KubeCon | CloudNativeCon

Europe 2025

SIG Security: Succession Planting for a Flowering Future

Cailyn Edwards - Auth0 by Okta
Iain Smart - AmberWolf
Rory McCune - Datadog
Mahé Tardy - Isovalent at Cisco
Tabitha Sable - Datadog

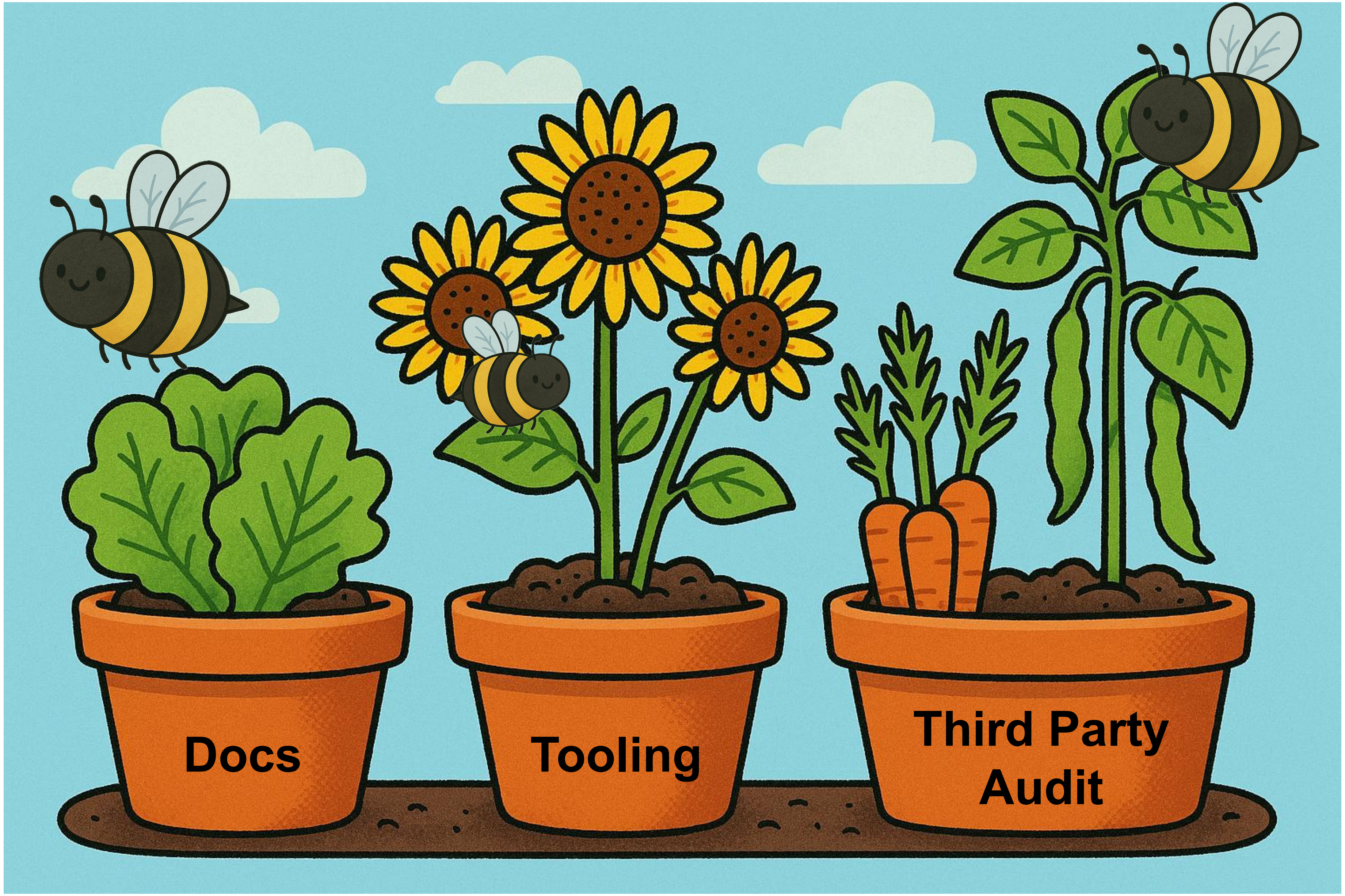
Intro to SIG-Security

Kubernetes SIG Security takes a community based approach to improve security for Kubernetes users and the project itself.

A horizontal SIG, we work together with our sibling SIGs to help them maintain and improve the security of code in their area. We also maintain security-related tools and processes used by the project overall, such as the CVE feed and external audits.

We have grown organically, attracting and nurturing contributions from all sorts of people, from experts to beginners.

The Subprojects



Future Plans

- 2025 Third Party Audit
- Ensure that the Kubernetes docs cover the security essentials
- Strengthen relationships with other SIGs
- Contribute to external kubernetes security documentation

Third Party Audit

Everyone loves an audit

Third Party Audit

A bit of history

Third Party Audit

Current state

What is SIG-Security-Docs?

this subproject works across SIGs to improve the security content of Kubernetes documentation, as well as independently create security docs in the form of concepts/blogs

Why Write Docs?

Build your understanding of project features

Why Write Docs?

Learn cool new things about Kubernetes

Why Write Docs?

