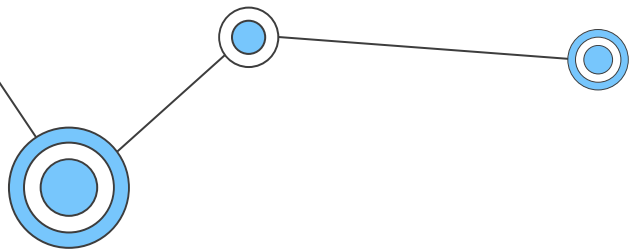




在你的DevOps 中加入一點 Security

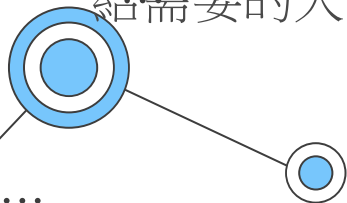
GitLab CI/CD with
Snyk



Barry Cheng

網創資訊
DevOps Team Lead

閒暇時會寫一些技術部落格
，幫助自己內化也可以分享
給需要的人



Agenda

01

Snyk公司簡介

02

Snyk四大產品

03

Snyk使用介紹

04

GitLab CI/CD





01

Snyk

公司簡介





Developers

2.5M

Employees

+600

Raised

\$470M

Founded in

2015

使用Snyk的公司

Google

aws

skyscanner

mongoDB


salesforce

intuit

New Relic

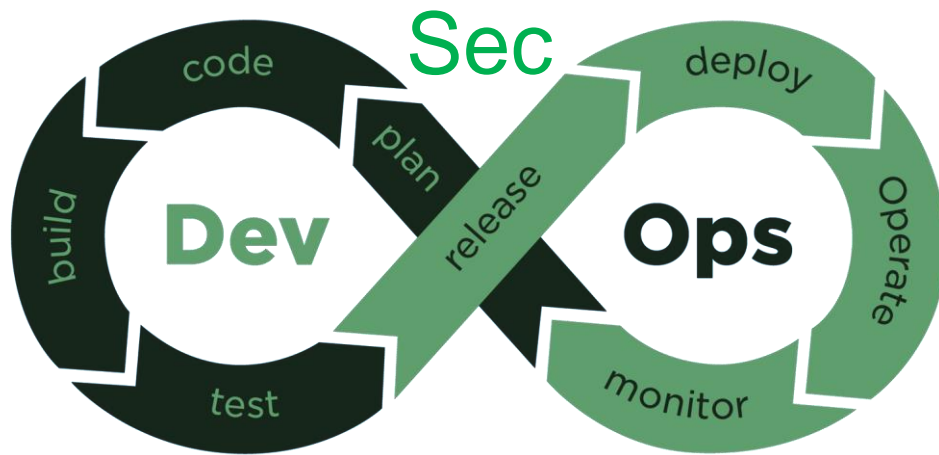
asurion

asos
discover fashion online



介紹 四大產品前...

