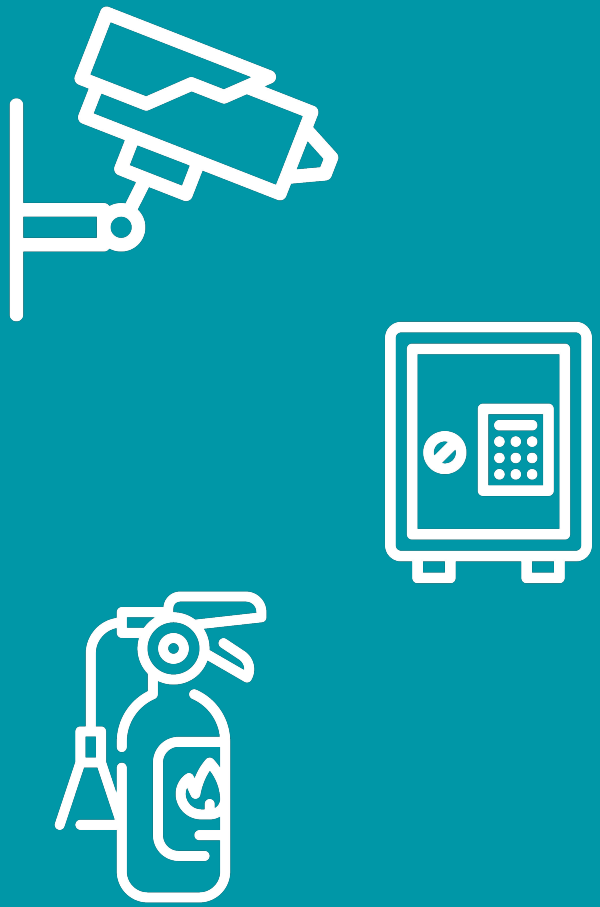
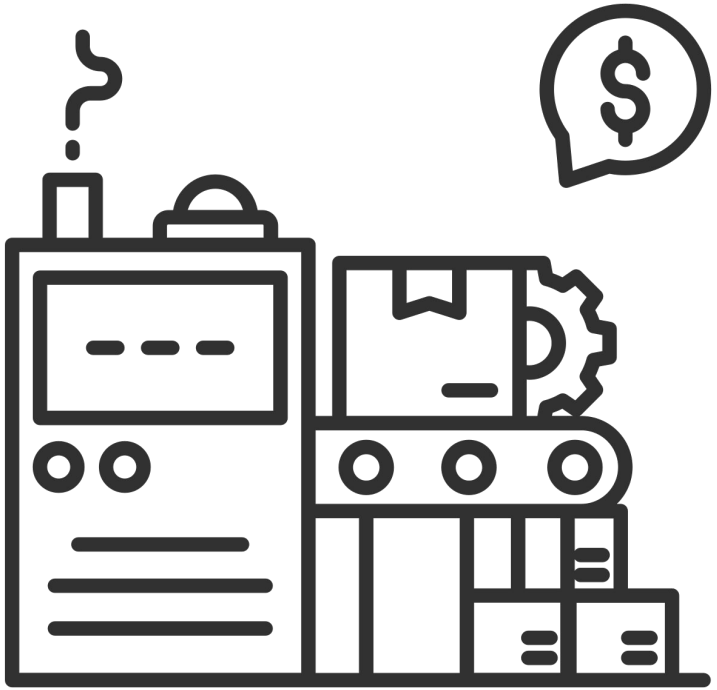
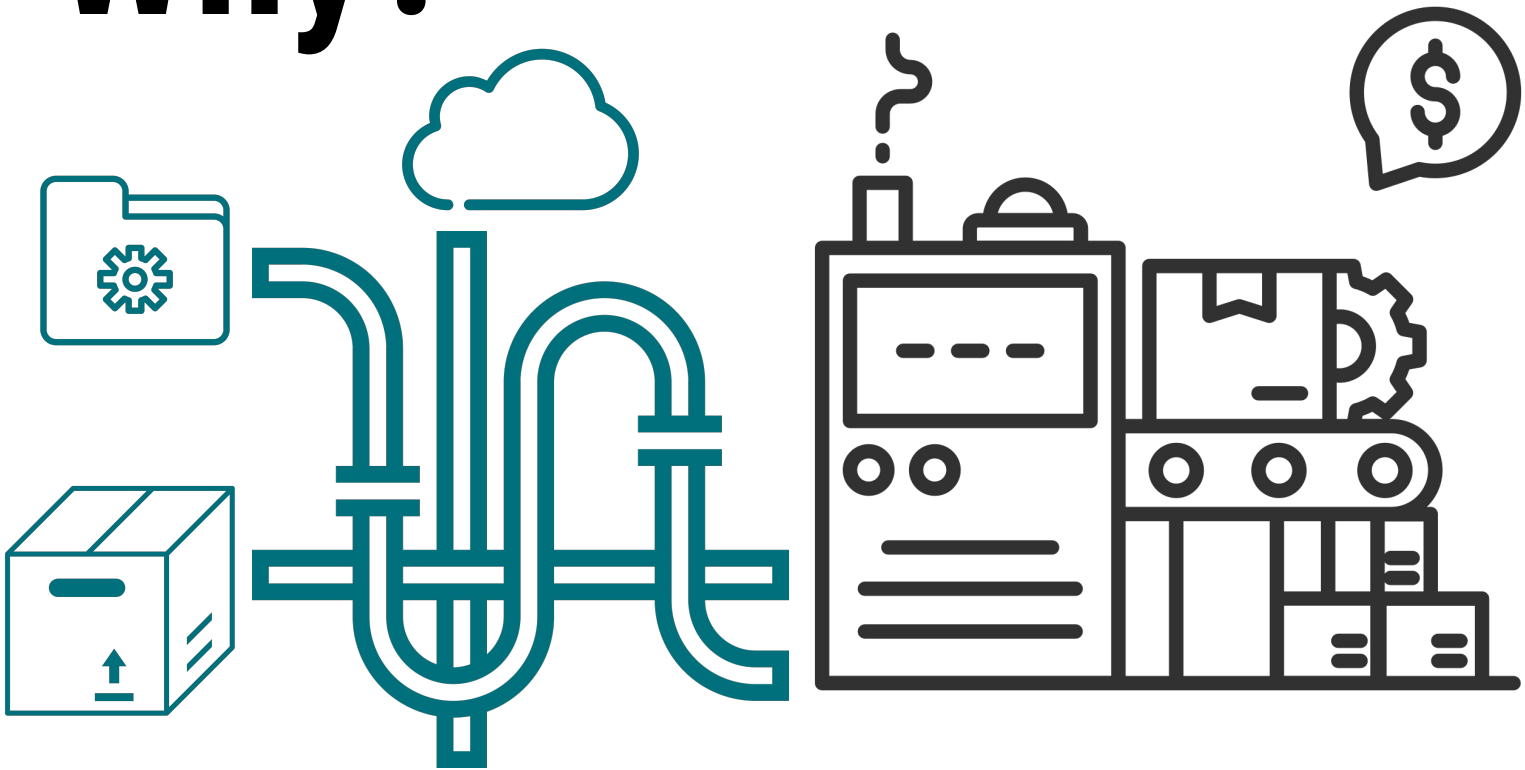


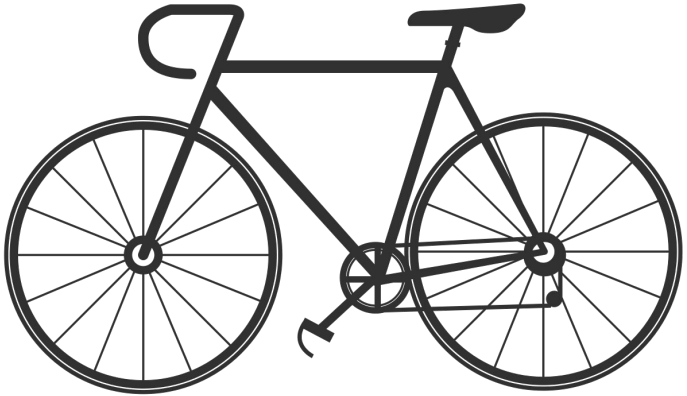
Practical pipeline security tools

Why?