Working with other parts of the project

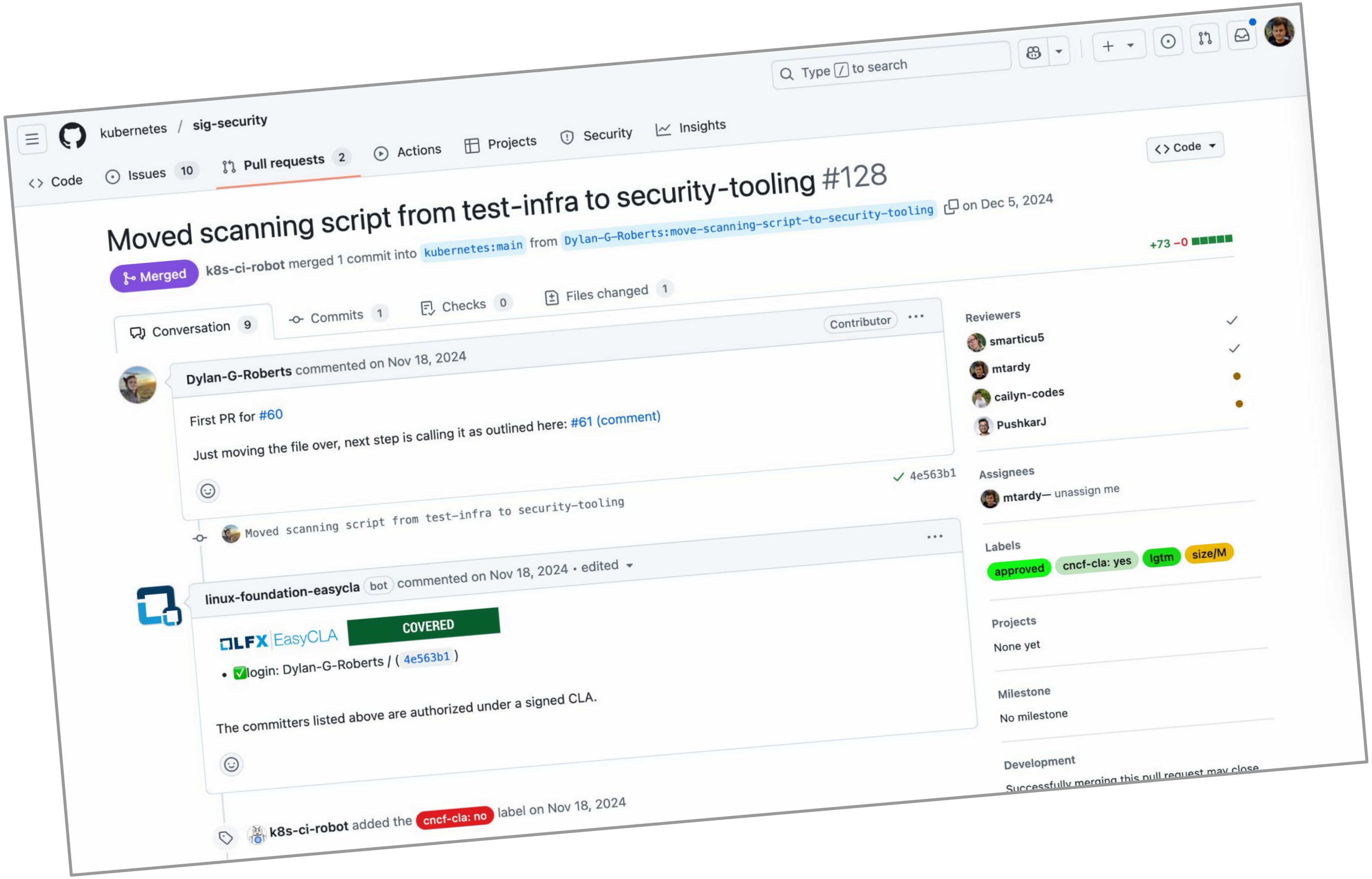
What are SIG-security tooling goals

- Build and improve security of Kubernetes by **working across SIGs** and other sub-projects.
- Create space for **new contributors** to share and learn.

How can you join the tooling subproject

- We have meetings at 14:00 UTC every other Friday
- You can propose learning sessions to present security tooling related work you’ve been working on!
- Or just join the working sessions to progress together.

Snyk scanner maintenance



Type / to search

kubernetes / sig-security

Code · Issues 10 · Pull requests 2 · Actions · Projects · Security · Insights

Moved scanning script from test-infra to security-tooling #128

Code

Merged k8s-ci-robot merged 1 commit into `kubernetes:main` from `Dylan-G-Roberts:move-scanning-script-to-security-tooling` on Dec 5, 2024

+73 −0

Conversation 9 · Commits 1 · Checks 0 · Files changed 1

Dylan-G-Roberts commented on Nov 18, 2024 · Contributor ···

First PR for #60

Just moving the file over, next step is calling it as outlined here: #61 (comment)

`Moved scanning script from test-infra to security-tooling` ✓ 4e563b1

linux-foundation-easycla bot commented on Nov 18, 2024 • edited ···

LFX EasyCLA COVERED

- ✅login: Dylan-G-Roberts / (4e563b1)

The committers listed above are authorized under a signed CLA.

