https://pkg.go.dev/vuln/GO-2021-0052
Module: github.com/gin-gonic/gin
  Found in: github.com/gin-gonic/gin@v1.1.4
  Fixed in: github.com/gin-gonic/gin@v1.7.7
  Example traces found:
    #1: main.go:16:7: govulncheck.main calls gin.Engine.Run
```

main.go

```
func main() {
  r := gin.Default()
  r.Get("/ping", func(c *gin.Context) {
    c.JSON(http.StatusOK, gin.H{
      "message": "pong",
    })
  })
  r.Run()  //  main.go:16
}
```

Package Management in Go

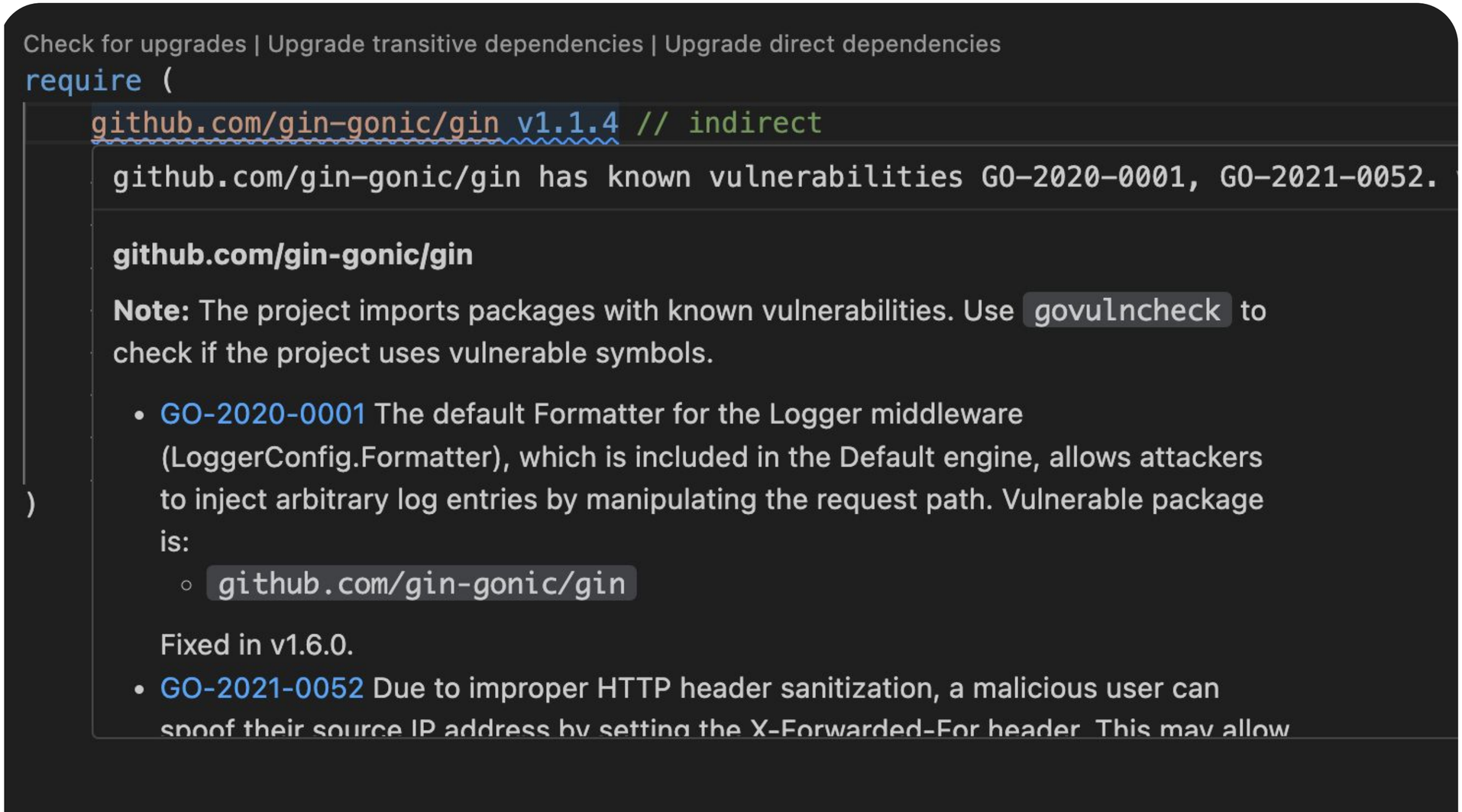
IDE

Integrated Development Environment

settings.json

