Christian Köberl

Supply Chain Security using Free and Open Tools

KCD AUSTRIA September 26th-27th 2023

Hi, I’m Christian

🪶 Chief Technical Architect @ Porsche Informatik.

👨‍💻 Professional developer since 1998.

You'll find my code at github.com/derkoe

More talks and information at derkoe.dev

I tweet at @derkoe

I toot at @derkoe@mastodon.social

Caveat

This talk only covers **dependency management**
(„Vulnerable and Outdated Components“
OWASP Top 10 - A06:2021)

There are more security relevant aspects.

Weekend 😀

Your next task is to figure out which applications in your org use log4j
imgflip.com

Source: https://twitter.com/cyb3rops/status/1469326219174891520

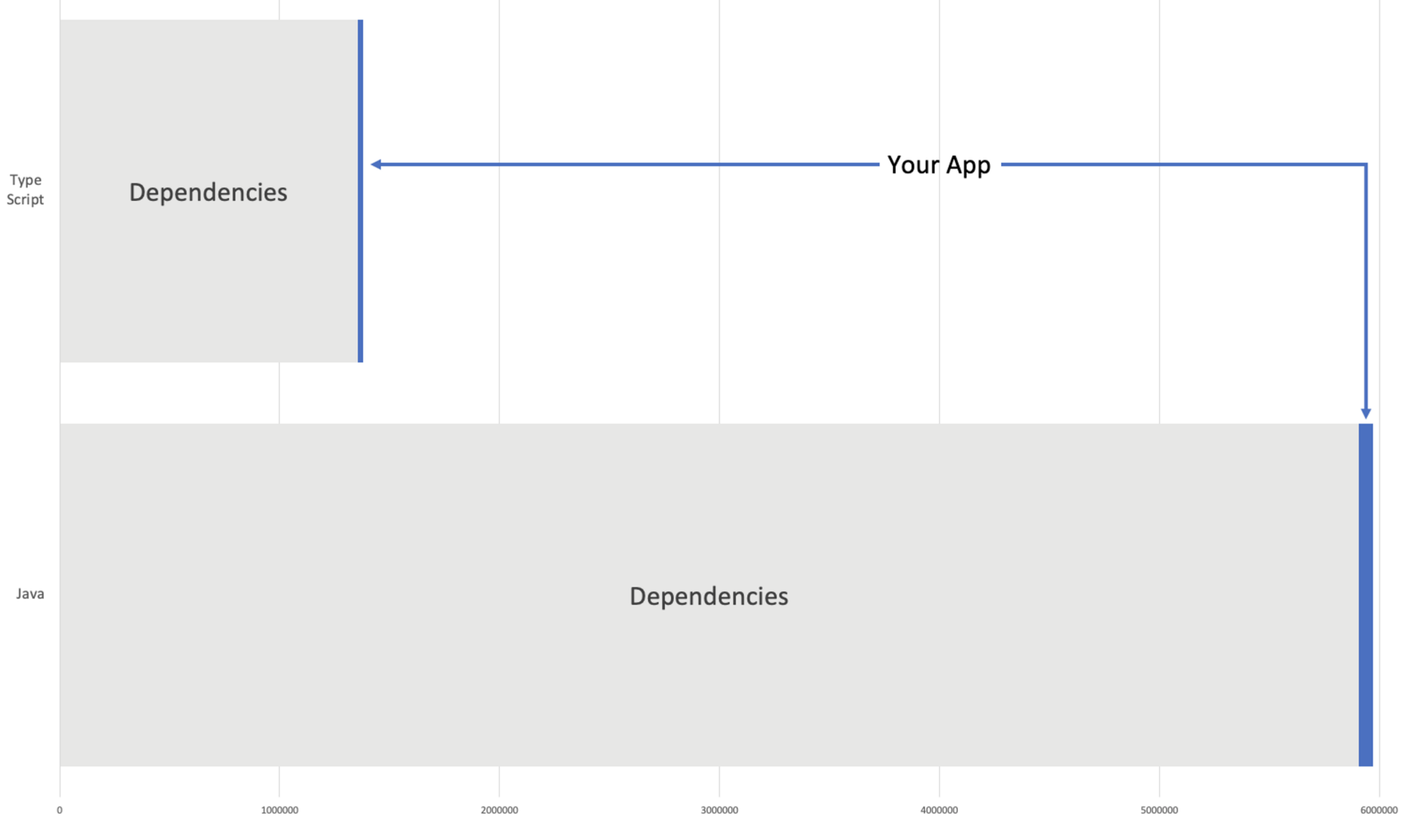
87%

had one or more supply chain security issues in last year

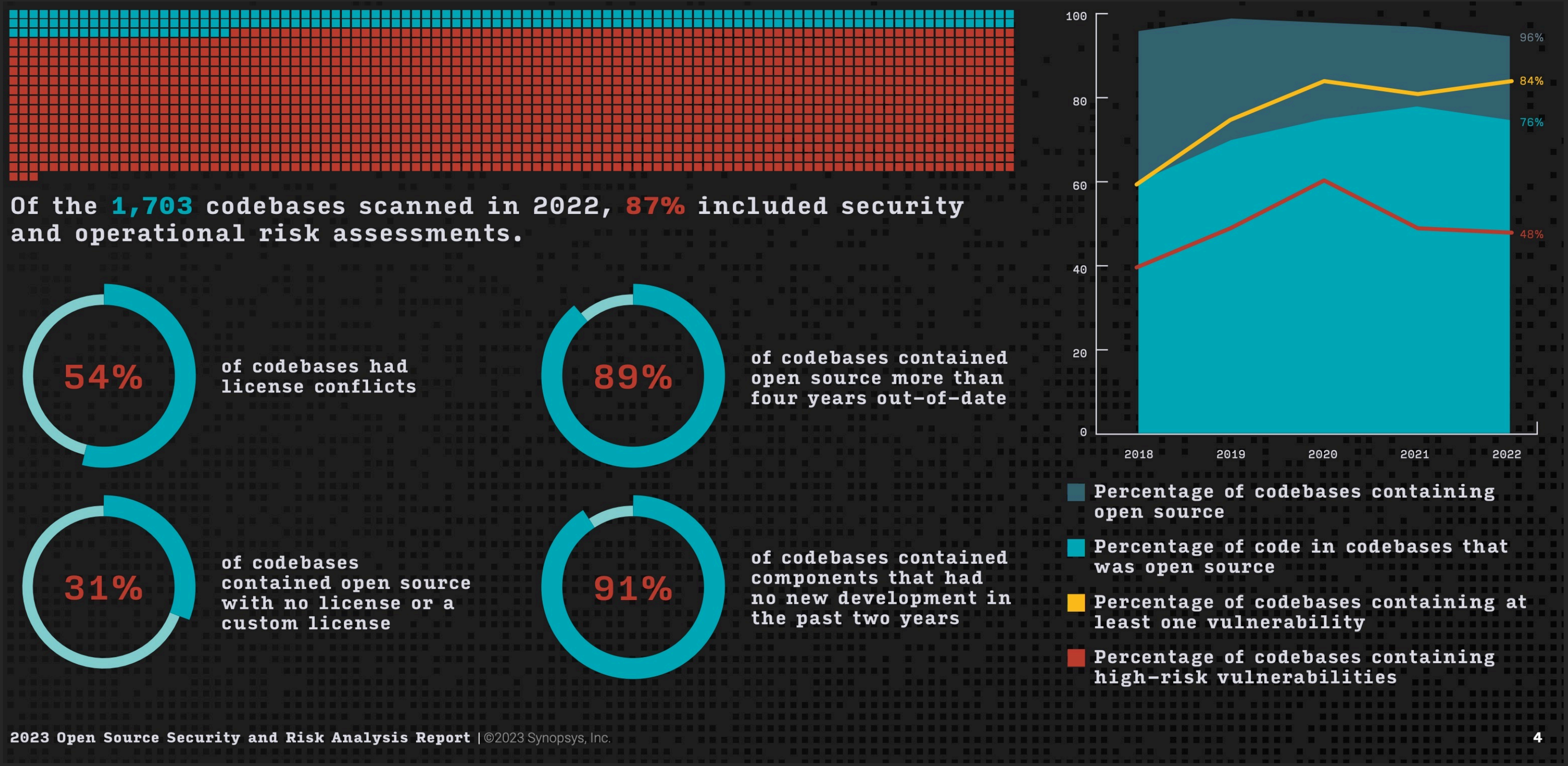
State of Open Source Security Report 2023, Snyk

snyk

Your App vs. Your Dependencies



2023 Synopsys Report



Of the 1,703 codebases scanned in 2022, 87% included security and operational risk assessments.