k8s-ci-robot added the cncf-cla: no label on Nov 18, 2024

Reviewers

smarticu5	✓
mtardy	✓
cailyn-codes	●
PushkarJ	●

Assignees

mtardy— unassign me

Labels

approved · cncf-cla: yes · lgtm · size/M

Projects

None yet

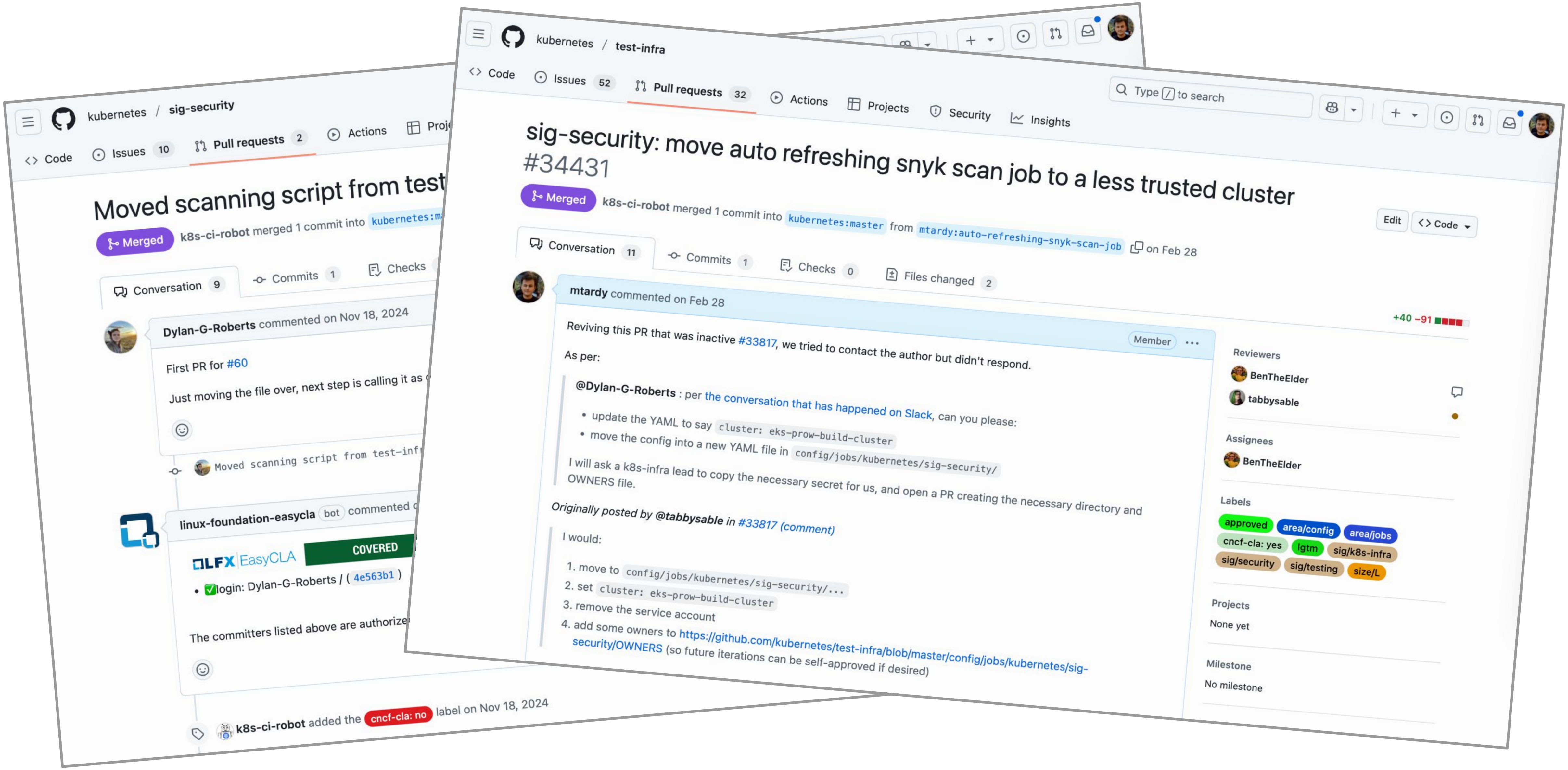
Milestone

No milestone

Development

Successfully merging this pull request may close

Snyk scanner maintenance



Moved scanning script from test

Merged k8s-ci-robot merged 1 commit into kubernetes:m

Dylan-G-Roberts commented on Nov 18, 2024

First PR for #60

Just moving the file over, next step is calling it as

Moved scanning script from test-inf

linux-foundation-easycla bot commented

LFX EasyCLA COVERED

- ✅login: Dylan-G-Roberts / (4e563b1)

The committers listed above are authorize

k8s-ci-robot added the cncf-cla: no label on Nov 18, 2024

sig-security: move auto refreshing snyk scan job to a less trusted cluster #34431

Merged k8s-ci-robot merged 1 commit into kubernetes:master from mtardy:auto-refreshing-snyk-scan-job on Feb 28

mtardy commented on Feb 28 Member

Reviving this PR that was inactive #33817, we tried to contact the author but didn't respond.

As per:

> **@Dylan-G-Roberts** : per the conversation that has happened on Slack, can you please:
>
> - update the YAML to say `cluster: eks-prow-build-cluster`
> - move the config into a new YAML file in `config/jobs/kubernetes/sig-security/`
>
> I will ask a k8s-infra lead to copy the necessary secret for us, and open a PR creating the necessary directory and OWNERS file.

*Originally posted by **@tabbysable** in #33817 (comment)*

> I would:
>
> 1. move to `config/jobs/kubernetes/sig-security/...`
> 2. set `cluster: eks-prow-build-cluster`
> 3. remove the service account
> 4. add some owners to https://github.com/kubernetes/test-infra/blob/master/config/jobs/kubernetes/sig-security/OWNERS (so future iterations can be self-approved if desired)

Reviewers

BenTheElder

tabbysable

Assignees

BenTheElder

Labels

approved area/config area/jobs cncf-cla: yes lgtm sig/k8s-infra sig/security sig/testing size/L

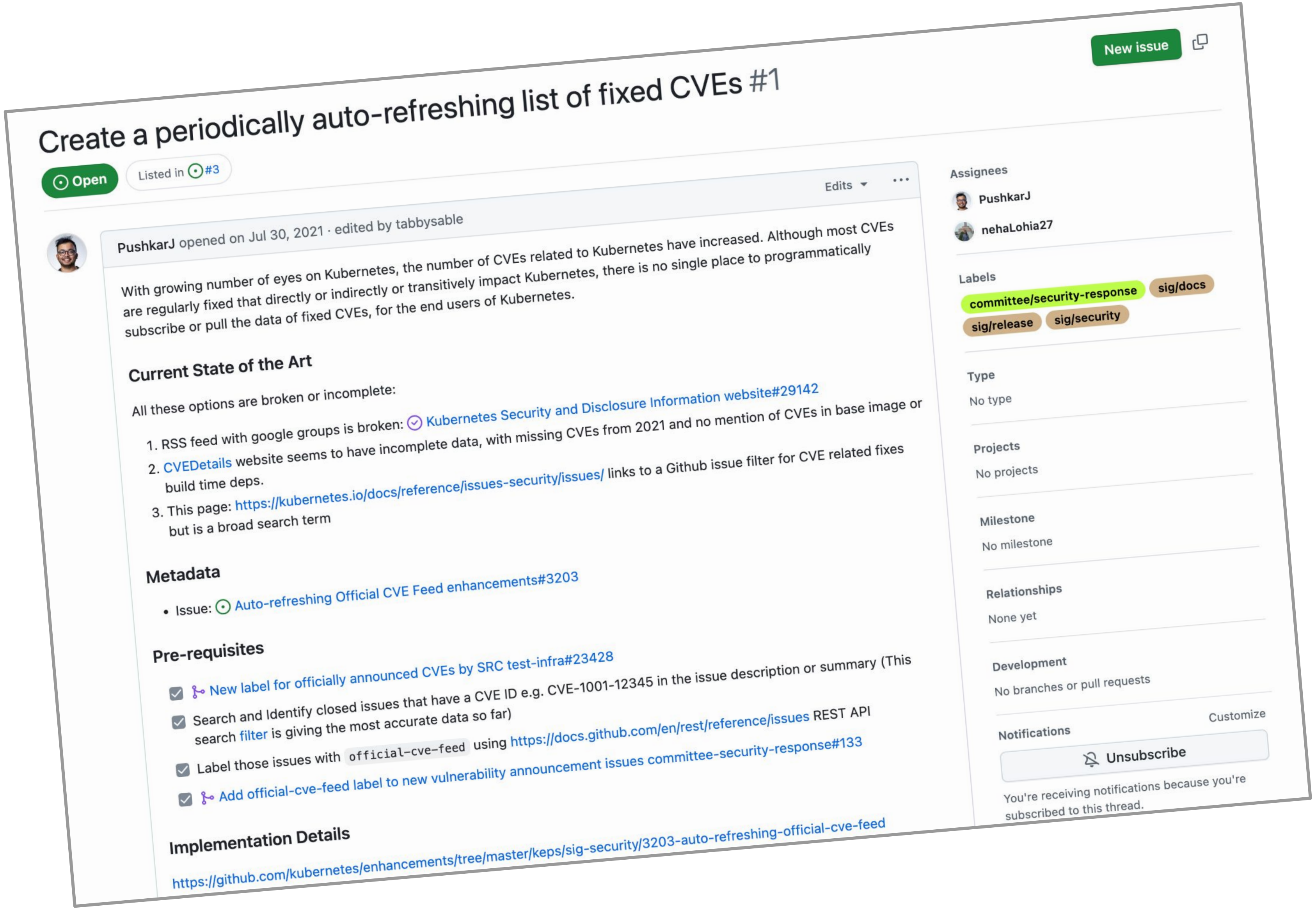
Projects

None yet

Milestone

No milestone

Official CVE feed



Create a periodically auto-refreshing list of fixed CVEs #1

PushkarJ opened on Jul 30, 2021 · edited by tabbysable

With growing number of eyes on Kubernetes, the number of CVEs related to Kubernetes have increased. Although most CVEs are regularly fixed that directly or indirectly or transitively impact Kubernetes, there is no single place to programmatically subscribe or pull the data of fixed CVEs, for the end users of Kubernetes.