```
{
  "go.diagnostic.vulncheck": "Imports",
  "gopls": {
    "codelenses": {
      "run_govulncheck": true,
    }
}
```

Visual Studio Code 설정



Package Management in Go

Makefile 파일

Makefile

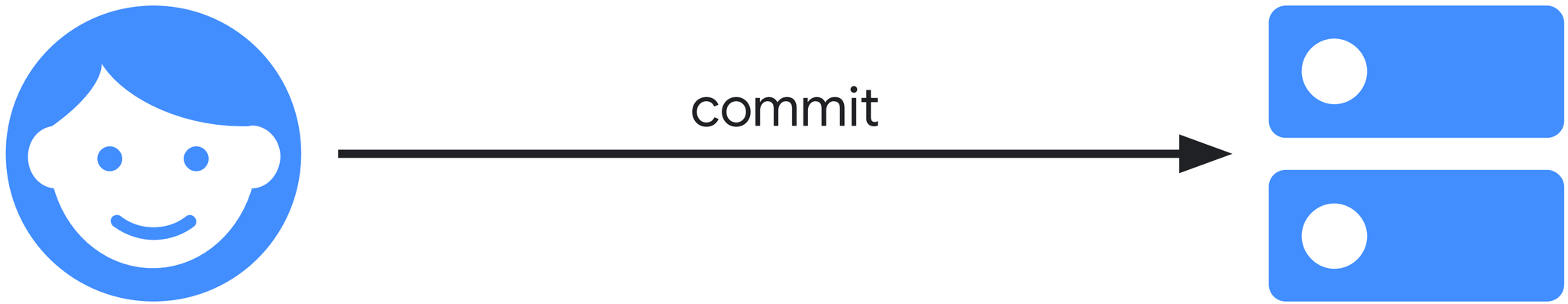
```
.PHONY: vuln-check
vuln-check:
  @govulncheck .

.PHONY: build
build:
  @make vuln-check && @go build -o test
```

Makefile

```
.PHONY: vuln-check
vuln-check:
  @govulncheck .

.PHONY: build
build:
  @make vuln-check && @go build -o test
```

```
$ make build

Vulnerability #2: GO-2021-0052
  Inconsistent interpretation of HTTP Requests in
github.com/gin-gonic/gin
More info: https://pkg.go.dev/vuln/GO-2021-0052
Module: github.com/gin-gonic/gin
  Found in: github.com/gin-gonic/gin@v1.1.4
  Fixed in: github.com/gin-gonic/gin@v1.7.7
  Example traces found:
    #1: main.go:16:7: govulncheck.main calls gin.Engine.Run
```

pre-commit 훅(Hook)


commit


pre-commit
commit

pre-commit.sh

```
#!/bin/sh

TARGET_DIRECTORY = $(find . -name go.mod -exec dirname {} \;)
cd $TARGET_DIRECTORY

govulncheck .