Why?





Akzharkyn Duisembiyeva

Security Engineer

akzharkyn-duisembiyeva

Women In Security
SWEDEN

Mariana Bocoi

SRE Consultant

marianabocoi

Google Developer Groups
Cloud Stockholm

ACME Company

4 ways it can go wrong!

1. Misconfiguration

Image is copied from https://www.huffpost.com/entry/a-house-built-on-faulty-foundations_b_59224825e4b0e8f558bb27e8


aqua
tfsec


checkov
by bridgecrew

```
Check: CKV2_AWS_35: "AWS NAT Gateways should be utilized for the default route"
        PASSED for resource: aws_route.public_internet_gateway
        File: /terraform/aws/ec2.tf:220-228
Check: CKV2_GCP_7: "Ensure that a MySQL database instance does not allow anyone to connect with administrative privileges"
        PASSED for resource: google_sql_database_instance.master_instance
        File: /terraform/gcp/big_data.tf:1-19
        Guide: https://docs.bridgecrew.io/docs/ensure-that-a-mysql-database-instance-does-not-allow-anyone-to-connect-with-administrative-privileges
Check: CKV_AWS_133: "Ensure that RDS instances has backup policy"
        FAILED for resource: aws_db_instance.default
Error:  File: /terraform/aws/db-app.tf:1-41
        Guide: https://docs.bridgecrew.io/docs/ensure-that-rds-instances-have-backup-policy

                1  | resource "aws_db_instance" "default" {
                2  |   name                   = var.dbname
                3  |   engine                 = "mysql"
                4  |   option_group_name      = aws_db_option_group.default.name
                5  |   parameter_group_name   = aws_db_parameter_group.default.name
                6  |   db_subnet_group_name   = aws_db_subnet_group.default.name
                7  |   vpc_security_group_ids = ["${aws_security_group.default.id}"]
                8  |
                9  |   identifier             = "rds-${local.resource_prefix.value}"
                10 |   engine_version         = "8.0" # Latest major version
                11 |   instance_class         = "db.t3.micro"
                12 |   allocated_storage      = "20"
                13 |   username               = "admin"
                14 |   password               = var.password
                15 |   apply_immediately      = true
                16 |   multi_az               = false
                17 |   backup_retention_period = 0
                18 |   storage_encrypted      = false
```

152 Open ✓ 87 Closed — Tool ▾ Branch ▾ Rule ▾ Severity ▾ Sort ▾

Ensure that Cloud Storage bucket is not anonymously or publicly accessible. Error — master
#239 opened 8 days ago • Detected by **tfsec** in terraform/gcp/gcs.tf:19

Ensure that Cloud SQL Database Instances are not publicly exposed Error — master
#233 opened 8 days ago • Detected by **tfsec** in terraform/gcp/big_data.tf:12

Ensure that Cloud SQL Database Instances are not publicly exposed Error — master
#232 opened 8 days ago • Detected by **tfsec** in terraform/gcp/big_data.tf:9

SSL connections to a SQL database instance should be enforced. Error — master
#231 opened 8 days ago • Detected by **tfsec** in terraform/gcp/big_data.tf:8

Legacy ABAC permissions are enabled. Error — master
#227 opened 8 days ago • Detected by **tfsec** in terraform/gcp/gke.tf:12

Node metadata value disables metadata concealment. Error — master
#223 opened 8 days ago • Detected by **tfsec** in terraform/gcp/gke.tf:28

Node metadata value disables metadata concealment. Error — master
#222 opened 8 days ago • Detected by **tfsec** in terraform/gcp/gke.tf:28

GKE Control Plane should not be publicly accessible Error — master
#221 opened 8 days ago • Detected by **tfsec** in terraform/gcp/gke.tf:19

Legacy metadata endpoints enabled. Error — master
#220 opened 8 days ago • Detected by **tfsec** in terraform/gcp/gke.tf:6

Pod security policy enforcement not defined. Error — master
#219 opened 8 days ago • Detected by **tfsec** in terraform/gcp/gke.tf:6

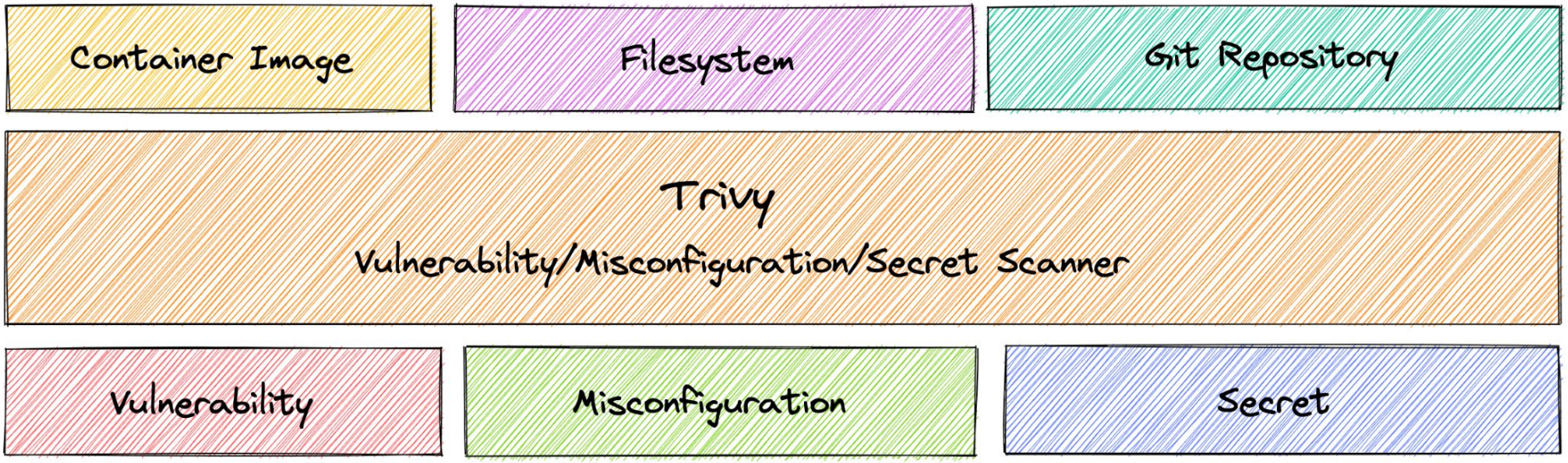
	Checkov	Tfsec
Tested Version	2.0.363	0.58.4
Terraform - AWS	69%	61%
Terraform - Azure	47%	18%
Terraform - Advanced Language Expressions	20%	0%
Total Catch Rate	59%	43%

source https://github.com/iacsecurity/tool-compare

Platform	checkov	TFsec
AWS	23	20
GCP	32	7

source https://www.revolgy.com/insights/blog/complete-guide-for-picking-the-right-tool-for-terraform-security-code-analysis