Current State of the Art

All these options are broken or incomplete:

1. RSS feed with google groups is broken: Kubernetes Security and Disclosure Information website#29142
2. CVEDetails website seems to have incomplete data, with missing CVEs from 2021 and no mention of CVEs in base image or build time deps.
3. This page: https://kubernetes.io/docs/reference/issues-security/issues/ links to a Github issue filter for CVE related fixes but is a broad search term

Metadata

- Issue: Auto-refreshing Official CVE Feed enhancements#3203

Pre-requisites

- ☑ New label for officially announced CVEs by SRC test-infra#23428
- ☑ Search and Identify closed issues that have a CVE ID e.g. CVE-1001-12345 in the issue description or summary (This search filter is giving the most accurate data so far)
- ☑ Label those issues with `official-cve-feed` using https://docs.github.com/en/rest/reference/issues REST API
- ☑ Add official-cve-feed label to new vulnerability announcement issues committee-security-response#133

Implementation Details

https://github.com/kubernetes/enhancements/tree/master/keps/sig-security/3203-auto-refreshing-official-cve-feed

Assignees

PushkarJ
nehaLohia27

Labels

committee/security-response · sig/docs · sig/release · sig/security

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

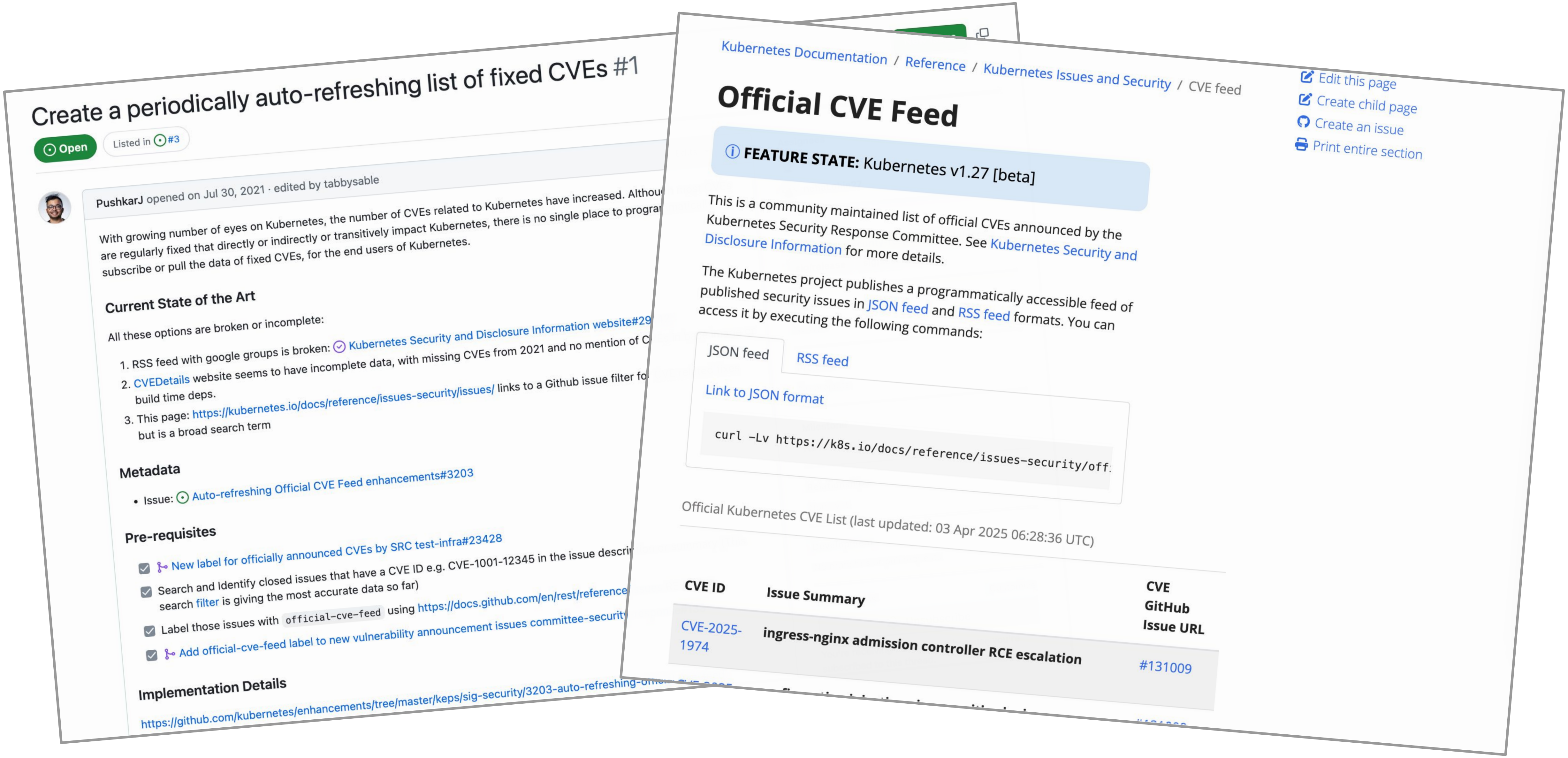
Development

No branches or pull requests

Notifications Customize

You're receiving notifications because you're subscribed to this thread.

Official CVE feed



Create a periodically auto-refreshing list of fixed CVEs #1

PushkarJ opened on Jul 30, 2021 · edited by tabbysable

With growing number of eyes on Kubernetes, the number of CVEs related to Kubernetes have increased. Althou are regularly fixed that directly or indirectly or transitively impact Kubernetes, there is no single place to progra subscribe or pull the data of fixed CVEs, for the end users of Kubernetes.

Current State of the Art

All these options are broken or incomplete:

1. RSS feed with google groups is broken: Kubernetes Security and Disclosure Information website#29
2. CVEDetails website seems to have incomplete data, with missing CVEs from 2021 and no mention of C build time deps.
3. This page: https://kubernetes.io/docs/reference/issues-security/issues/ links to a Github issue filter fo but is a broad search term

Metadata

- Issue: Auto-refreshing Official CVE Feed enhancements#3203

Pre-requisites

- ☑ New label for officially announced CVEs by SRC test-infra#23428
- ☑ Search and Identify closed issues that have a CVE ID e.g. CVE-1001-12345 in the issue descri search filter is giving the most accurate data so far)
- ☑ Label those issues with `official-cve-feed` using https://docs.github.com/en/rest/reference
- ☑ Add official-cve-feed label to new vulnerability announcement issues committee-security

Implementation Details

https://github.com/kubernetes/enhancements/tree/master/keps/sig-security/3203-auto-refreshing-offici

Kubernetes Documentation / Reference / Kubernetes Issues and Security / CVE feed

Official CVE Feed

FEATURE STATE: Kubernetes v1.27 [beta]

This is a community maintained list of official CVEs announced by the Kubernetes Security Response Committee. See Kubernetes Security and Disclosure Information for more details.