if [ $? -ne 0 ]; then
  echo "취약성 발견!"
  exit 1
fi
```

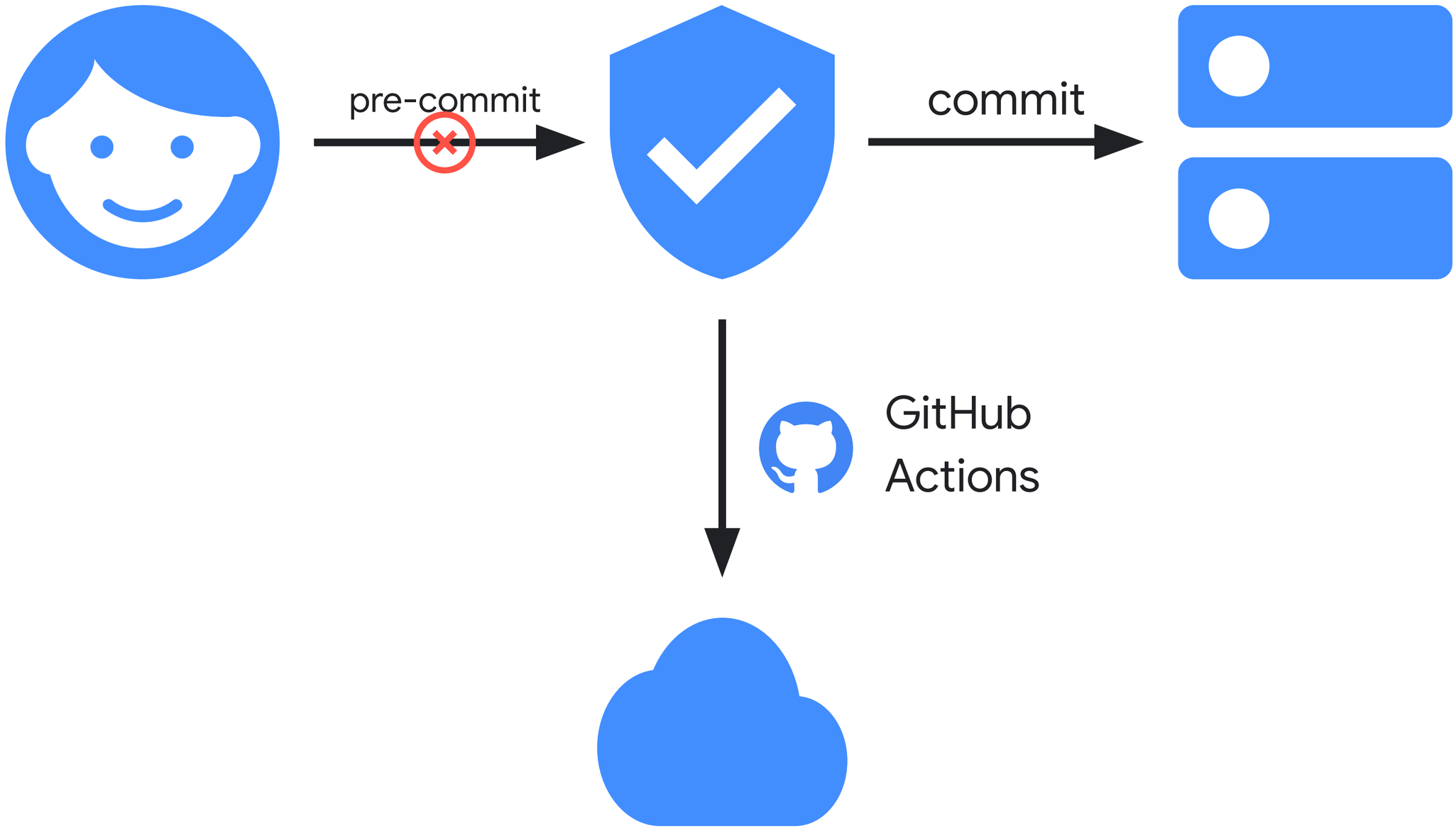
pre-commit.sh

```
#!/bin/sh

TARGET_DIRECTORY = $(find . -name go.mod -exec dirname {} \;)
cd $TARGET_DIRECTORY

govulncheck .