aqua trivy



source https://aquasecurity.github.io/trivy/v0.28.1

build / **Build**
succeeded 3 minutes ago in 31s

Search logs

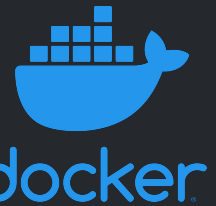
- ✓ **Set up job** 2s
- ✓ **Pull docker.io/aquasec/trivy:latest** 2s
- ✓ **Setup Go** 9s
- ✓ **Checkout code** 1s
- ✓ **Build an image from Dockerfile** 13s
- ✓ **Run vulnerability scanner** 4s

```
▼ Run aquasecurity/trivy-action@0.0.6
  with:
    severity: CRITICAL,HIGH,MEDIUM
    format: table
    exit-code: 0
    image-ref: docker.io/danielpacak/trivy-action-test-drive:728f8e468c350141ab328a420c6fcdfd4912f92f
  env:
    GOROOT: /opt/hostedtoolcache/go/1.14.4/x64
/usr/bin/docker run --name dockerioaquasectrivylatest_91e01b --label 3888d3 --workdir /github/workspace --rm -e GOROOT -e INPUT_SEVERITY -e INPUT_FORMAT -e INPUT_EXIT-CODE -e INPUT_IMAGE-REF -e HOME -e GITHUB_JOB -e GITHUB_REF -e GITHUB_SHA -e GITHUB_REPOSITORY -e GITHUB_REPOSITORY_OWNER -e GITHUB_RUN_ID -e GITHUB_RUN_NUMBER -e GITHUB_ACTOR -e GITHUB_WORKFLOW -e GITHUB_HEAD_REF -e GITHUB_BASE_REF -e GITHUB_EVENT_NAME -e GITHUB_SERVER_URL -e GITHUB_API_URL -e GITHUB_GRAPHQL_URL -e GITHUB_WORKSPACE -e GITHUB_ACTION -e GITHUB_EVENT_PATH -e RUNNER_OS -e RUNNER_TOOL_CACHE -e RUNNER_TEMP -e RUNNER_WORKSPACE -e ACTIONS_RUNTIME_URL -e ACTIONS_RUNTIME_TOKEN -e ACTIONS_CACHE_URL -e GITHUB_ACTIONS=true -e CI=true -v "/var/run/docker.sock":"/var/run/docker.sock" -v "/home/runner/work/_temp/_github_home":"/github/home" -v "/home/runner/work/_temp/_github_workflow":"/github/workflow" -v "/home/runner/work/trivy-action-test-drive/trivy-action-test-drive":"/github/workspace" docker.io/aquasec/trivy:latest  "image" "--format=table" "--exit-code=0" "--severity=CRITICAL,HIGH,MEDIUM" "docker.io/danielpacak/trivy-action-test-drive:728f8e468c350141ab328a420c6fcdfd4912f92f"
2020-06-02T22:25:58.564Z        INFO    Need to update DB
2020-06-02T22:25:58.564Z        INFO    Downloading DB...
2020-06-02T22:26:00.058Z        INFO    Detecting Alpine vulnerabilities...

docker.io/danielpacak/trivy-action-test-drive:728f8e468c350141ab328a420c6fcdfd4912f92f (alpine 3.10.2)
==========================================================================================
Total: 4 (UNKNOWN: 0, LOW: 0, MEDIUM: 4, HIGH: 0, CRITICAL: 0)

+---------+------------------+----------+-------------------+---------------+--------------------------------+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |             TITLE              |
+---------+------------------+----------+-------------------+---------------+--------------------------------+
| openssl | CVE-2019-1549    | MEDIUM   | 1.1.1c-r0         | 1.1.1d-r0     | openssl: information           |
|         |                  |          |                   |               | disclosure in fork()           |
+         +------------------+          +                   +---------------+--------------------------------+
```

- ✓ **Post Checkout code** 0s
- ✓ **Complete job** 0s



```
13
14 docker.io/danielpacak/trivy-action-test-drive:728f8e468c350141ab328a420c6fcdfd4912f92f (alpine 3.10.2)
15 ========================================================================================================
16 Total: 4 (UNKNOWN: 0, LOW: 0, MEDIUM: 4, HIGH: 0, CRITICAL: 0)
17
18 +---------+------------------+----------+-------------------+---------------+--------------------------------+
19 | LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |             TITLE              |
20 +---------+------------------+----------+-------------------+---------------+--------------------------------+
21 | openssl | CVE-2019-1549    | MEDIUM   | 1.1.1c-r0         | 1.1.1d-r0     | openssl: information           |
22 |         |                  |          |                   |               | disclosure in fork()           |
23 +         +------------------+          +                   +---------------+--------------------------------+
```

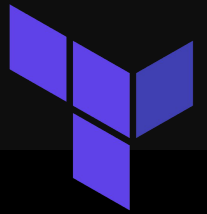
▶ ✓ **Post Checkout code**

▶ ✓ **Complete job**

build

- build 16s
  - Initialize job 2s
  - Checkout Infrastructure... 1s
  - TerraformInstaller 2s
  - Download and Install Tr... 4s
  - Terraform Init 4s
  - LOW/MED - Trivy vulne... 1s
  - HIGH/CRIT - Trivy vuln... <1s
  - Terraform Plan <1s
  - Copy Files to Staging <1s
  - Archive Terraform Arti... <1s
  - Publish Pipeline Artifact <1s
  - Post-job: Checkout Inf... <1s

```
33
34
35  .terraform/modules/dynamic-subnets/variables.tf (terraform)
36  ============================================================
37  Tests: 22 (SUCCESSES: 22, FAILURES: 0, EXCEPTIONS: 0)
38  Failures: 0 (HIGH: 0, CRITICAL: 0)
39
40
41  main.tf (terraform)
42  ===================
43  Tests: 3 (SUCCESSES: 2, FAILURES: 1, EXCEPTIONS: 0)
44  Failures: 1 (HIGH: 0, CRITICAL: 1)
45
46  +-----------------------------------+-------------+-----------------------------------+----------+-----------------------------------+
47  |               TYPE                |  MISCONF ID |               CHECK               | SEVERITY |              MESSAGE              |
48  +-----------------------------------+-------------+-----------------------------------+----------+-----------------------------------+
49  |  Terraform Security Check powered |  AVD-GEN-0001 | Potentially sensitive data stored in | CRITICAL | Block 'provider.azurerm' includes a potentially
50  |                by tfsec           |             | block attribute.                  |          | sensitive attribute which is defined within the proj
51  |                                   |             |                                   |          | -->tfsec.dev/docs/general/secrets/sensitive-in-attri
52  +-----------------------------------+-------------+-----------------------------------+----------+-----------------------------------+
53
54  network.tf (terraform)
55  ======================
56  Tests: 6 (SUCCESSES: 6, FAILURES: 0, EXCEPTIONS: 0)
57  Failures: 0 (HIGH: 0, CRITICAL: 0)
58
59
60  variables.tf (terraform)
```

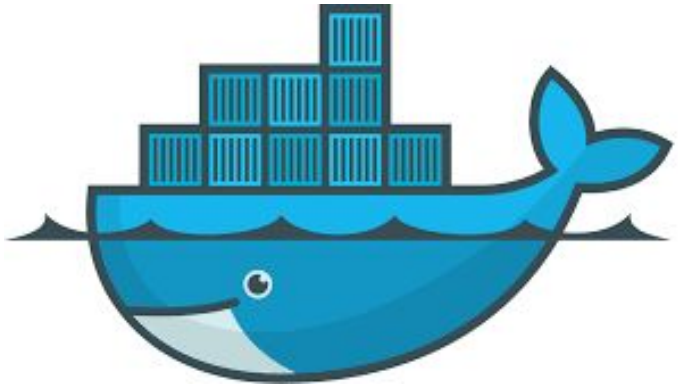


source https://dev.to/pwd9000/terraform-iac-scanning-with-trivy-3cai

source https://dev.to/pwd9000/terraform-iac-scanning-with-trivy-3cai

2. Permissions

source https://permsecure.com/wp-content/uploads/2021/06/PoLP.jpg



```
vlatka@vlatka-VirtualBox:~/recipes$ docker run -v /:/host -it avocado_secret_th
eft
root@c43c5d556c12:/# ls
bin   dev  home  lib    media  opt   root  sbin  sys  usr
boot  etc  host  lib64  mnt    proc  run   srv   tmp  var
root@c43c5d556c12:/# cd host
root@c43c5d556c12:/host# ls
bin    dev   initrd.img      lib64       mnt   root  snap      sys  var
boot   etc   initrd.img.old  lost+found  opt   run   srv       tmp  vmlinuz
cdrom  home  lib             media       proc  sbin  swapfile  usr
root@c43c5d556c12:/host# cd home
root@c43c5d556c12:/host/home# ls
vlatka
root@c43c5d556c12:/host/home# cd vlatka/recipes/ && ls -l
total 4
-rw------- 1 root root 52 Apr  5 13:48 secret_ingredient.txt
root@c43c5d556c12:/host/home/vlatka/recipes# cat secret_ingredient.txt
I always put some chili flakes on my avocado toast.
root@c43c5d556c12:/host/home/vlatka/recipes#
```