The Kubernetes project publishes a programmatically accessible feed of published security issues in JSON feed and RSS feed formats. You can access it by executing the following commands:

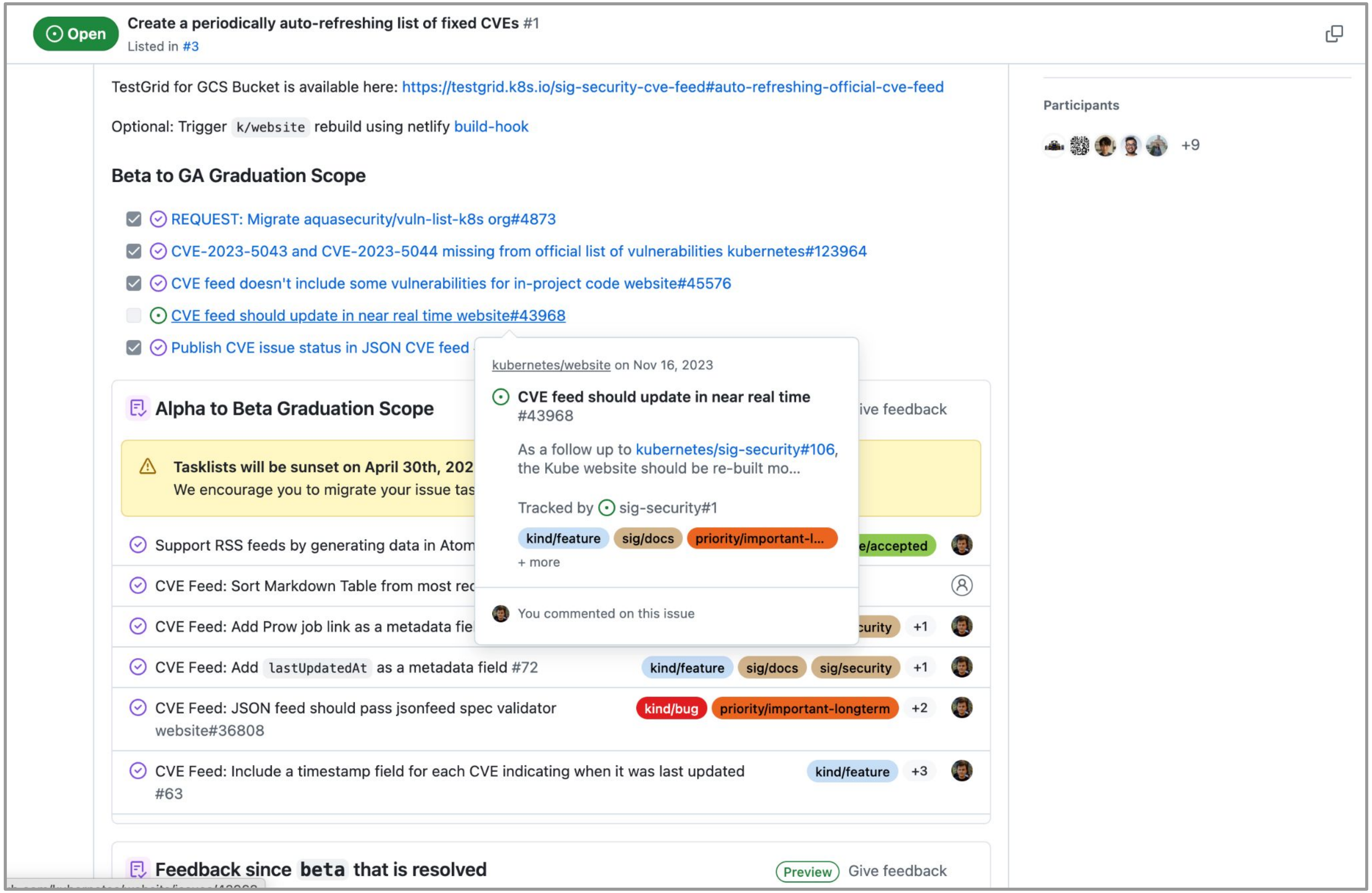
Link to JSON format

```
curl -Lv https://k8s.io/docs/reference/issues-security/off:
```

Official Kubernetes CVE List (last updated: 03 Apr 2025 06:28:36 UTC)

CVE ID	Issue Summary	CVE GitHub Issue URL
CVE-2025-1974	ingress-nginx admission controller RCE escalation	#131009

Official CVE feed



Open Create a periodically auto-refreshing list of fixed CVEs #1

Listed in #3

TestGrid for GCS Bucket is available here: https://testgrid.k8s.io/sig-security-cve-feed#auto-refreshing-official-cve-feed

Optional: Trigger `k/website` rebuild using netlify build-hook

Beta to GA Graduation Scope

- ☑ REQUEST: Migrate aquasecurity/vuln-list-k8s org#4873
- ☑ CVE-2023-5043 and CVE-2023-5044 missing from official list of vulnerabilities kubernetes#123964
- ☑ CVE feed doesn't include some vulnerabilities for in-project code website#45576
- □ CVE feed should update in near real time website#43968
- ☑ Publish CVE issue status in JSON CVE feed

kubernetes/website on Nov 16, 2023

CVE feed should update in near real time #43968

As a follow up to kubernetes/sig-security#106, the Kube website should be re-built mo...

Tracked by sig-security#1

kind/feature | sig/docs | priority/important-l...