if [ $? -ne 0 ]; then
  echo "취약성 발견!"
  exit 1
fi
```

```
$ git commit -m "Initial commit"
```

"취약성 발견!"


pre-commit
commit


pre-commit
commit
GitHub
Actions

Google I/O Extended

Open Source Insight

Open Source Insight

Kubernetes v1.27.0 취약성

Overview Dependencies Dependents Compare Versions

Security Advisories

6

In this package

Kubernetes mountable secrets policy bypass
6.5 MODERATE · GHSA-cgcv-5272-97pr
MORE DETAILS

kube-apiserver vulnerable to policy bypass
6.5 MODERATE · GHSA-qc2g-gmh6-95p4
MORE DETAILS

Kubelet vulnerable to bypass of seccomp profile enforcement
4.4 MODERATE · GHSA-xc8m-28vv-4pjc
MORE DETAILS

In the dependencies

runc AppArmor bypass with symlinked /proc
6.1 MODERATE · GHSA-g2j6-57v7-gm8c
MORE DETAILS

deps.dev API

Overview

The deps.dev API provides access to Open Source Insights data. It can be used by tool builders, researchers, and tinkerers who want to answer questions like:

- What versions are available for this package?
- What are the licenses that cover this version of a package?
- How many dependencies does this package have? What are they?
- What versions of what packages correspond to this file?

The API can be accessed in two ways: as JSON over HTTP, which is described on this page, as well as via gRPC. For more information about accessing the API via gRPC, please visit github.com/google/deps.dev.

```
$ pip install fastapi
$ pip freeze > requirements.txt
```

requirements.txt

```
fastapi==0.50.0
pydantic==1.10.11
starlette==0.13.2
typing_extensions==4.7.1
```

parser.py

```python
class TextfileParser:
  @staticmethod
  def parse_to_dictionary(file_path: str) -> list[Package]:
    packages_information: list[Package] = []

    with open(file=file_path) as file:
      packages: list[str] = file.read().strip().split("\n")

    for package in packages:
      name, version = package.split("==")
      packages_information.append(Package(name=name, version=version))
    return packages_information
```

Package Data Model

```
[
  {
    name: "fastapi",
    version: "0.05.0"
  },
  {
    name: "pydantic",
    version: "1.10.11"
  }
]
```

GetVersion API

```
def get_version(self,
  package_name: str,
  package_version: str
) -> GetVersionAPIResponse:
  return (
    self.session
    .get(url=...)
    .json()
  )
```

GetVersion

`GET /v3alpha/systems/{versionKey.system}/packages/{versionKey`

GetVersion returns information about a specific package version, including its known to affect it.

Example: `/v3alpha/systems/npm/packages/%40colors%2Fcolors/vers`

Path parameters

versionKey.system: string

The package management system containing the package.

Can be one of `GO`, `NPM`, `CARGO`, `MAVEN`, `PYPI`, `NUGET`

versionKey.name: string

The name of the package.

versionKey.version: string

The version of the package.

main.py

```
packages: list[Package] = TextfileParser.parse_to_dictionary()
client: OpenSourceInsightAPI = OpenSourceInsightAPI()

for package in packages:
  advisories: list[Advisory] = (
    client.get_version(package_name=..., package_version=...)
    .get("advisoryKeys")
  )
```

GetAdvisory API

```
def get_advisory(self,
  advisory_key: str
) -> GetAdvisioryAPIResponse:
  return (
    self.session
    .get(url=...)
    .json()
  )
```

GetAdvisory

`GET /v3alpha/advisories/{advisoryKey.id}`

GetAdvisory returns information about security advisories hosted by OSV.

Example: `/v3alpha/advisories/GHSA-2qrg-x229-3v8q`

Path parameters

advisoryKey.id: string

The OSV identifier for the security advisory.

Response

advisoryKey: object

The identifier for the security advisory. Note that this may differ from t
canonicalization.

advisoryKey.id: string

The OSV identifier for the security advisory.

main.py