54% of codebases had license conflicts

89% of codebases contained open source more than four years out-of-date

31% of codebases contained open source with no license or a custom license

91% of codebases contained components that had no new development in the past two years

■ Percentage of codebases containing open source

🟦 Percentage of code in codebases that was open source

🟨 Percentage of codebases containing at least one vulnerability

🟥 Percentage of codebases containing high-risk vulnerabilities

Three Things

🗃️

Inventory

Create an inventory of your apps and dependencies

🔍

Scan

Scan your dependencies for known vulnerabilities

🔄

Update

Regularly update your dependencies

🗃️ Inventory

SBOM

Software Bill of Materials

- List of all software dependencies (including transitive)
- With versions
- Usually also the license
- Sometimes with vulnerabilities

Formats

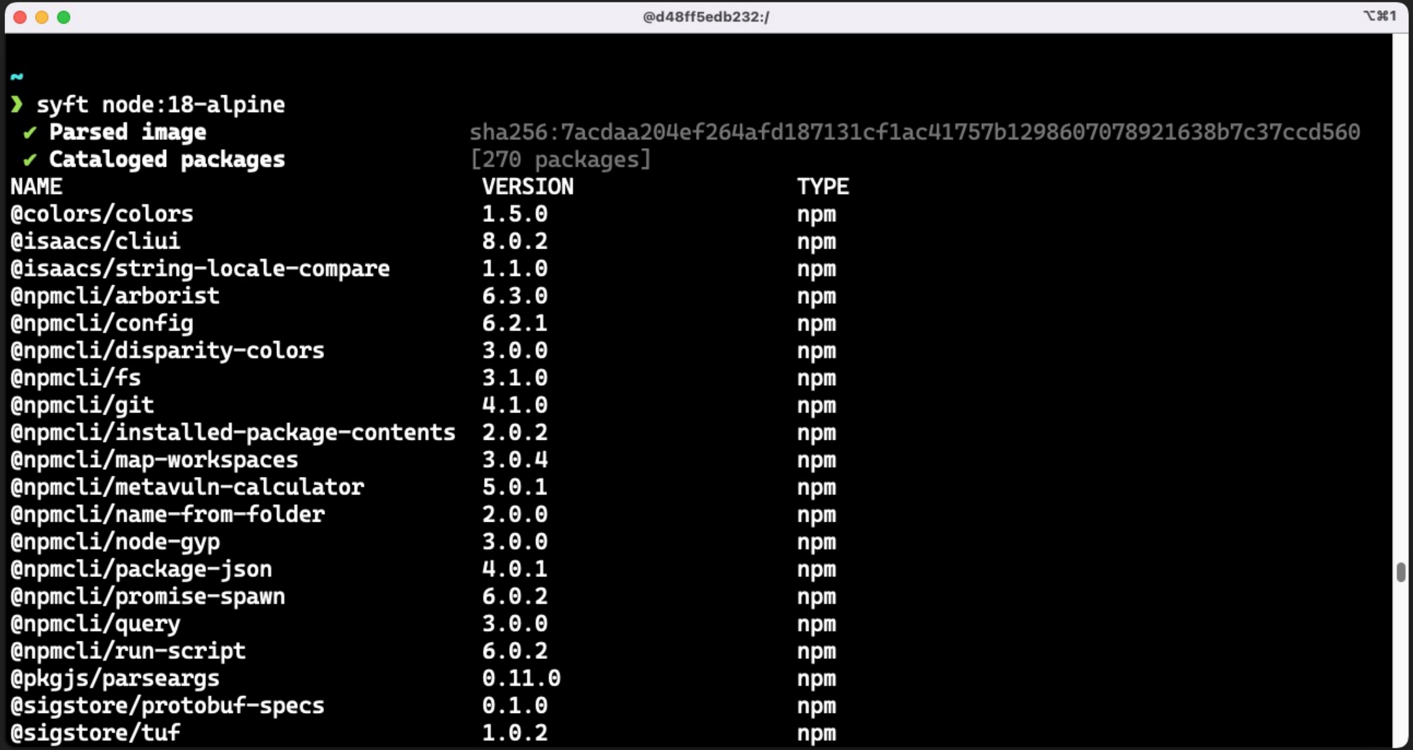
- SPDX® - Software Package Data Exchange (Linux Foundation)
- CycloneDX (OWASP)