source https://medium.com/jobteaser-dev-team/docker-user-best-practices-a8d2ca5205f4

```
vlatka@vlatka-VirtualBox:~/recipes$ docker run -v /:/host -it avocado_secret_th
eft
root@c43c5d556c12:/# ls
bin   dev  home  lib    media  opt   root  sbin  sys  usr
boot  etc  host  lib64  mnt    proc  run   srv   tmp  var
root@c43c5d556c12:/# cd host
root@c43c5d556c12:/host# ls
bin    dev   initrd.img      lib64       mnt   root  snap      sys  var
boot   etc   initrd.img.old  lost+found  opt   run   srv       tmp  vmlinuz
cdrom  home  lib             media       proc  sbin  swapfile  usr
root@c43c5d556c12:/host# cd home
root@c43c5d556c12:/host/home# ls
vlatka
root@c43c5d556c12:/host/home# cd vlatka/recipes/ && ls -l
total 4
-rw------- 1 root root 52 Apr  5 13:48 secret_ingredient.txt
root@c43c5d556c12:/host/home/vlatka/recipes# cat secret_ingredient.txt
I always put some chili flakes on my avocado toast.
root@c43c5d556c12:/host/home/vlatka/recipes#
```

source https://medium.com/jobteaser-dev-team/docker-user-best-practices-a8d2ca5205f4


Semgrep

Semgrep

Search Explore

Contribute to Registry

dockerfile.security.last-user-is-root.last-user-is-root

Add these to Rule Board | Language | Category | Technology | OWASP | Severity | Visibility

Rules (2) Sorted by relevance

dockerfile.security.last-user-is-root.last-user-is-root error

The last user in the container is 'root'. This is a security hazard because if an attacker gains control of the container...

by r2c

generic.dockerfile.security.last-user-is-root.last-user-is-root error

The last user in the container is 'root'. This is a security hazard because if an attacker gains control of the container...

by r2c

Follow best practices!

Private data

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"PublicRead",
      "Effect":"Allow",
      "Principal": {"AWS": "*"},
      "Action":["s3:GetObject","s3:GetObjectVersion"],
      "Resource":["arn:aws:s3:::bucket-with-public-policy-2/*"]
    }
  ]
}
```

source https://cloudrail.app/blog/securing-s3-buckets-built-in-terraform-using-iac-security-tools

Private data

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"PublicRead",
      "Effect":"Allow",
      "Principal": {"AWS": "*"},
      "Action":["s3:GetObject","s3:GetObjectVersion"],
      "Resource":["arn:aws:s3:::bucket-with-public-policy-2/*"]
    }
  ]
}
```

```
# Ensure no public access is possible
resource "aws_s3_bucket_public_access_block" "bucket" {
  bucket = aws_s3_bucket.bucket.id

  block_public_acls       = var.block_public_acls # default: true
  block_public_policy     = var.block_public_policy # default: true
  ignore_public_acls      = var.ignore_public_acls # default: true
  restrict_public_buckets = var.restrict_public_buckets # default: true
}
```

source https://cloudrail.app/blog/securing-s3-buckets-built-in-terraform-using-iac-security-tools