Shift Left



81%

認為開發者需
要管理好程式
安全

33%

認為維護程式
安全是造成交
付延後的主因

02 Snyk

四大產品



Snyk四大產品

01

Snyk Code

確保寫出安全的Code

02

Snyk Open Source

預防有漏洞的相依套件

03

Snyk Container

確保base image與相依套件安全

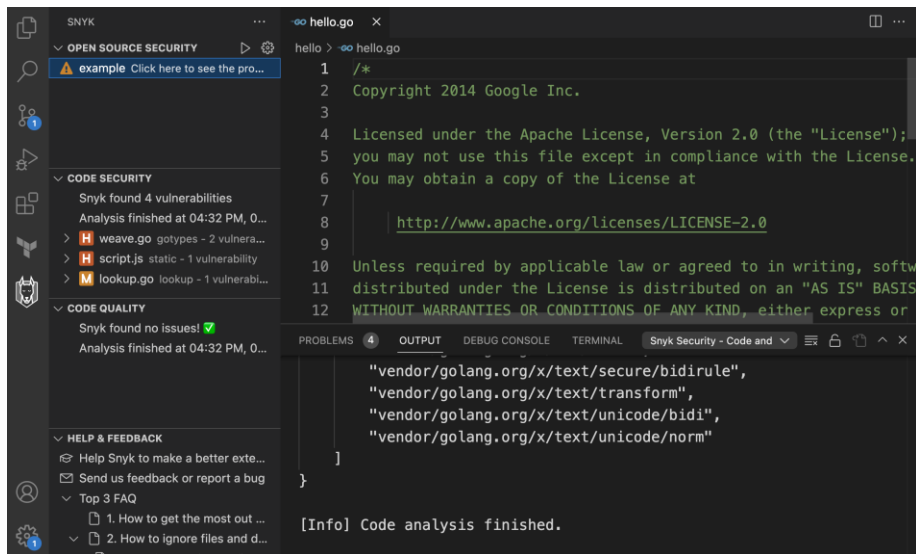
04

Snyk IaC

修正錯誤的Configuration

Snyk Code

- 靜態分析 SAST
- 開發者優先
- 整合IDE



Snyk Open Source

- Dependency tree
- Fix merge request

Issues 5 Fixes Dependencies 7							
<div><div></div><div>Search...</div><div><div></div><div></div></div></div>							
DEPENDENCY	LATEST	LAST PUBLISHED	ISSUES	LICENSES	COPYRIGHTS	PATHS	
bleach@3.0.0	5.0.1	2 months ago	0 C 1 H 3 M 0 L	Apache-2.0 license	© 2014-2017, Mozill...	1	
certifi@2022.6.15	2022.6.15	3 months ago	0 C 0 H 0 M 0 L	MPL-2.0 license	© 1999 Entrust.net ...	1	
pipenv@2022.8.31	2022.8.31	9 hours ago	0 C 0 H 0 M 0 L	MIT license	© 2020 Python...	1	
setuptools@39.0.1	65.3.0	8 days ago	0 C 0 H 0 M 0 L	MIT license	© 2016 Jason R Coorn...	1	
six@1.16.0	1.16.0	May 5, 2021	0 C 0 H 0 M 0 L	MIT license	© 2010-2020 Benjami...	1	
virtualenv-clone@0.5.7	0.5.7	a year ago	0 C 0 H 0 M 0 L	MIT license	© 2011, Edward Geor...	1	
webencodings@0.5.1	0.5.1	Apr 6, 2017	0 C 0 H 0 M 0 L	BSD-2-Clause license	© 2012 by Simon Sap...	1	

Snyk Container

- Base image版本建議

Recommendations for upgrading the base image

	BASE IMAGE	VULNERABILITIES	SEVERITY
Current image	node:12	605	6 C 35 H 35 M 529 L
Major upgrades	node:16.16.0	477	2 C 49 H 16 M 410 L
Alternative upgrades	node:14.20.0-bullseye-slim	44	1 C 0 H 0 M 43 L
	node:current-bullseye-slim	44	1 C 0 H 0 M 43 L
	node:18.7.0-buster-slim	70	1 C 1 H 0 M 68 L
	node:18.7.0-buster	474	2 C 47 H 15 M 410 L

Snyk IaC

- 支援多種格式
 - Terraform
 - CloudFormation
 - Kubernetes YAML
 - ...
- 預防錯誤的設定產生

03

Snyk

使用介紹

SaaS

We use cookies to ensure you get the best experience on our website. [Read more →](#)



snyk

Products ▾

Resources ▾

Company ▾

Pricing

Log in

Book a demo

Sign up

Snyk Cloud, the industry's first developer-centric cloud security solution →

Developer loved, Security trusted.

Find and automatically fix vulnerabilities in your code, open source dependencies, containers, and infrastructure as code — all powered by Snyk's industry-leading security intelligence.