Demo

Anchore syft + OWASP Dependency Track

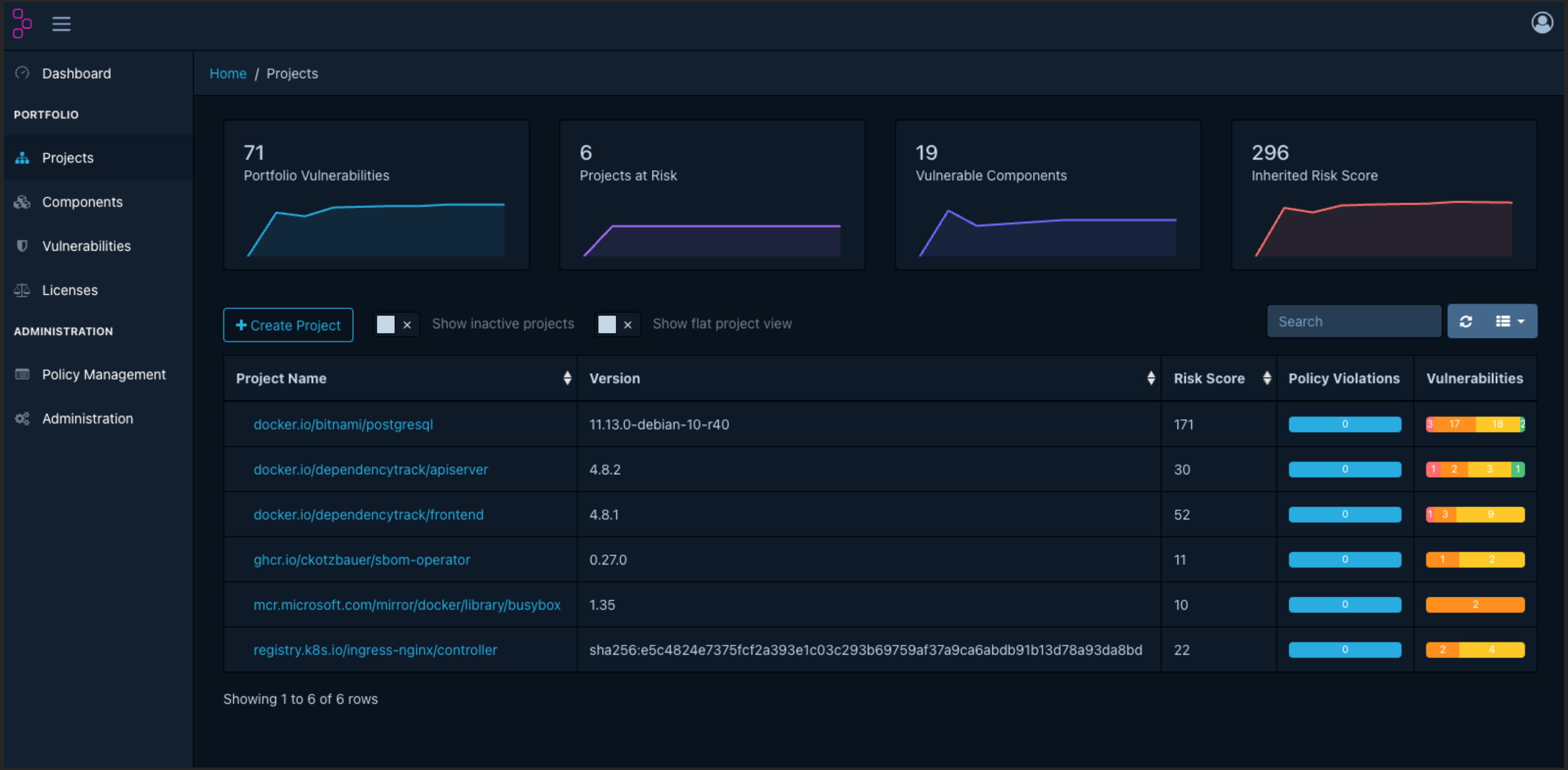
Code: https://github.com/derkoe/kcd-austria2023