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: security-context-demo-2
spec:
  securityContext:
    runAsUser: 1000
  containers:
  - name: sec-ctx-demo-2
    image: gcr.io/google-samples/node-hello:1.0
    securityContext:
      runAsUser: 2000
      allowPrivilegeEscalation: false
```

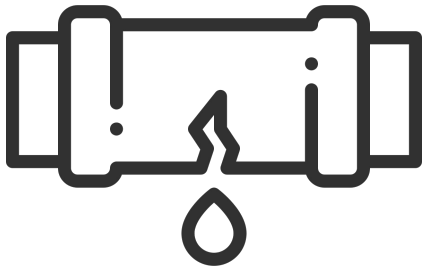
source https://kubernetes.io/docs/tasks/configure-pod-container/security-context

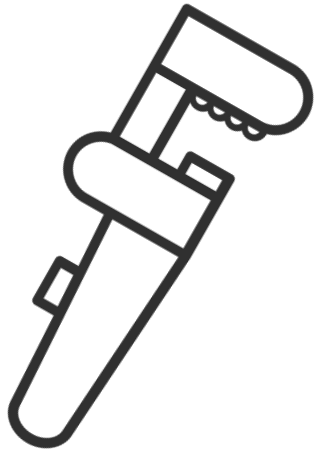
```yaml
apiVersion: v1
kind: Pod
metadata:
  name: security-context-demo-2
spec:
  securityContext:
    runAsUser: 1000
  containers:
  - name: sec-ctx-demo-2
    image: gcr.io/google-samples/node-hello:1.0
    securityContext:
      runAsUser: 2000
      allowPrivilegeEscalation: false
```

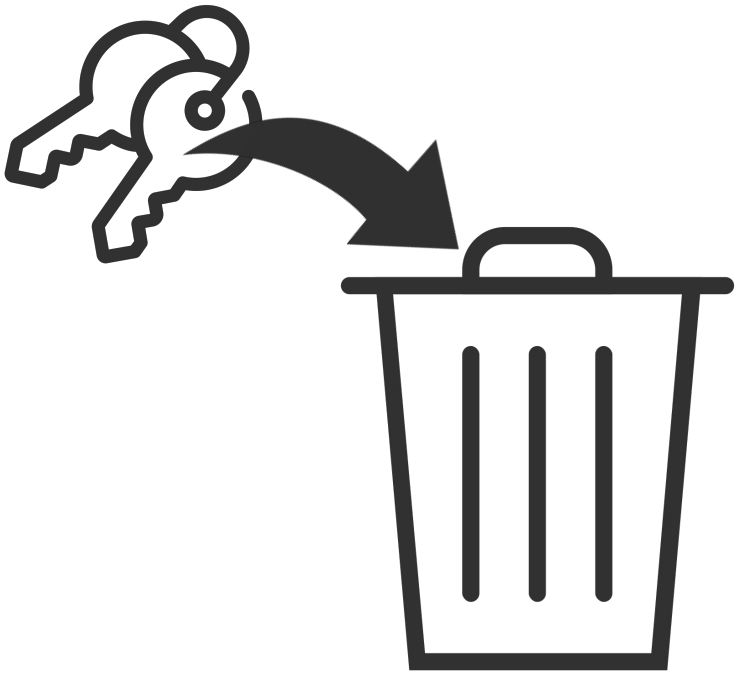
source https://kubernetes.io/docs/tasks/configure-pod-container/security-context

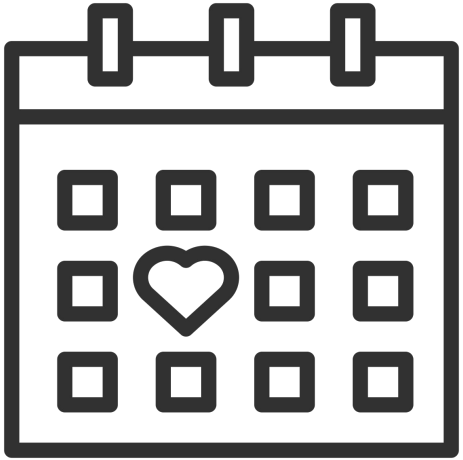
source https://sysdig.com/blog/dockerfile-best-practices

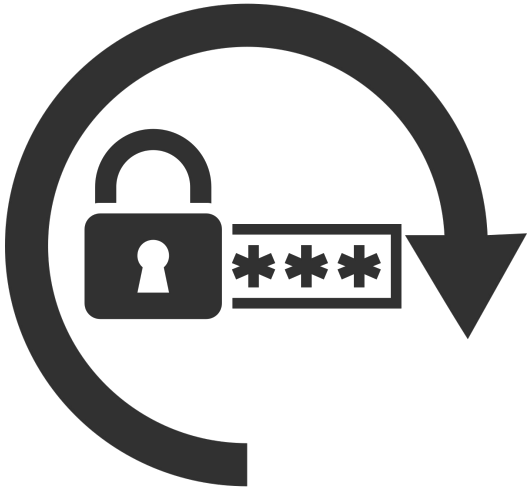
3. Leaked secrets


انبوب



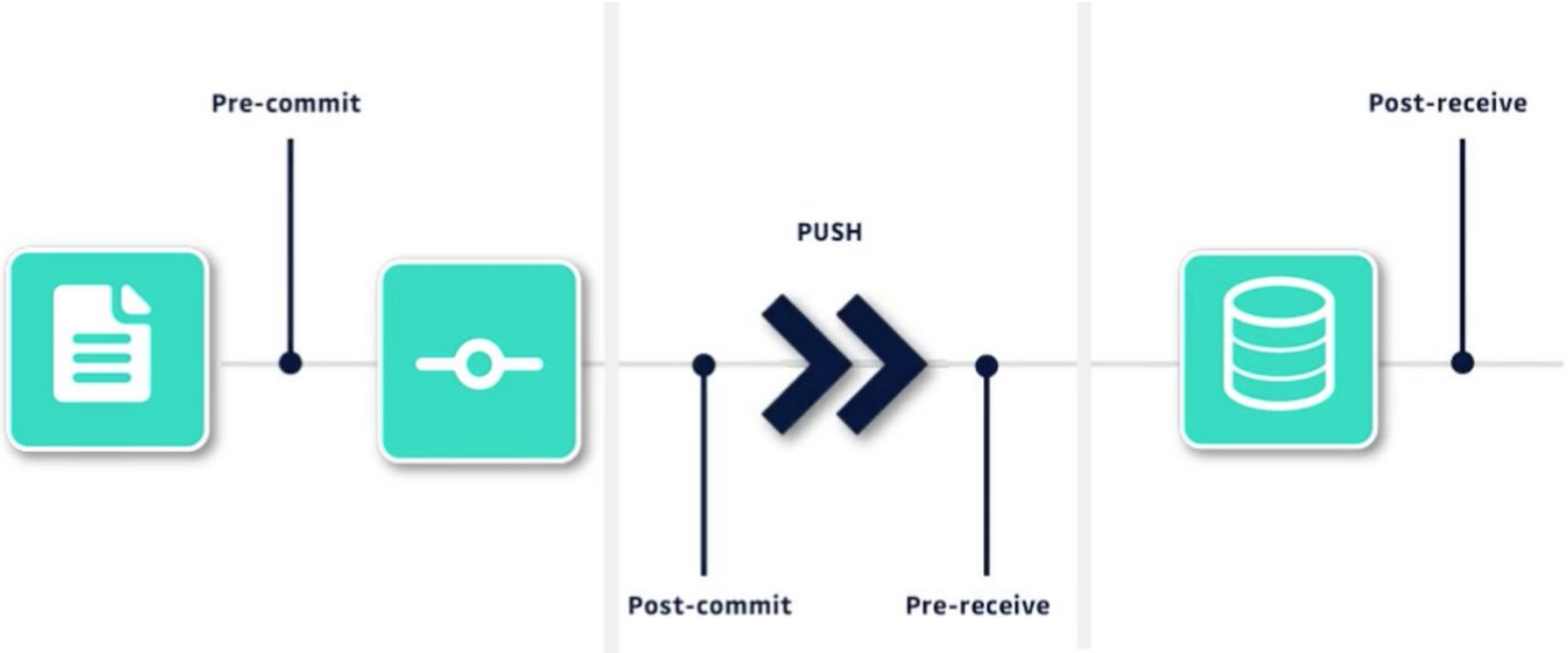




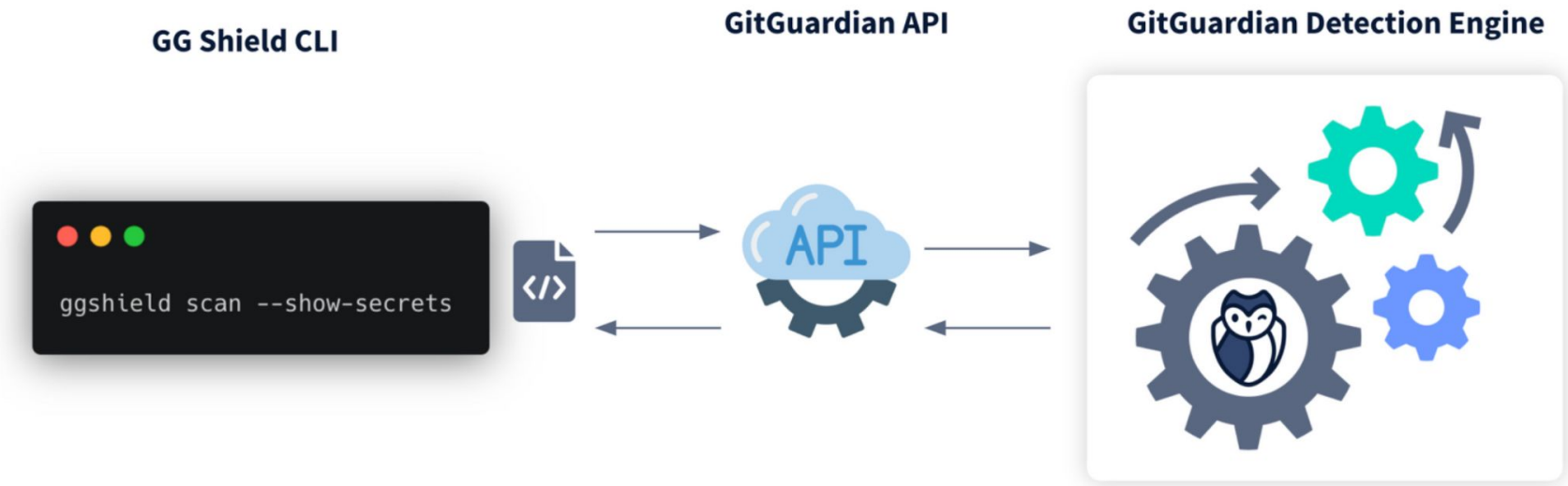



AkzharkynDM/terragoat
73ed190
terraform/aws/ec2.tf
GitGuardian
GENERIC HIGH ENTROPY SECRET
apikey
@@ -17,28 +17,55 @@ export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMAAAKEY
export AWS_DEFAULT_REGION=us-west-2
echo "<h1>Deployed via Terraform</h1>" | sudo tee /var/www/html/index.html
EOF
- tags = {
+ tags = merge({
Name = "${local.resource_prefix.value}-ec2"