Get started with a free forever account, and scale up if needed.

Start free

Book a demo →



→ snyk test

Testing /Users/goooddog/projects/woof...

Tested 3 dependencies for known issues, found 2 vulnerabilities

x Remote Code Execution (RCE) [Critical Severity] in log4j-core@2.14.1 introduced by io.goooddog:woof@0.0.1

This issue was fixed in versions: 2.3.1,

x Remote Code Execution (RCE) [Critical Severity] in log4j-core@2.14.1 introduced by io.goooddog:woof@0.0.1

This issue was fixed in versions: 2.3.1,

Package manager: maven

Target file: pom.xml

Project name: io.goooddog:woof

WARNING: Critical severity vulnerabilities were found with Log4j.

- SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720 (See <https://snyk.io/vuln/SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720>)

JAVA-ORGAPACHELOGGINGLOG4J-2314720)

We highly recommend fixing this vulnerability. If it cannot be fixed by upgrading, see mitigation information here:

- <https://security.snyk.io/vuln/SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720>

- <https://snyk.io/blog/log4shell-remediation-cheat-sheet/>

Patch the Dog from Snyk

Woof! I'm Patch! How can I help you today?

I have a question about open source vulnerabilities

I have a question about code vulnerabilities



I have a question about cloud security

I have a technical support question





I need something else

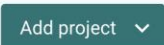



Dashboard

snyk  **BarrtTest** 


Dashboard Reports Projects Integrations Members

   **B** 


Vulnerable projects 

 **barrttest**
barrytest1/gitlabci(master):Dockerfile

6 **C** 36 **H** 37 **M** 526 **L** updated a day ago [Fix vulnerabilities](#)

 **barrttest**
barrytest1/gitlabci(master):requirements.txt

0 **C** 1 **H** 4 **M** 0 **L** updated 11 hours ago [Fix vulnerabilities](#)

 **barrttest**
barrytest1/gitlabci(master):k8s.yaml

0 **C** 0 **H** 3 **M** 5 **L** updated 7 days ago

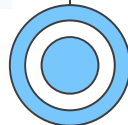
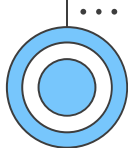
Current security issues

CRITICAL SEVERITY
6

HIGH SEVERITY
37

MEDIUM SEVERITY
43

LOW SEVERITY
531



Issues

Issues 605

Dependencies 413

🔍

Search...

605 of 605 issues

Sort by highest priority score ▾

ISSUE TYPE

☐ Vulnerabilities 605

☐ License issues 0

SEVERITY

☐ Critical 6

☐ High 36

☐ Medium 37

☐ Low 526

PRIORITY SCORE

Scored between 0 - 1000

FIXABILITY

☐ Fixable 0

☐ Partially fixable 5

☐ No fix available 600

EXPLOIT MATURITY

☐ Mature 7

☐ Proof of concept 0

☐ No known exploit 598

☐ No data 0

STATUS

☒ Open 605

☐ Patched 0

☐ Ignored 0

OS BINARIES

☐ OS packages 6

☐ Node 6

C

dpkg/libdpkg-perl - Directory Traversal

VULNERABILITY | CVE-2022-1664 ^u | CVSS 9.8 ^u **CRITICAL** | SNYK-DEBIAN9-DPKG-2847943 ^u

Introduced through

dpkg/libdpkg-perl@1.18.25, dpkg/dpkg-dev@1.18.25 and others

Exploit maturity

NO KNOWN EXPLOIT

Fixed in

dpkg/libdpkg-perl@1.18.26

Show more detail ▾

Ignore

C

openssl/libssl1.1 - OS Command Injection

VULNERABILITY | CVE-2022-1292 ^u | CVSS 9.8 ^u **CRITICAL** | SNYK-DEBIAN9-OPENSSL-2807589 ^u

Introduced through

openssl/libssl1.1@1.1.0-i-1--deb9u5, openssl/libssl-dev@1.1.0-i-1--deb9u5 and others