Syft Demo



```
~
❯ syft node:18-alpine
 ✔ Parsed image                    sha256:7acdaa204ef264afd187131cf1ac41757b1298607078921638b7c37ccd560
 ✔ Cataloged packages              [270 packages]
NAME                                VERSION                 TYPE
@colors/colors                      1.5.0                   npm
@isaacs/cliui                       8.0.2                   npm
@isaacs/string-locale-compare       1.1.0                   npm
@npmcli/arborist                    6.3.0                   npm
@npmcli/config                      6.2.1                   npm
@npmcli/disparity-colors            3.0.0                   npm
@npmcli/fs                          3.1.0                   npm
@npmcli/git                         4.1.0                   npm
@npmcli/installed-package-contents  2.0.2                   npm
@npmcli/map-workspaces              3.0.4                   npm
@npmcli/metavuln-calculator         5.0.1                   npm
@npmcli/name-from-folder            2.0.0                   npm
@npmcli/node-gyp                    3.0.0                   npm
@npmcli/package-json                4.0.1                   npm
@npmcli/promise-spawn               6.0.2                   npm
@npmcli/query                       3.0.0                   npm
@npmcli/run-script                  6.0.2                   npm
@pkgjs/parseargs                    0.11.0                  npm
@sigstore/protobuf-specs            0.1.0                   npm
@sigstore/tuf                       1.0.2                   npm
```

SBOM Operator + Dependency Track



71 Portfolio Vulnerabilities

6 Projects at Risk

19 Vulnerable Components

296 Inherited Risk Score

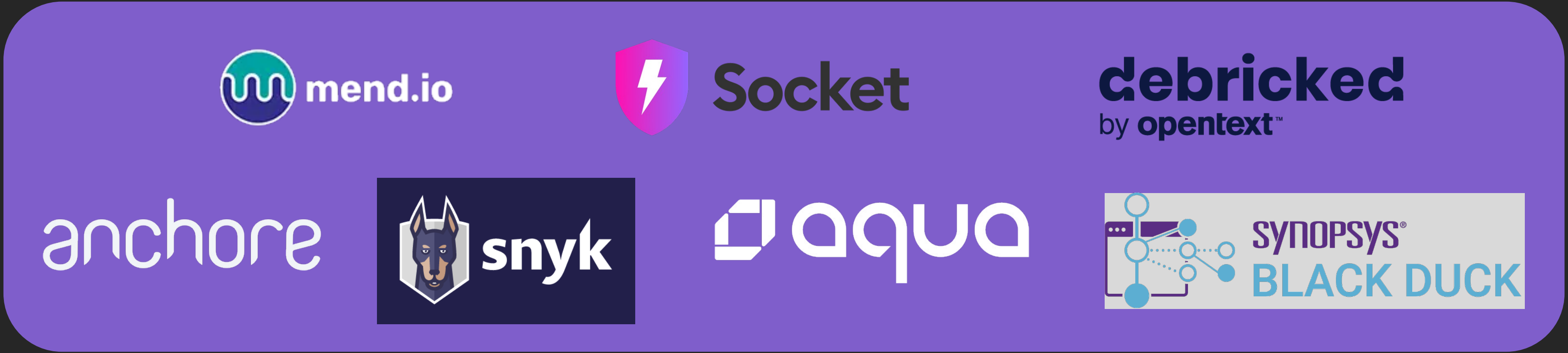
Project Name	Version	Risk Score	Policy Violations	Vulnerabilities
docker.io/bitnami/postgresql	11.13.0-debian-10-r40	171	0	3 17 18 2
docker.io/dependencytrack/apiserver	4.8.2	30	0	1 2 3 1
docker.io/dependencytrack/frontend	4.8.1	52	0	1 3 9
ghcr.io/ckotzbauer/sbom-operator	0.27.0	11	0	1 2
mcr.microsoft.com/mirror/docker/library/busybox	1.35	10	0	2
registry.k8s.io/ingress-nginx/controller	sha256:e5c4824e7375fcf2a393e1c03c293b69759af37a9ca6abdb91b13d78a93da8bd	22	0	2 4