+ more

You commented on this issue

Alpha to Beta Graduation Scope

ive feedback

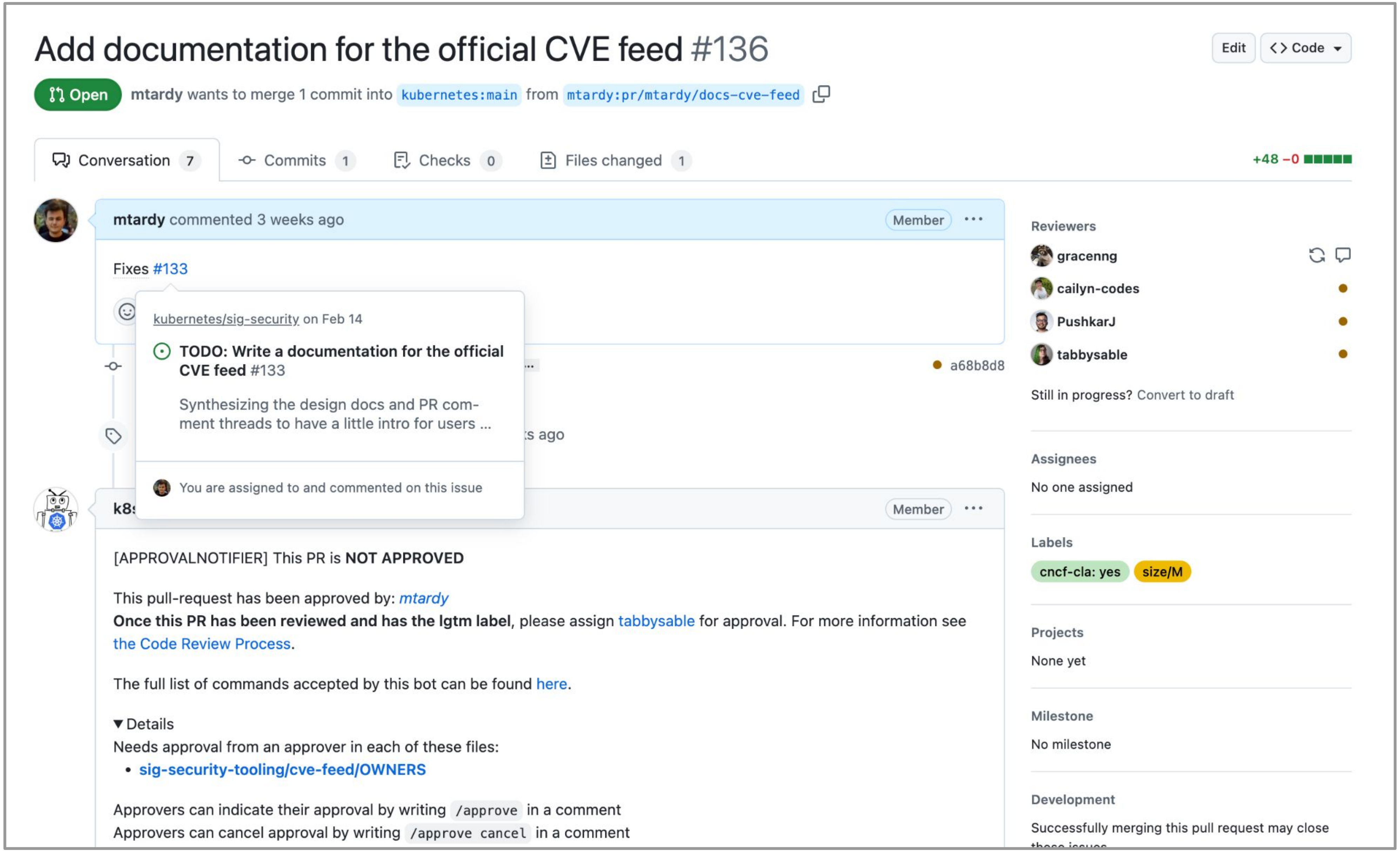
Tasklists will be sunset on April 30th, 202
We encourage you to migrate your issue tas

- Support RSS feeds by generating data in Atom — e/accepted
- CVE Feed: Sort Markdown Table from most rec
- CVE Feed: Add Prow job link as a metadata fie — curity +1
- CVE Feed: Add `lastUpdatedAt` as a metadata field #72 — kind/feature, sig/docs, sig/security +1
- CVE Feed: JSON feed should pass jsonfeed spec validator website#36808 — kind/bug, priority/important-longterm +2
- CVE Feed: Include a timestamp field for each CVE indicating when it was last updated #63 — kind/feature +3

Feedback since `beta` that is resolved

Preview Give feedback

Official CVE feed



Add documentation for the official CVE feed #136

Open mtardy wants to merge 1 commit into `kubernetes:main` from `mtardy:pr/mtardy/docs-cve-feed`

mtardy commented 3 weeks ago

Fixes #133

kubernetes/sig-security on Feb 14

TODO: Write a documentation for the official CVE feed #133

Synthesizing the design docs and PR comment threads to have a little intro for users ...

You are assigned to and commented on this issue

a68b8d8

ts ago

k8s

[APPROVALNOTIFIER] This PR is **NOT APPROVED**

This pull-request has been approved by: *mtardy*
Once this PR has been reviewed and has the lgtm label, please assign tabbysable for approval. For more information see the Code Review Process.

The full list of commands accepted by this bot can be found here.

▼Details
Needs approval from an approver in each of these files:

- **sig-security-tooling/cve-feed/OWNERS**

Approvers can indicate their approval by writing `/approve` in a comment
Approvers can cancel approval by writing `/approve cancel` in a comment