Exploit maturity

NO KNOWN EXPLOIT

Fixed in

openssl/libssl1.1@1.1.0-i-1--deb9u6

Show more detail ▾

Ignore

H

imagemagick/libmagickwand-dev - Buffer Overflow

VULNERABILITY | CVE-2022-28463 ^u | CVSS 7.8 ^u **HIGH** | SNYK-DEBIAN9-IMAGEMAGICK-2812517 ^u

Introduced through

imagemagick/libmagickwand-dev@8.6.9.7.4+dfsg-11+deb9u13, imagemagick/libmagickwand-6.q16-dev@8.6.9.7.4+dfsg-11+deb9u13 and others

Exploit maturity

NO KNOWN EXPLOIT

Fixed in

imagemagick/libmagickwand-dev@8.6.9.7.4+dfsg-11+deb9u14

Show more detail ▾

Ignore

Snyk Auth

- 瀏覽器授權
- API Token

```
snyk auth [API_TOKEN]
```

- 設定env: **SNYK_TOKEN**

API Token

Use this token when using our API for authentication. Learn more about our authentication API in [our docs](#).

For integrations such as with a CI tool, you can opt to use a [service account](#) for authentication instead.

KEY

CREATED

click to show

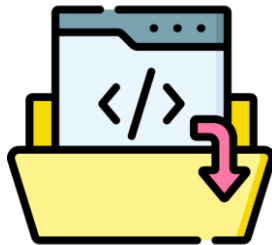
17 [REDACTED] 3

Revoke & Regenerate

Snyk Test



Code
snyk code test



Open Source
snyk test




Container
snyk container test




IaC
snyk iac test

Snyk Monitor








- 持續監控是否有新的漏洞

 node docker-image|node

 docker-image|node

Overview History Settings

Created Fri 13th May 2022 | Snapshot taken by recurring test 6 hours ago | [Retest now](#)

IMPORTED BY	PROJECT OWNER	SOURCE	TARGET OS
 barry.cheng@gaiatechs.com	 Add a project owner	 CI/CLI	debian:9
IMAGE ID	IMAGE TAG	BASE IMAGE	PLATFORM
ca29fbd37c91	12	node:12	linux/arm64
ENVIRONMENT	BUSINESS CRITICALITY	LIFECYCLE STAGE	TAGS
 Add a value	 Add a value	 Add a value	 Add a key/value...

Recommendations for upgrading the base image

	BASE IMAGE	VULNERABILITIES	SEVERITY
Current image	node:12	605	6 C 35 H 35 M 529 L
Major upgrades	node:16.16.0	470	3 C 45 H 13 M 409 L

Snyk Integrations



IDEs

Visual Studio Code,
IntelliJ



Git repository

GitHub, GitLab



CI/CD

Jenkins, CircleCI



Notification

Slack, Jira



Registries

Docker Hub, Harbor



Private Registries

Harbor

GitLab Integration

▼ SEVERITY

☐ Critical

0

☐ High

1

☐ Medium

3

☐ Low

0

▼ PRIORITY SCORE

Scored between 0 - 1000

▼ FIXABILITY

☐ Fixable

4

☐ Partially fixable

0

☐ No fix available

0

▼ EXPLOIT MATURITY

☐ Mature

0

☐ Proof of concept

2

☐ No known exploit

2

☐ ...

2

Search...

Fix these vulnerabilities

4 of 4 issues

Sort by highest priority score ▼

H

bleach - Regular Expression Denial of Service (ReDoS)

VULNERABILITY

CWE-400 ²

CVE-2020-6817 ²

CVSS 7.5 ²

HIGH

SNYK-PYTHON-BLEACH-561754 ²

SCORE

696

Introduced through

bleach@3.0.0

Exploit maturity

PROOF OF CONCEPT

Fixed in

bleach@3.1.4

Show less detail

^

Detailed paths and remediation

▪ Introduced through: project@0.0.0 › bleach@3.0.0

Fix: Upgrade bleach to version 3.1.4 ²

Overview

bleach is a whitelist-based HTML sanitizing library that escapes or strips markup and attributes.

Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS). Calls to `bleach.clean` with an allowed tag and style attribute are vulnerable to ReDoS. For example, `bleach.clean(..., attributes={'a': ['style']})`.

Ignore

Fix this vulnerability

GitLab Automatic Fixing

[Open](#)Created 2 weeks ago by [Fatgle](#) [Maintainer](#)[Report abuse](#)

[Snyk] Security upgrade bleach from 3.0.0 to 3.3.0

[Overview](#) [0](#) [Commits](#) [1](#) [Pipelines](#) [1](#) [Changes](#) [1](#)

Snyk has created this PR to fix one or more vulnerable packages in the `pip` dependencies of this project.

Changes included in this Merge Request

- Changes to the following files to upgrade the vulnerable dependencies to a fixed version:
 - requirements.txt

Vulnerabilities that will be fixed

By pinning:

Severity	Issue	Upgrade	Breaking Change	Exploit Maturity
M	Cross-site Scripting (XSS) SNYK-PYTHON-BLEACH-1069893	bleach: 3.0.0 -> 3.3.0	No	No Known Exploit
M	Cross-site Scripting (XSS) SNYK-PYTHON-BLEACH-552160	bleach: 3.0.0 -> 3.3.0	No	No Known Exploit
M	Cross-site Scripting (XSS) SNYK-PYTHON-BLEACH-561119	bleach: 3.0.0 -> 3.3.0	No	Proof of Concept
H	Regular Expression Denial of Service (ReDoS) SNYK-PYTHON-BLEACH-561754	bleach: 3.0.0 -> 3.3.0	No	Proof of Concept

Some vulnerabilities couldn't be fully fixed and so Snyk will still monitor the project is tested again. This may be because the vulnerability existed within more than one direct dependency, but not all of the effected dependencies could be upgraded.

Check the changes in this Merge Request to ensure they won't cause issues with your project.

Note: You are seeing this because you or someone else with access to this repository has authorized Snyk to open fix PRs.

For more information: [View latest project report](#)

[Adjust project settings](#)

[Read more about Snyk's upgrade and patch logic](#)

[Request to merge](#) [snyk-fix-2ec05a0145d3...](#) [into master](#)

[Open in Web IDE](#)[Check out branch](#)

Pipeline #402723923 passed for 72c4528f on snyk-fix-2ec05a0145d3... 2 weeks ago



IaC – Kubernetes YAML



 purpledobie/iac-demo-video:kubernetes/privilegedPod.yaml


[Overview](#) [History](#) [Settings](#)

Snapshot taken by recurring test 11 hours ago.

[Retest now](#)

Issues	6
Repository	iac-demo-video
Taken by	Recurring

Source	 GitHub
Branch	master
Imported by	 demo-user@demo.org

Type	 Kubernetes
Target	kubernetes/privilegedPod.yaml
Project owner	Add a project owner

Issues



Search issues...