- }
+ }, {
+ git_commit = "d68d2897add9bc2203a5ed0632a5cdd8ff8cefb0"
+ git_file = "terraform/aws/ec2.tf"
+ git_last_modified_at = "2020-06-16 14:46:24"
+ git_last_modified_by = "nimrodkor@gmail.com"
+ git_modifiers = "nimrodkor"
+ git_org = "bridgecrewio"
+ git_repo = "terragoat"
+ yor_trace = "347af3cd-4f70-4632-aca3-4d5e30ffc0b6"
+ })
}


GitGuardian
+
PagerDuty
=



source https://blog.gitguardian.com/setting-up-a-pre-commit-git-hook-with-gitguardian-shield-to-scan-for-secrets



source https://blog.gitguardian.com/setting-up-a-pre-commit-git-hook-with-gitguardian-shield-to-scan-for-secrets

WrongSecrets

Examples with how **not** to use secrets

GitGuardian

OPEN SOURCE

This is Free!

For public repositories listed under a GitHub Organization

Available in Saas

Quick start for free

SMALL TEAMS

This is Free!

1 - 25 developers

Available in Saas

Quick start for free

STANDARD

$500 / month

billed annually

30 developers

Available in Saas

Available on Prem

Quick start for free

ENTERPRISE

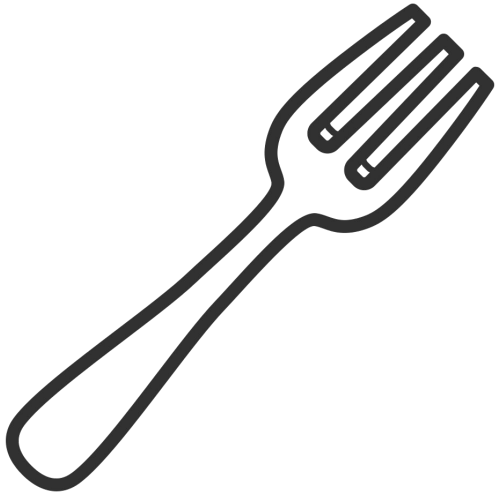
Let's talk!

> 200 developers

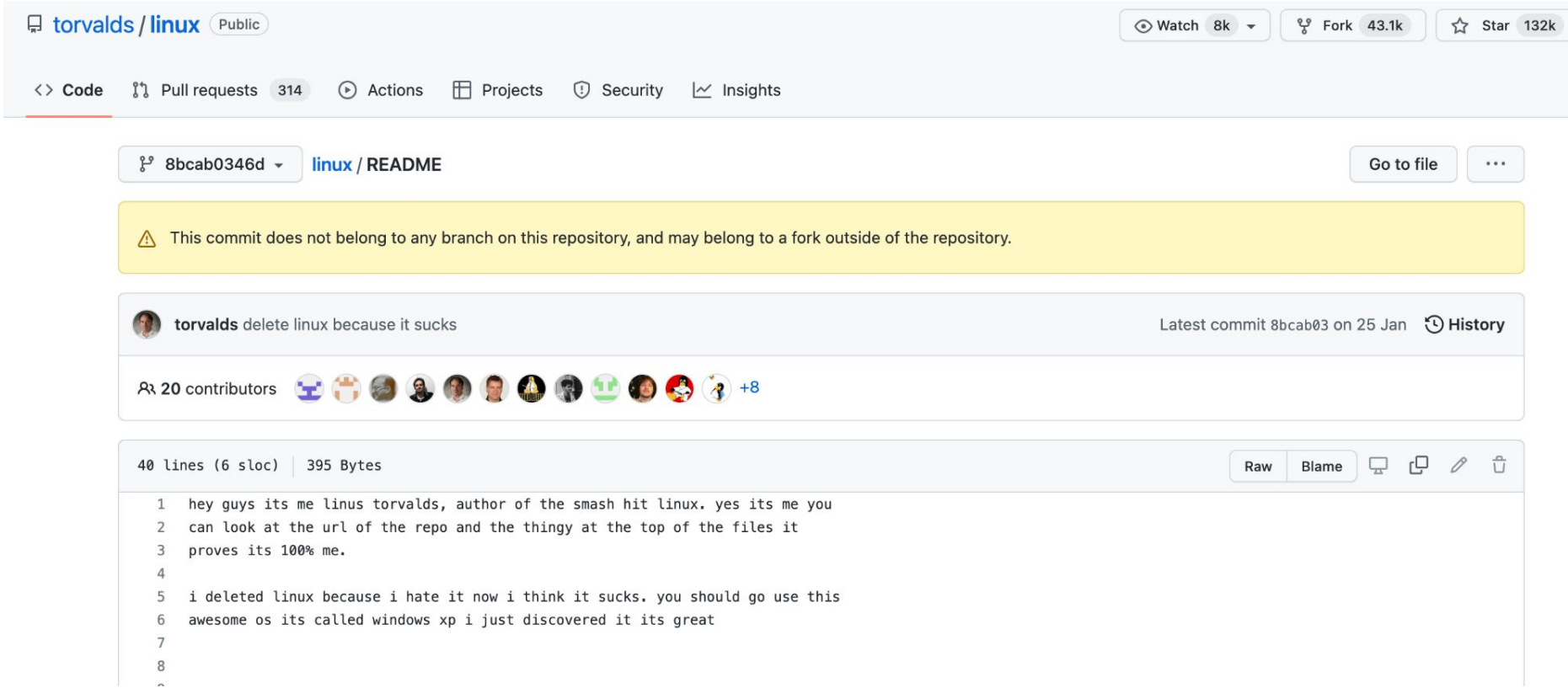
Available in Saas

Available on Prem

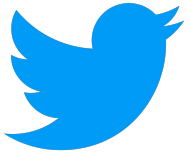
Schedule a demo



Cross-fork
object sharing
in git
(is not a bug)



source https://github.com/torvalds/linux/blob/8bcab0346d4fcf21b97046eb44db8cf37ddd6da0/README



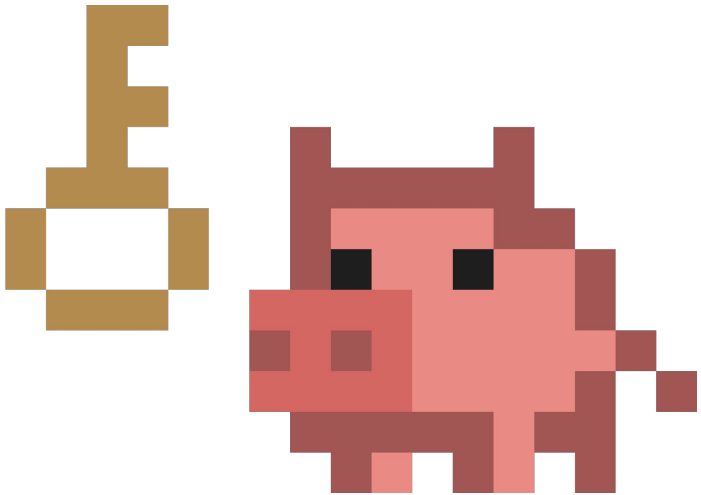
TomNomNom
@TomNomNom

daft one-liner: grep git repo for pattern:

