Protect your code with GitHub security features

dotnetsheff

https://myoctocat.com

@robbos81

Protect your code with GitHub security features

dotnetsheff

Rob Bos

DevOps Consultant – Xpirit

The Netherlands

https://devopsjournal.io

@robbos81

https://myoctocat.com

Security features

Commit signing

Dependabot

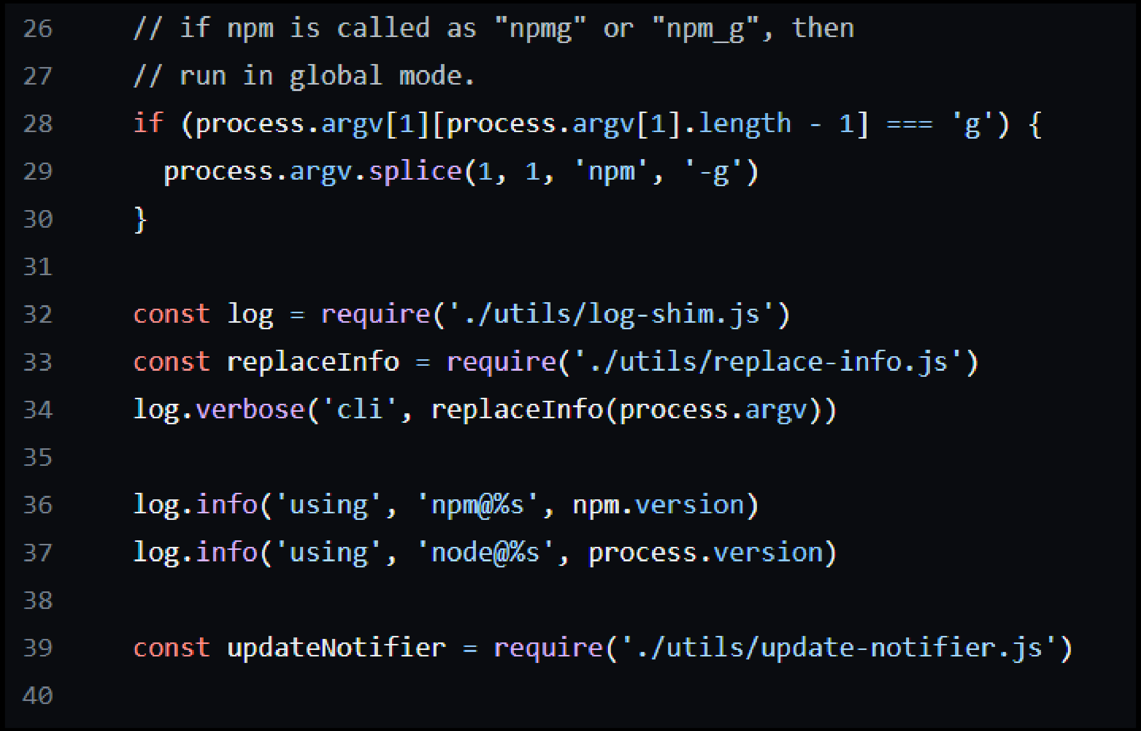
Security alerts on dependencies

Secret scanning

CodeQL

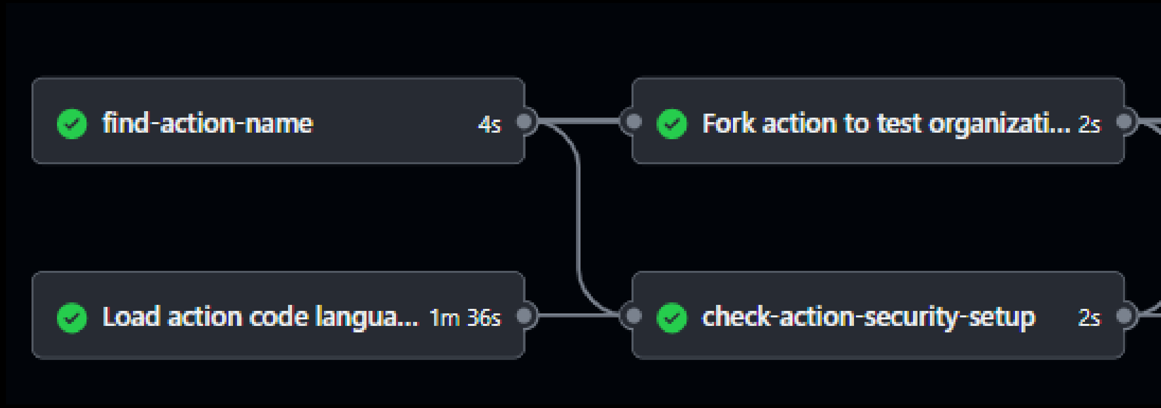
Why? Attack vectors!