Reviewers
gracenng
cailyn-codes ●
PushkarJ ●
tabbysable ●

Still in progress? Convert to draft

Assignees
No one assigned

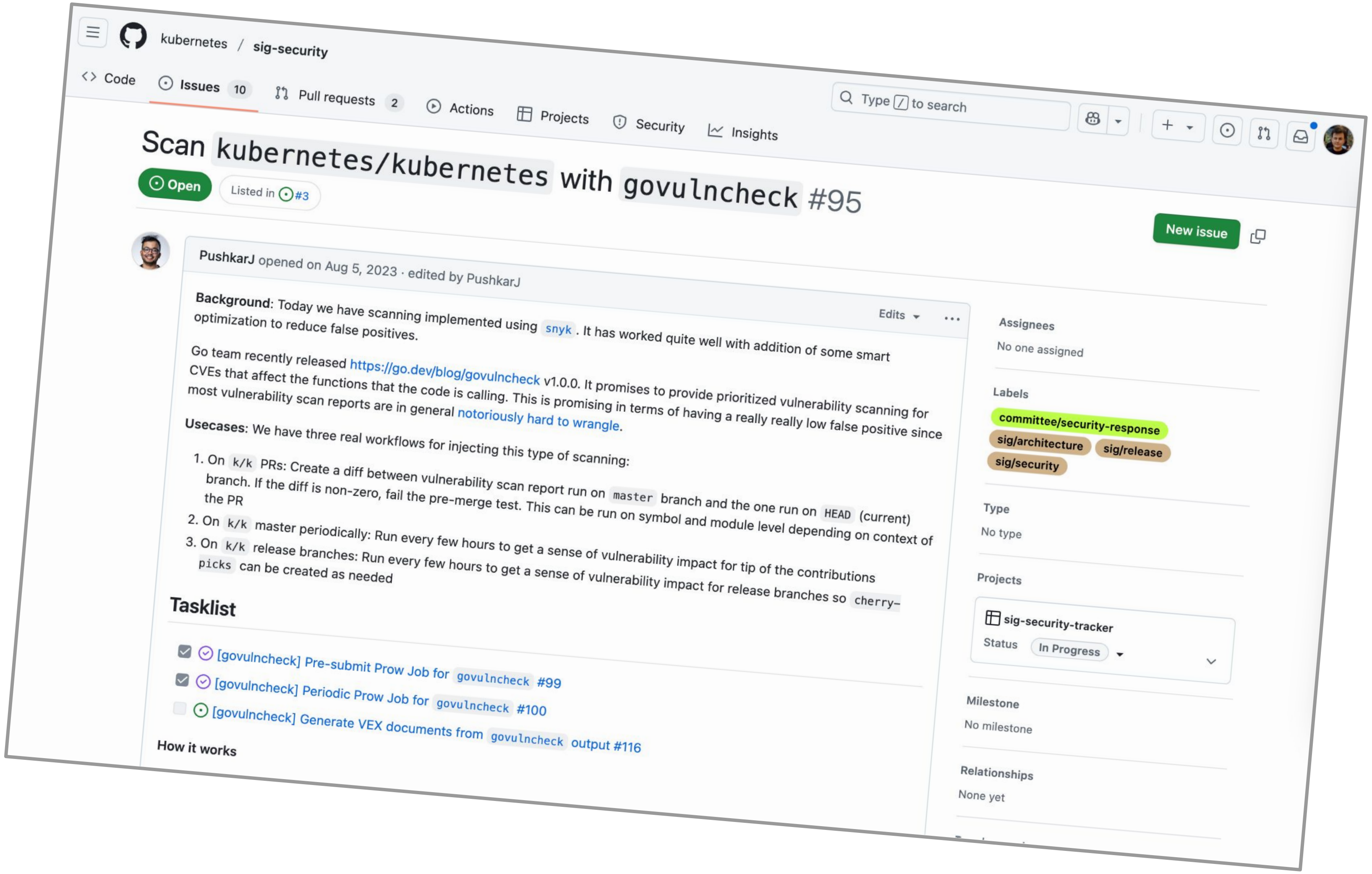
Labels
cncf-cla: yes size/M

Projects
None yet

Milestone
No milestone

Development
Successfully merging this pull request may close these issues.

Trying to merge CVE feed efforts



Scan `kubernetes/kubernetes` with `govulncheck` #95

Open · Listed in #3

PushkarJ opened on Aug 5, 2023 · edited by PushkarJ

Background: Today we have scanning implemented using `snyk`. It has worked quite well with addition of some smart optimization to reduce false positives.

Go team recently released https://go.dev/blog/govulncheck v1.0.0. It promises to provide prioritized vulnerability scanning for CVEs that affect the functions that the code is calling. This is promising in terms of having a really really low false positive since most vulnerability scan reports are in general notoriously hard to wrangle.

Usecases: We have three real workflows for injecting this type of scanning:

1. On `k/k` PRs: Create a diff between vulnerability scan report run on `master` branch and the one run on `HEAD` (current) branch. If the diff is non-zero, fail the pre-merge test. This can be run on symbol and module level depending on context of the PR
2. On `k/k` master periodically: Run every few hours to get a sense of vulnerability impact for tip of the contributions
3. On `k/k` release branches: Run every few hours to get a sense of vulnerability impact for release branches so `cherry-picks` can be created as needed

Tasklist

- ☑ [govulncheck] Pre-submit Prow Job for `govulncheck` #99
- ☑ [govulncheck] Periodic Prow Job for `govulncheck` #100
- □ [govulncheck] Generate VEX documents from `govulncheck` output #116

How it works

Assignees
No one assigned

Labels
committee/security-response
sig/architecture
sig/release
sig/security

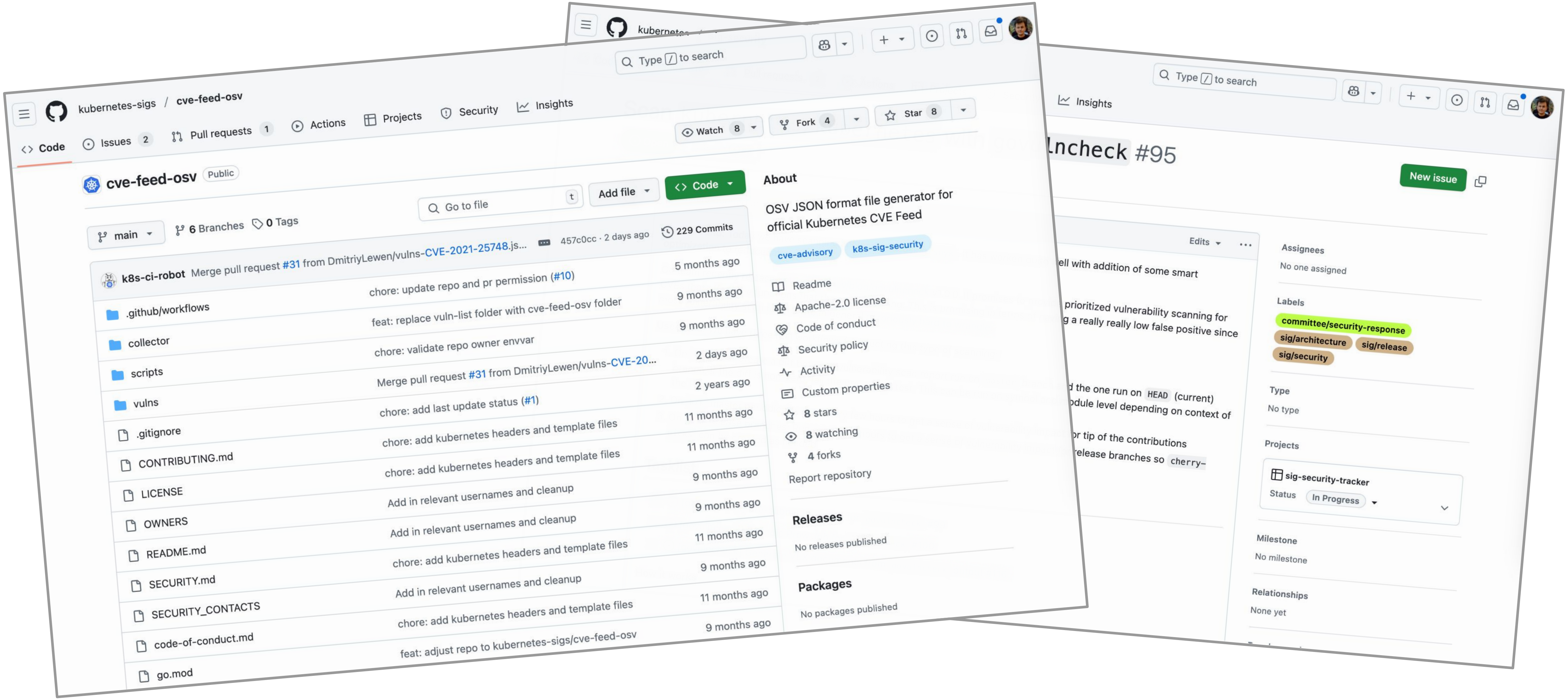
Type
No type

Projects
sig-security-tracker
Status: In Progress

Milestone
No milestone

Relationships
None yet

Trying to merge CVE feed efforts



cve-feed-osv Public

main · 6 Branches · 0 Tags · Go to file · Add file · Code

k8s-ci-robot Merge pull request #31 from DmitriyLewen/vulns-CVE-2021-25748.js... 457c0cc · 2 days ago · 229 Commits