```
{ find .git/objects/pack/ -name "*.idx"|while read i;do
git show-index < "$i"|awk '{print $2}';done;find
.git/objects/ -type f|grep -v '/pack/'|awk -F'/' '{print
$(NF-1)$NF}'; }|while read o;do git cat-file -p
$o;done|grep -E 'pattern'
```

2:14 PM · May 28, 2019 · Twitter Web Client

TruffleHog



Demo


TruffleHog Enterprise July 2021 Demo
Watch later
Share
UNEARTH YOUR Secrets
Truffle Security offers the first automated solution to continuously scan your environment for secrets like private keys and credentials, so you can protect your data before a breach occurs.
9:41
Monday, June 3
TruffleHog found a secret
Verified Slack User Token found in Github repository "Backend".
TruffleHog found a secret
Verified AWS credentials found in Jira issue "Requesting Access to S3 Bucket".
swipe up to open
Watch on YouTube
trufflesecurity.com

Gitrob

Gitrob

Finished (100%)

291	234,262	35,205	539	26	00:15:13
Findings	Files	Commits	Repositories	Targets	Duration

Findings

Search...

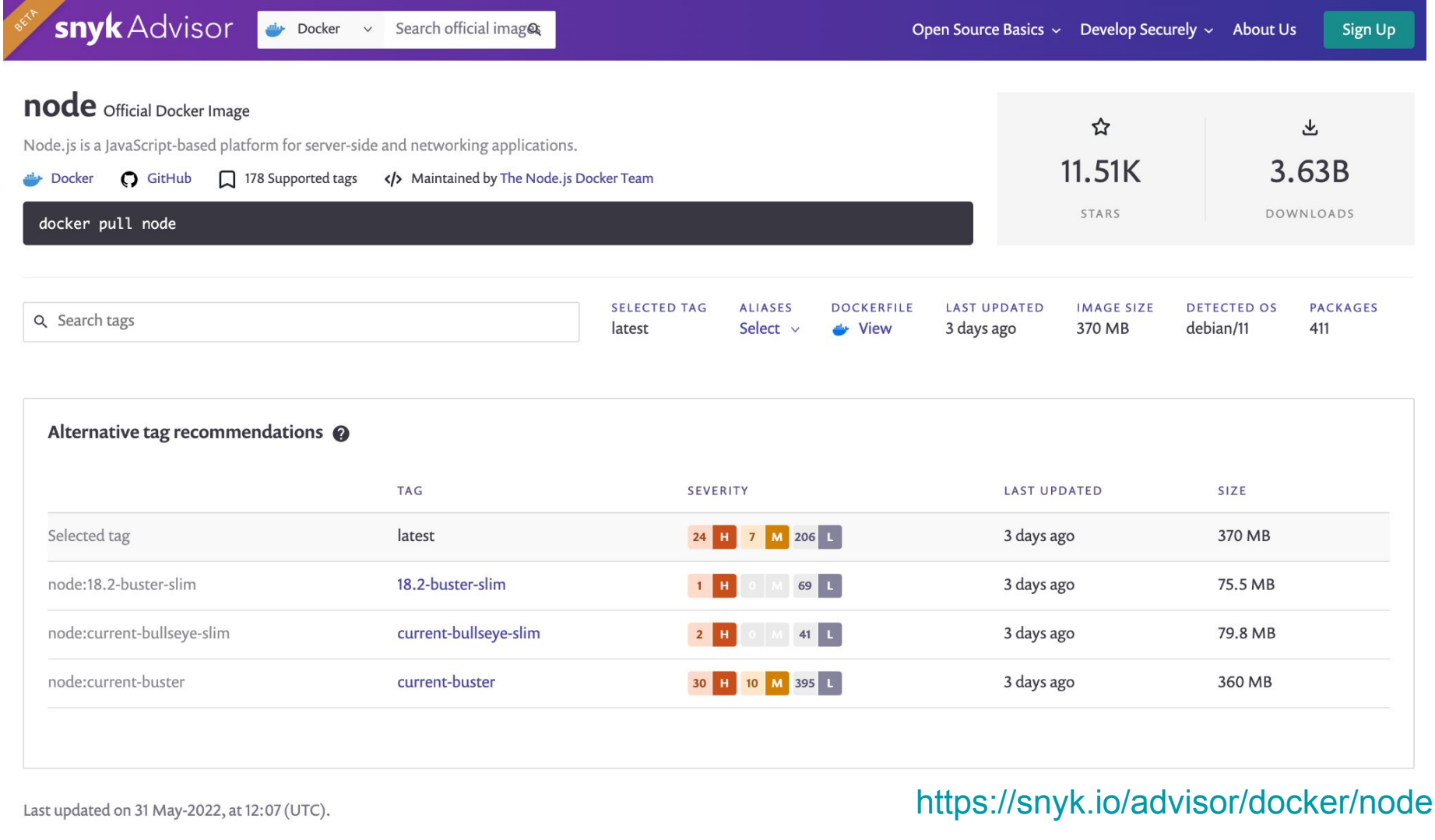
Action	Path	Commit	Repository
MODIFY	zshrc	00d3951	danchen/dotfiles
MODIFY	zshrc	7f0b334	danchen/dotfiles
CREATE	gitconfig	99c2163	danchen/dotfiles
MODIFY	zshrc	7218edd	danchen/dotfiles
MODIFY	zshrc	3baa98c	danchen/dotfiles
CREATE	src/instrumentTest/res/raw/user_credentials.properties	528c401	bjorncs/chess-saldo
DELETE	tests/ChessSaldoTest/res/raw/user_credentials.properties	528c401	bjorncs/chess-saldo
CREATE	tests/ChessSaldoTest/res/raw/user_credentials.properties	6a90e0d	bjorncs/chess-saldo
CREATE	handlers/sfbc_ga_key.pem	fbab03a	drewfish/webapp-iot
CREATE	sidecar.log	58365e2	francisco-perez-sorrosal/msopenhack-stat-sidecar

4. Open-source dependencies

! RCE

Remote Code Execution

Scan for known vulnerabilities



https://snyk.io/advisor/docker/node

Juice Shop

Open a Fix PR

marianabocoi/juice-shop:package.json

Back to project

Issues with a fix

An upgrade is available to fix these issues:

- [x] H Uninitialized Memory Exposure in base64url
- [ ] H Authorization Bypass in express-jwt
- [ ] H Authentication Bypass in jsonwebtoken
- [ ] H Forgeable Public/Private Tokens in jws
- [ ] H Command Injection in lodash
- [ ] H Prototype Pollution in lodash
- [ ] H Prototype Pollution in lodash

Open a Fix PR

marianabocoi/juice-shop:package.json

Back to project

Issues with a fix

An upgrade is available to fix these issues:

- [x] H Uninitialized Memory Exposure in base64url ⚠
- [ ] H Authorization Bypass in express-jwt ⚠
- [ ] H Authentication Bypass in jsonwebtoken ⚠
- [ ] H Forgeable Public/Private Tokens in jws ⚠
- [ ] H Command Injection in lodash
- [ ] H Prototype Pollution in lodash
- [ ] H Prototype Pollution in lodash

Issues with a partial fix

An upgrade is available to fix some of these issues:

H Regular Expression Denial of Service (ReDoS) in ansi-regex

- [ ] Partially fix this vulnerability.

Open a Fix PR

marianabocoi/juice-shop:package.json

Back to project

Issues with a fix

An upgrade is available to fix these issues:

- [x] H Uninitialized Memory Exposure in base64url
- [ ] H Authorization Bypass in express-jwt
- [ ] H Authentication Bypass in jsonwebtoken
- [ ] H Forgeable Public/Private Tokens in jws
- [ ] H Command Injection in lodash
- [ ] H Prototype Pollution in lodash
- [ ] H Prototype Pollution in lodash

Issues with a partial fix

An upgrade is available to fix some of these issues:

H Regular Expression Denial of Service (ReDoS) in ansi-regex

- [ ] Partially fix this vulnerability.

Issues with no fix

No upgrade or patch is currently available for these issues:

- H Denial of Service (DoS) in dicer
- H Prototype Pollution in lodash.set
- H Prototype Pollution in unset-value
- M Arbitrary File Write via Archive Extraction (Zip Slip) in decompress-tar
- M Prototype Pollution in eivindfjeldstad-dot
- L Information Exposure in hbs
- C Arbitrary Code Injection in marsdb
- M Sandbox Bypass in notevil
- L Prototype Pollution in minimist
- C Sandbox Bypass in vm2
- C Sandbox Bypass in vm2

snyk-bot commented 16 seconds ago First-time contributor

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

Changes included in this PR

- Changes to the following files to upgrade the vulnerable dependencies to a fixed version:
  - package.json

Vulnerabilities that will be fixed

With an upgrade:

Severity	Priority Score (*)	Issue	Breaking Change	Exploit Maturity
H	**741/1000** **Why?** Mature exploit, Has a fix available, CVSS 7.1	Uninitialized Memory Exposure npm:base64url:20180511	Yes	Mature

(*) Note that the real score may have changed since the PR was raised.

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

Security Scorecards

by
Open Source
Security Foundation
(OpenSSF)

Posted by u/rootnessify 1 year ago

11

out of the loop question: wtf is honking?

I see it everywhere by people who are considered influencers for k8s stuff, I see it as a title of videos in youtube, I see it as a title in podcast.. hell there's even a CI called honkci..

what does goose and honking have to do with k8s?

8 Comments Share Save Hide Report 92% Upvoted

Log in or sign up to leave a comment Log In Sign Up

Sort By: Best

Comment deleted by user · 1 yr. ago

mr_toph · 1 yr. ago

Untitled Goose Game is definitely the origin of it, but it actually goes back to 2019..

It started as a small inside joke, but kinda just blew up. A bunch of us really loved UGG (which, if you haven't played it, still highly recommend it even if you aren't normally into video games), and as some of us have been known to do, take jokes a little too far/literal. A plug-in for the Kubernetes CI system was built (https://github.com/kubernetes/test-infra/pull/14587) that posts goose pictures on command. Then there were some contests/activities put together at our contributor summit that were goose-themed.

Ian's fantastic keynote in San Diego (https://youtu.be/3jGNjan6I3Y) was when it became "mainstream".. basically breaking out from "an inside joke between a small number of k8s contributors" to a much bigger thing.

And now the goose is so ubiquitous with kubernetes and security, that when the OpenSSF was formed, its logo is a goose: https://openssf.org

Basically: a goose/honking is an amusing mascot representing cloud native mischief :)

4 Reply Share Report Save Follow