Showing 1 to 6 of 6 rows

🔍 Scan

Security Scanners

aqua
trivy
clair
grype



Major Issue

False Positives

🔄 Update

Continuous Dependency Updates

Renovate

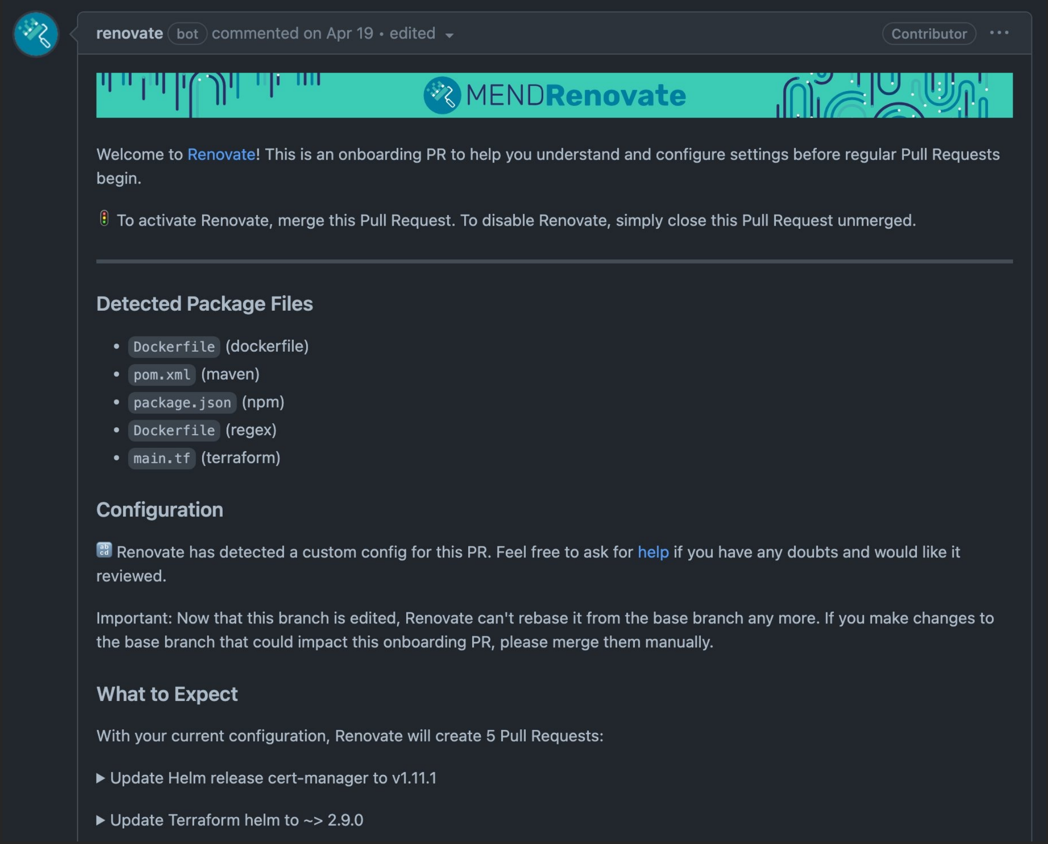
DependaBot

Demo

Renovate

Code: https://github.com/derkoe/kcd-austria2023

Renovate Demo



renovate bot commented on Apr 19 • edited

Contributor

MEND Renovate

Welcome to Renovate! This is an onboarding PR to help you understand and configure settings before regular Pull Requests begin.

🚦 To activate Renovate, merge this Pull Request. To disable Renovate, simply close this Pull Request unmerged.

Detected Package Files

- `Dockerfile` (dockerfile)
- `pom.xml` (maven)
- `package.json` (npm)
- `Dockerfile` (regex)
- `main.tf` (terraform)

Configuration

🔡 Renovate has detected a custom config for this PR. Feel free to ask for help if you have any doubts and would like it reviewed.

Important: Now that this branch is edited, Renovate can't rebase it from the base branch any more. If you make changes to the base branch that could impact this onboarding PR, please merge them manually.