```
_SAFE: int = 0

for advisory in advisories:
  advisory_information: GetAdvisioryAPIResponse = (
    client.get_advisiory(advisory_key_id=...)
  )
  score: int = advisory_information.get("cvss3Score")
  if score > _SAFE:
    print("취약성이 발견되었어요.")
```

```
$ python main.py

4개의 패키지에 대한 취약성 검증을 시작해요.
----------
fastapi 패키지의 0.50.0 버전에서 Cross-Site Request Forgery (CSRF) in
FastAPI 취약성이 발견 되었고, 취약성 점수는 8.2/10점이에요!

자세한 내용은 https://osv/dev/vulnerability/GHSH-8h2j-cgx8-6xv7을 방문하여
확인해주세요.
```

```
$ python main.py

4개의 패키지에 대한 취약성 검증을 시작해요.
----------
fastapi 패키지의 0.50.0 버전에서 Cross-Site Request Forgery (CSRF) in
FastAPI 취약성이 발견 되었고, 취약성 점수는 8.2/10점이에요!

자세한 내용은 https://osv/dev/vulnerability/GHSH-8h2j-cgx8-6xv7을 방문하여
확인해주세요.
```

CVE와 CVSS v3

advisoryKey.id: string

The OSV identifier for the security advisory.

url: string

The URL of the security advisory.

title: string

A brief human-readable description.

aliases[]: string[]

Other identifiers used for the advisory, including CVEs.

cvss3Score: number

The severity of the advisory as a CVSS v3 score in the range [0,10]. A higher score represents greater severity.

cvss3Vector: string

The severity of the advisory as a CVSS v3 vector string.

CVE와 CVSS v3

advisoryKey.id: string

The OSV identifier for the security advisory.

url: string

The URL of the security advisory.

title: string

A brief human-readable description.

aliases[]: string[]

Other identifiers used for the advisory, including CVEs.

cvss3Score: number

The severity of the advisory as a CVSS v3 score in the range [0,10]. A higher score represents greater severity.

cvss3Vector: string

The severity of the advisory as a CVSS v3 vector string.

Open Source Insight

CVE

Common Vulnerabilities and Exposure

Open Source Insight

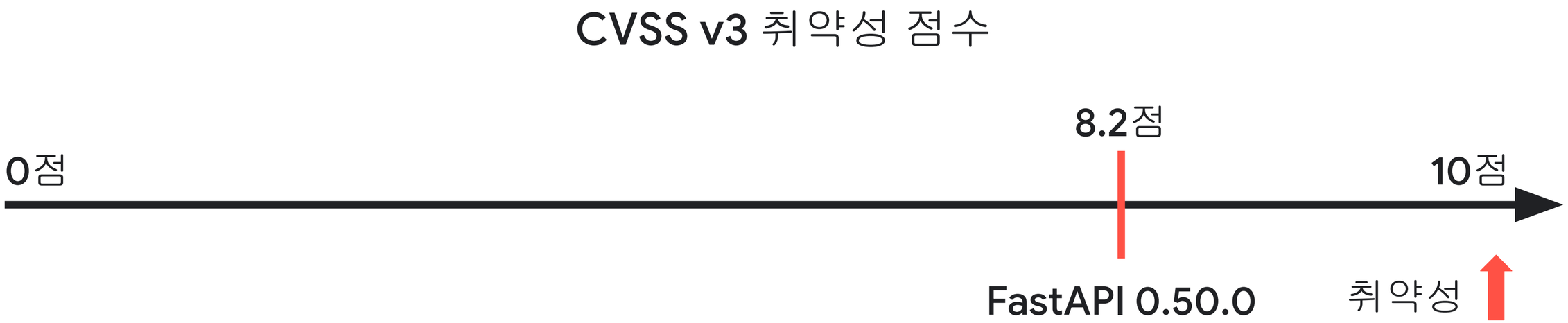
CVSS

Common Vulnerability Scoring System

Open Source Insight

CVSS v3 취약성 점수

Open Source Insight



```
$ python main.py

4개의 패키지에 대한 취약성 검증을 시작해요.
----------
fastapi 패키지의 0.50.0 버전에서 Cross-Site Request Forgery (CSRF) in
FastAPI 취약성이 발견 되었고, 취약성 점수는 8.2/10점이에요!