1 H 3 M 2 L

Line #8

> Container is sharing the host PID

M

Line #13

> Memory limits not set

L

Line #17

> Container is running as root

M

> Container not using a read-only root filesystem

L

Line #18

> Container running in privileged mode

H

Line #27

> Container is mounting the Docker socket from the host

M

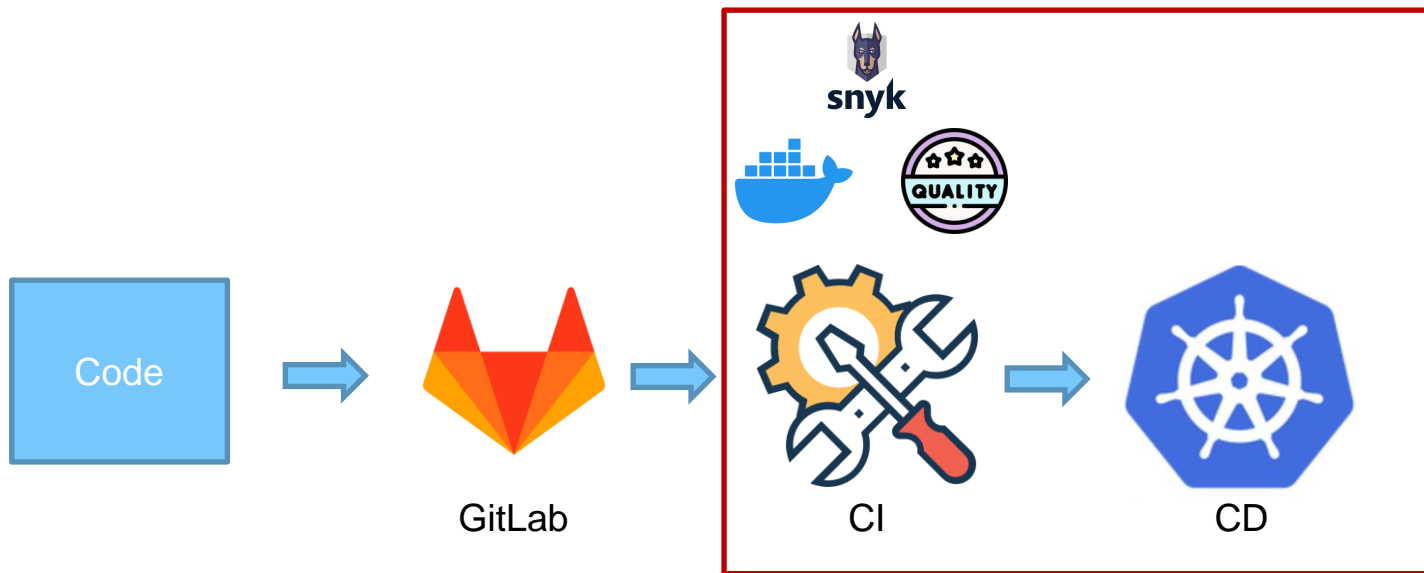
```
1  apiVersion: v1
2  kind: Pod
3  metadata:
4    name: myapp-pod
5    labels:
6      app: myapp
7  spec:
8    hostPID: true
9    containers:
10     - name: myapp-container
11       image: busybox
12       command: ['sh', '-c', 'echo Hello Kubernetes! && sleep 3600']
13     resources:
14       # limits:
15       #   cpu: 100m
16       #   memory: 100Mi
17     securityContext:
18       privileged: true
19     capabilities:
20       drop:
21         - all
22       # add:
23       #   - CAP_SYS_ADMIN
24     volumes:
25     - name: dockersock
26       hostPath:
27         path: /var/run/docker.sock
28
```


04

GitLab

CI/CD






CI/CD 示意圖



GitLab CI/CD pipeline

- .gitlab-ci.yml
- Pipeline
 - Stages
 - build
 - test
 - Variables
 - Environments



Status	Pipeline	Triggerer	Commit	Stages	Duration
 passed	#1485 latest		P g [redacted] ng ~ 165612d9  M [redacted] b...	  	🕒 00:06:45 📅 41 minutes ago

GitLab CI/CD with Snyk

- `npm install -g snyk`
- `snyk auth $SNYK_TOKEN`
- `snyk monitor --project-name=devopsday`
- `snyk test`

Summary

- Snyk四大產品
 - Code
 - Open Source
 - Container
 - IaC
- DevOps -> DevSecOps
 - 漏洞無所不在
 - 開發者優先



Thanks!

Do you have any
questions?

網創資訊