```
./scorecard --repo=github.com/ossf-tests/scorecard-check-branch-protection-e2e --checks Branch-te
Starting [Pinned-Dependencies]
Finished [Pinned-Dependencies]

RESULTS
-------
|---------|------------------------|---------------------------------|-------------------------------
|  SCORE  |          NAME          |             REASON              |            DETAILS
|---------|------------------------|---------------------------------|-------------------------------
| 9 / 10  | Branch-Protection      | branch protection is not        | Info: 'force pushes' disabled
|         |                        | maximal on development and all  | on branch 'main' Info: 'allow
|         |                        | release branches                | deletion' disabled on branch
|         |                        |                                 | 'main' Info: linear history
|         |                        |                                 | enabled on branch 'main' Info:
|         |                        |                                 | strict status check enabled
|         |                        |                                 | on branch 'main' Warn: status
|         |                        |                                 | checks for merging have no
|         |                        |                                 | specific status to check on
|         |                        |                                 | branch 'main' Info: number
|         |                        |                                 | of required reviewers is 2
|         |                        |                                 | on branch 'main' Info: Stale
|         |                        |                                 | review dismissal enabled on
|         |                        |                                 | branch 'main' Info: Owner
|         |                        |                                 | review required on branch
|         |                        |                                 | 'main' Info: 'admininistrator
|         |                        |                                 | PRs need reviews before being
|         |                        |                                 | merged on branch 'main'
|---------|------------------------|---------------------------------|-------------------------------
```

Code | Pull requests | Actions | Projects | Wiki | Security 2,126 | Insights | Settings

- Overview
- Security policy
- Security advisories
- Dependabot alerts
- Code scanning alerts 2,126

Code scanning

Add scanning tool

Latest scan	Branch	Workflow	Duration	Result
2 minutes ago	master	build	3s	2126 alerts

is:open branch:master

2,126 Open | 2,082 Closed | Tool | Branch | Rule | Severity | Sort

CVE-2019-5953 Package: wget Error — master
#4202 opened 2 minutes ago • Detected by **Trivy** in docker.io/my-organization/my-app:2d7cad4c8795f93eb...:1

CVE-2017-13090 Package: wget Error — master
#4201 opened 2 minutes ago • Detected by **Trivy** in docker.io/my-organization/my-app:2d7cad4c8795f93eb...:1

CVE-2017-13089 Package: wget Error — master
#4200 opened 2 minutes ago • Detected by **Trivy** in docker.io/my-organization/my-app:2d7cad4c8795f93eb...:1

CVE-2020-9484 Package: tomcat-servlet-3.0-api Error — master
#4109 opened 2 minutes ago • Detected by **Trivy** in docker.io/my-organization/my-app:2d7cad4c8795f93eb...:1

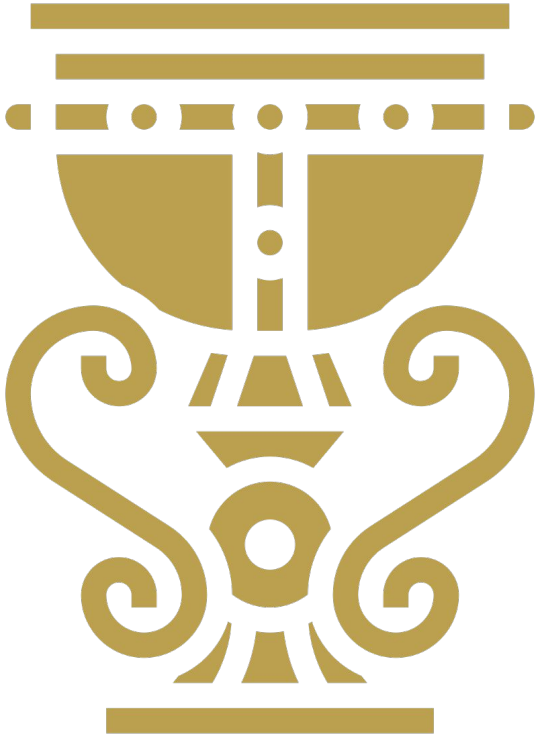
CVE-2020-1938 Package: tomcat-servlet-3.0-api Error — master
#4108 opened 2 minutes ago • Detected by **Trivy** in docker.io/my-organization/my-app:2d7cad4c8795f93eb...:1

Ian Coldwater 📦💥 @IanColdwater · 4h

I don't know who needs to hear this, but if you're doing a security presentation and you're sharing your screen, please update your Chrome

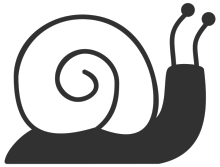
18 29 511

Not the Holly Grail



Problems:

not solving
all issues



lagging
behind

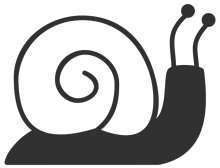
where is
my data

many & complex
results

time to fix
findings

Problems:

not solving all issues



lagging behind

where is my data

many & complex results

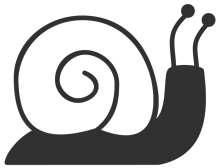
time to fix findings

Open Policy Agent

openpolicyagent.org

Problems:

not solving all issues



lagging behind

where is my data

many & complex results

time to fix findings

Open Policy Agent

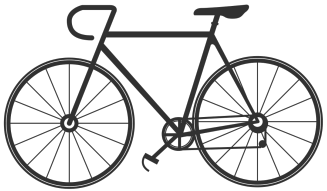
openpolicyagent.org

13 June at the Google Office

Google Developer Groups

Cloud Stockholm

Try them Out!



aqua tfsec

Semgrep

checkov by bridgecrew

snyk

aqua trivy

Security Scorecards

GitGuardian

Akzharkyn Duisembiyeva
Security Engineer

akzharkyn-duisembiyeva

Women In Security
SWEDEN

Mariana Bocoi
SRE Consultant

marianabocoi

Google Developer Groups
Cloud Stockholm