자세한 내용은 https://osv/dev/vulnerability/GHSH-8h2j-cgx8-6xv7을 방문하여
확인해주세요.
```

FastAPI v0.50.0 취약성

PyPI package

fastapi

0.50.0

Overview | Dependencies | Dependents | Compare | Versions

Security Advisories

2

In this package

PYSEC-2021-100

PYSEC-2021-100

MORE DETAILS

SIMILAR ADVISORIES

Cross-Site Request Forgery (CSRF) in FastAPI

8.2 HIGH · GHSA-8h2j-cgx8-6xv7

MORE DETAILS

In the dependencies

```
$ pip install --upgrade fastapi
$ pip freeze > requirements.txt
```

requirements.txt

```
anyio==3.7.1
fastapi==0.100.1
idna==3.4
pydantic==1.10.11
sniffio==1.3.0
starlette==0.27.0
typing_extensions==4.7.1
```

```
$ pip uninstall fastapi
$ pip freeze > requirements.txt
```

requirements.txt

```
pydantic==1.10.11
starlette==0.13.2
typing_extensions==4.7.1
```

FastAPI v0.50.0 의존성 취약성

In this package

PYSEC-2021-100
PYSEC-2021-100

MORE DETAILS

SIMILAR ADVISORIES

Cross-Site Request Forgery (CSRF) in FastAPI
8.2 HIGH · GHSA-8h2j-cgx8-6xv7

MORE DETAILS

In the dependencies

PYSEC-2023-48
PYSEC-2023-48

MORE DETAILS

SIMILAR ADVISORIES

MultipartParser denial of service with too many fields or files
MODERATE · GHSA-74m5-2c7w-9w3x

MORE DETAILS

Starlette allows an unauthenticated and remote attacker to specify any number of form fields or files
7.5 HIGH · GHSA-3qj8-93xh-pwh2

MORE DETAILS

Open Source Insight

Poetry 패키지 사용

```
$ poetry add fastapi

pyproject.toml

[tool.poetry.dependencies]
fastapi = "0.50.0"
```

```
$ poetry add fastapi

pyproject.toml

[tool.poetry.dependencies]
fastapi = "0.50.0"
```

```
poetry.lock

[[package]]
name = "fastapi"

[package.dependencies]
pydantic = ">=0.32.2,<2.0.0"
starlette = "0.13.2"
```

```
poetry.lock

[[package]]
name = "fastapi"

[package.dependencies]
pydantic = ">=0.32.2,<2.0.0"
starlette = "0.13.2"
```

```
$ poetry remove fastapi


- Removing fastapi (0.50.0)
- Removing pydantic (1.10.12)
- Removing starlette (0.13.2)
- Removing typing-extensions (4.7.1)
```

Google I/O Extended

결론

Conclusion

Conclusion

소프트웨어 공급망

- 소프트웨어 개발 생명 주기
- 소프트웨어 공급망
- 소프트웨어 공급망 공격

패키지 취약성

- **Log4j** 취약점 사태
- 의존성 그래프

Go 언어의 패키지 관리

- **go.mod** 파일의 패키지 의존성 관리
- **go.sum** 파일의 패키지 해시값 관리

govulncheck 활용법

- CLI 명령어
- IDE
- **Makefile** 파일
- **pre-commit** 훅(Hook)

Open Source Insight

- 패키지 검색 방법

deps.dev API

- API를 활용한 다른 프로그래밍 언어 활용