.github/workflows	chore: update repo and pr permission (#10)	5 months ago
collector	feat: replace vuln-list folder with cve-feed-osv folder	9 months ago
scripts	chore: validate repo owner envvar	9 months ago
vulns	Merge pull request #31 from DmitriyLewen/vulns-CVE-20...	2 days ago
.gitignore	chore: add last update status (#1)	2 years ago
CONTRIBUTING.md	chore: add kubernetes headers and template files	11 months ago
LICENSE	chore: add kubernetes headers and template files	11 months ago
OWNERS	Add in relevant usernames and cleanup	9 months ago
README.md	Add in relevant usernames and cleanup	9 months ago
SECURITY.md	chore: add kubernetes headers and template files	11 months ago
SECURITY_CONTACTS	Add in relevant usernames and cleanup	9 months ago
code-of-conduct.md	chore: add kubernetes headers and template files	11 months ago
go.mod	feat: adjust repo to kubernetes-sigs/cve-feed-osv	9 months ago

About

OSV JSON format file generator for official Kubernetes CVE Feed

cve-advisory · k8s-sig-security

- Readme
- Apache-2.0 license
- Code of conduct
- Security policy
- Activity
- Custom properties
- 8 stars
- 8 watching
- 4 forks

Report repository

Releases

No releases published

Packages

No packages published

ncheck #95

New issue

Edits

...ell with addition of some smart

...prioritized vulnerability scanning for ...g a really really low false positive since

...d the one run on `HEAD` (current) ...odule level depending on context of

...or tip of the contributions ...release branches so `cherry-`

Assignees: No one assigned

Labels: committee/security-response · sig/architecture · sig/release · sig/security

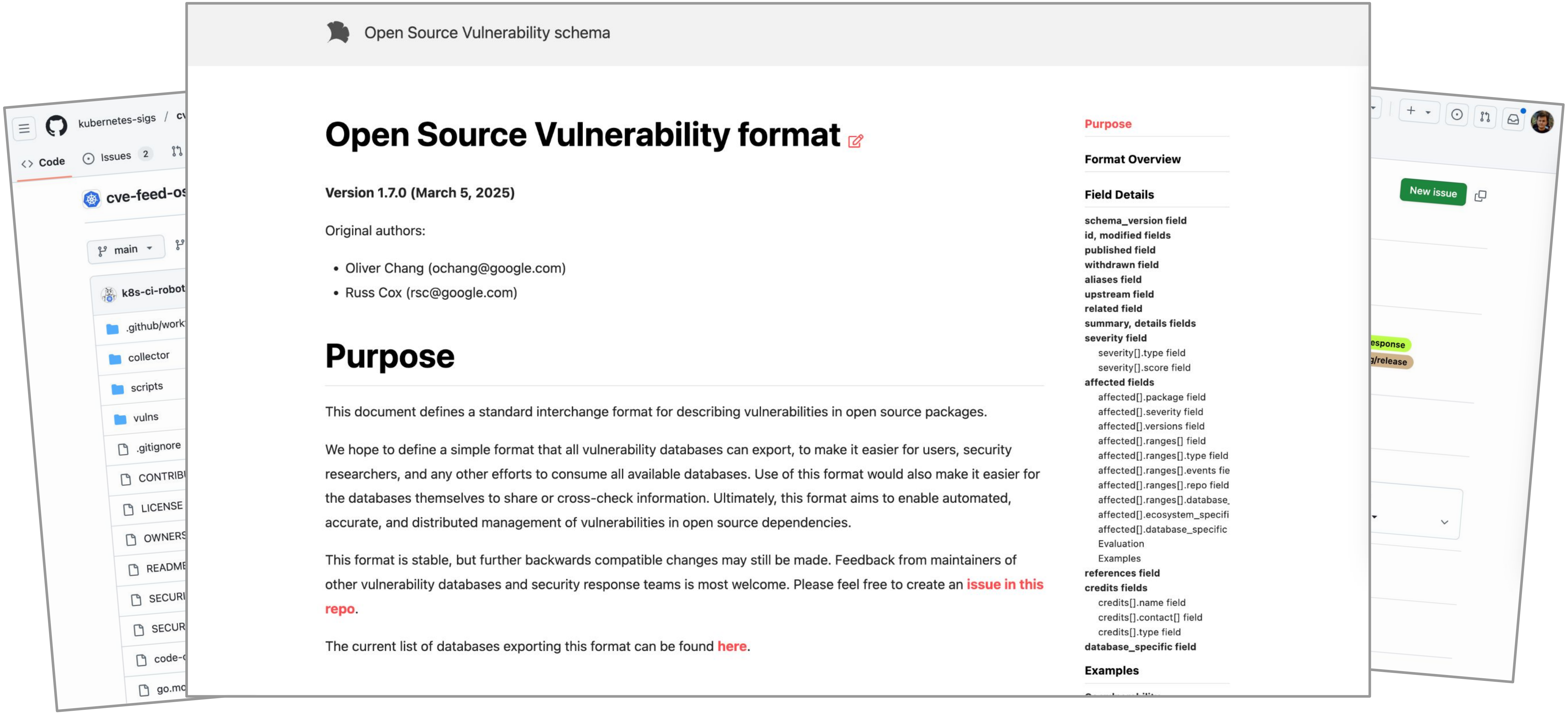
Type: No type

Projects: sig-security-tracker · Status: In Progress

Milestone: No milestone

Relationships: None yet

Trying to merge CVE feed efforts



Open Source Vulnerability schema

Open Source Vulnerability format

Version 1.7.0 (March 5, 2025)

Original authors:

- Oliver Chang (ochang@google.com)
- Russ Cox (rsc@google.com)

Purpose

This document defines a standard interchange format for describing vulnerabilities in open source packages.

We hope to define a simple format that all vulnerability databases can export, to make it easier for users, security researchers, and any other efforts to consume all available databases. Use of this format would also make it easier for the databases themselves to share or cross-check information. Ultimately, this format aims to enable automated, accurate, and distributed management of vulnerabilities in open source dependencies.

This format is stable, but further backwards compatible changes may still be made. Feedback from maintainers of other vulnerability databases and security response teams is most welcome. Please feel free to create an issue in this repo.

The current list of databases exporting this format can be found here.

How can you get involved?

SIG Security

README &
Mailing list

K8s Slack

#sig-security

Thank you!

Questions!?