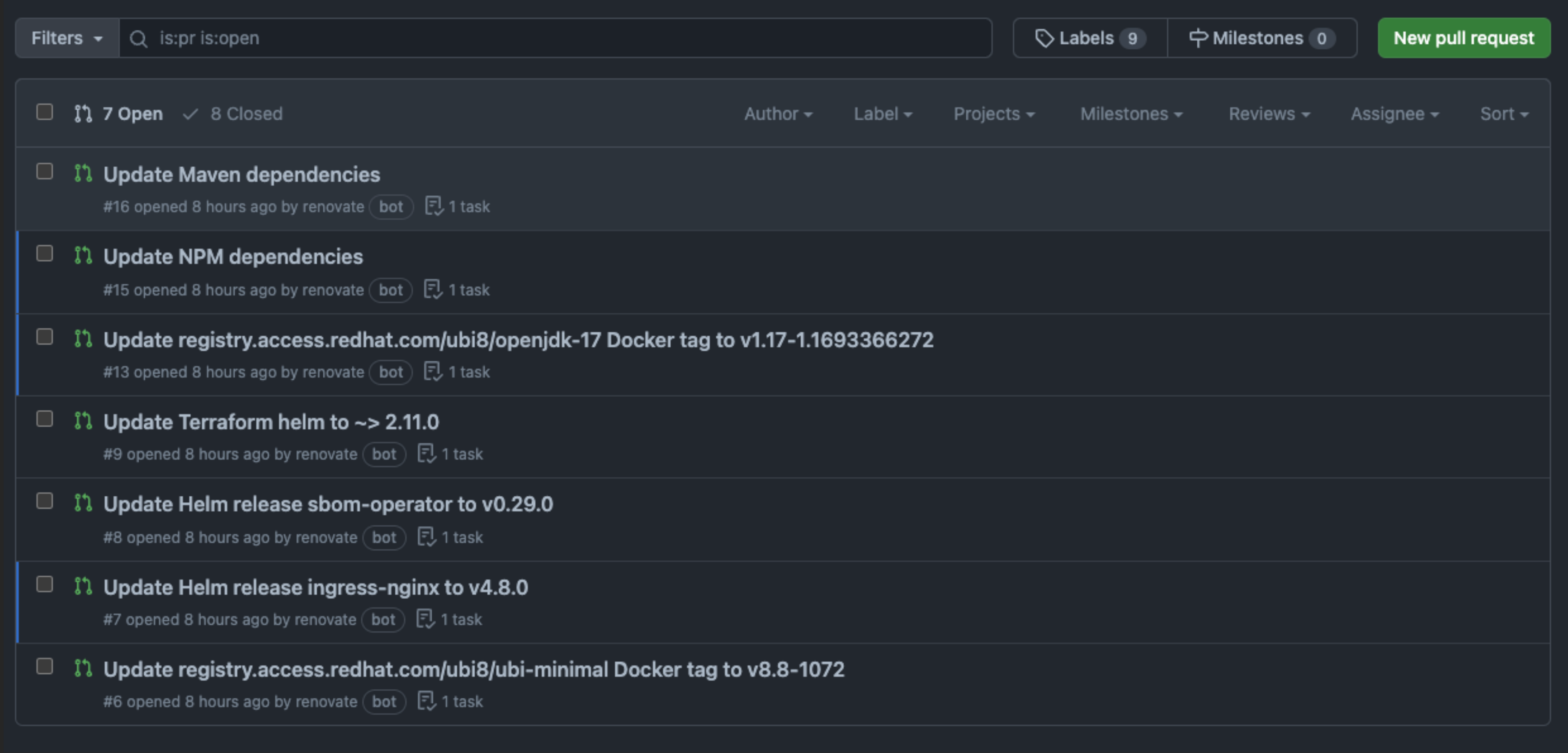
What to Expect

With your current configuration, Renovate will create 5 Pull Requests:

▶ Update Helm release cert-manager to v1.11.1

▶ Update Terraform helm to ~> 2.9.0

Renovate Demo



7 Open ✓ 8 Closed

□ **Update Maven dependencies**
#16 opened 8 hours ago by renovate bot 1 task

□ **Update NPM dependencies**
#15 opened 8 hours ago by renovate bot 1 task

□ **Update registry.access.redhat.com/ubi8/openjdk-17 Docker tag to v1.17-1.1693366272**
#13 opened 8 hours ago by renovate bot 1 task

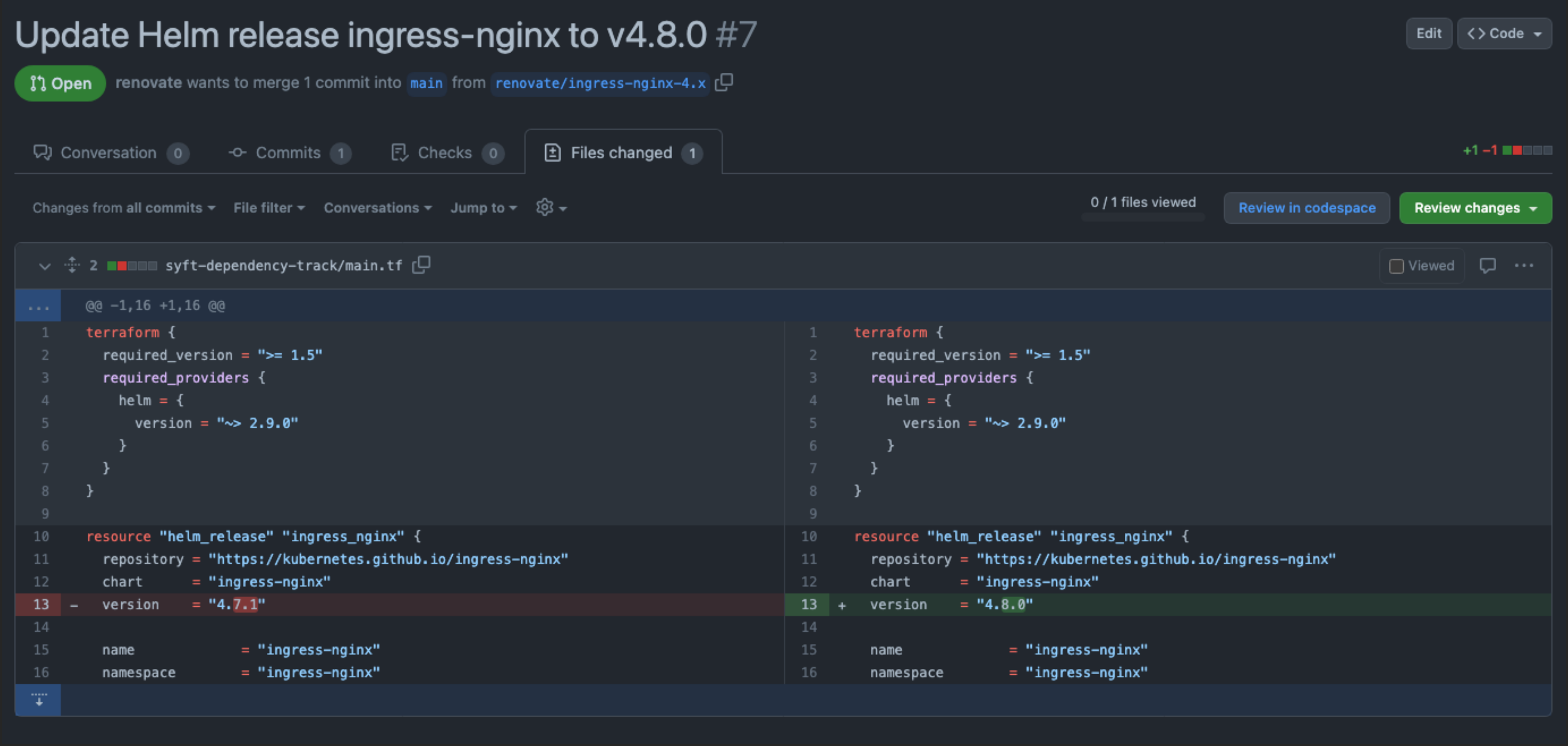
□ **Update Terraform helm to ~> 2.11.0**
#9 opened 8 hours ago by renovate bot 1 task

□ **Update Helm release sbom-operator to v0.29.0**
#8 opened 8 hours ago by renovate bot 1 task

□ **Update Helm release ingress-nginx to v4.8.0**
#7 opened 8 hours ago by renovate bot 1 task

□ **Update registry.access.redhat.com/ubi8/ubi-minimal Docker tag to v8.8-1072**
#6 opened 8 hours ago by renovate bot 1 task

Renovate Demo



Update Helm release ingress-nginx to v4.8.0 #7

Open renovate wants to merge 1 commit into main from renovate/ingress-nginx-4.x

2 syft-dependency-track/main.tf

```
@@ -1,16 +1,16 @@
terraform {
  required_version = ">= 1.5"
  required_providers {
    helm = {
      version = "~> 2.9.0"
    }
  }
}

resource "helm_release" "ingress_nginx" {
  repository = "https://kubernetes.github.io/ingress-nginx"
  chart      = "ingress-nginx"
-  version    = "4.7.1"
+  version    = "4.8.0"

  name             = "ingress-nginx"
  namespace        = "ingress-nginx"
```

Conclusion

Remember the three things

🗃️ Inventory

🔍 Scan

🔄 Update

Open Source security tools are awesome 🎉

Thank you!

- github.com/derkoe
- derkoe.dev
- @derkoe
- @derkoe@mastodon.social

PORSCHE INFORMATIK 🤫 We are hiring:
https://www.porscheinformatik.com/en/career/

Sources

- State of Open Source Security Report 2023, Snyk
- 2023 Open Source Security and Risk Analysis, Synopsys
- Anchore's syft and grype
- SBOM Operator
- OWASP Dependency Track
- OWASP Defect Dojo
- Renovate Bot (Renovate Docs)
- Snyk: The State of Open Source Security 2020
- Whitesource: The State of Open Source Security Vulnerabilites 2021

Thank you