your code



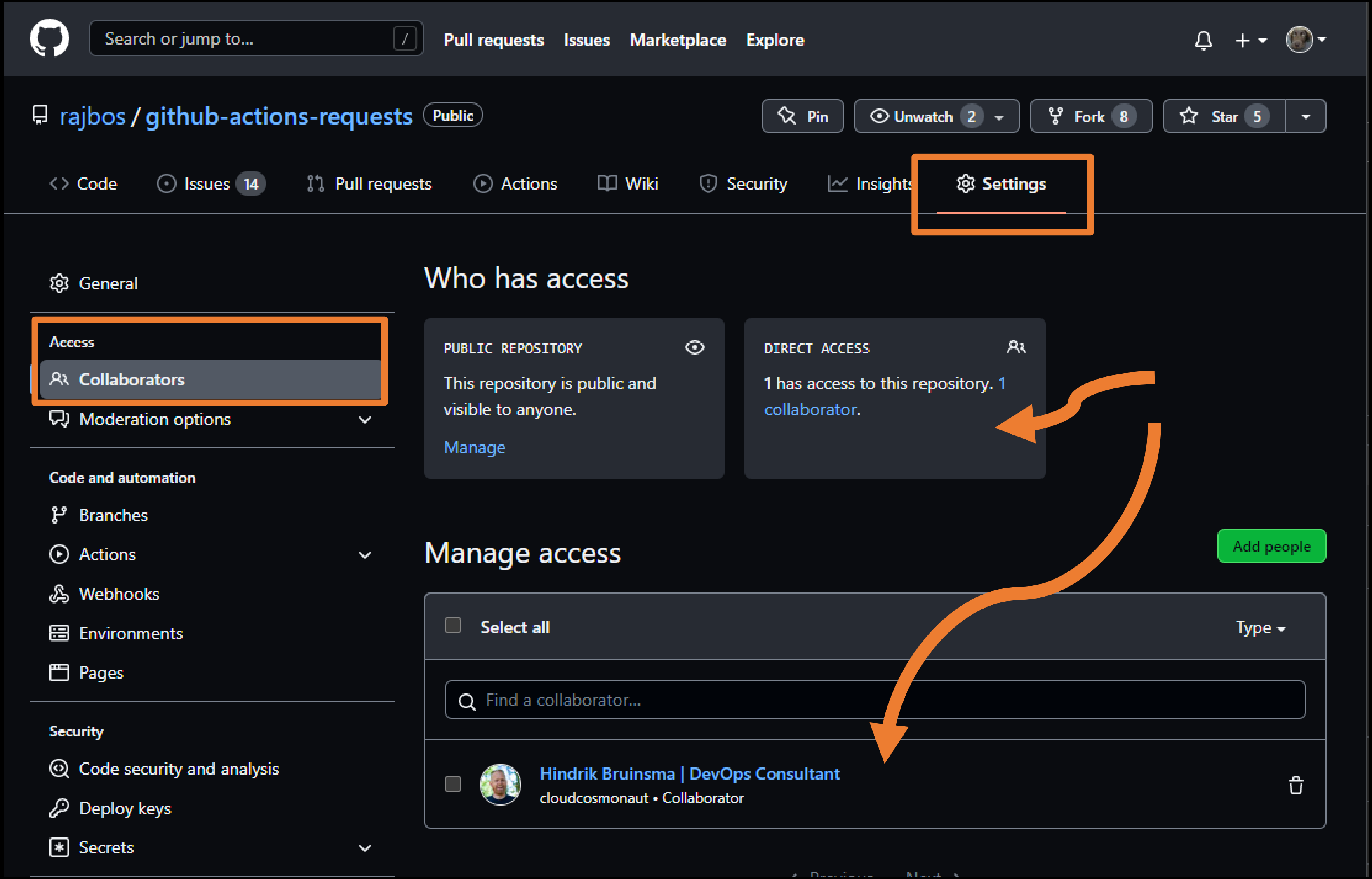
```
// if npm is called as "npmg" or "npm_g", then
// run in global mode.
if (process.argv[1][process.argv[1].length - 1] === 'g') {
  process.argv.splice(1, 1, 'npm', '-g')
}

const log = require('./utils/log-shim.js')
const replaceInfo = require('./utils/replace-info.js')
log.verbose('cli', replaceInfo(process.argv))

log.info('using', 'npm@%s', npm.version)
log.info('using', 'node@%s', process.version)

const updateNotifier = require('./utils/update-notifier.js')

```

your pipelines


find-action-name 4s
Fork action to test organizati... 2s
Load action code langua... 1m 36s
check-action-security-setup 2s

https://owasp.org/Top10

Who can push code?



Search or jump to... /

Pull requests Issues Marketplace Explore

rajbos / github-actions-requests Public

Pin | Unwatch 2 | Fork 8 | Star 5

Code | Issues 14 | Pull requests | Actions | Wiki | Security | Insights | Settings

General

Access

- Collaborators
- Moderation options

Code and automation

- Branches
- Actions
- Webhooks
- Environments
- Pages

Security

- Code security and analysis
- Deploy keys
- Secrets

Who has access

PUBLIC REPOSITORY

This repository is public and visible to anyone.

Manage

DIRECT ACCESS

1 has access to this repository. 1 collaborator.

Manage access

Add people

□ Select all Type ▾

Find a collaborator...

□ Hindrik Bruinsma | DevOps Consultant
cloudcosmonaut • Collaborator

‹ Previous Next ›

Who can push code?

Direct: users with write access

- https
- ssh

Deploy keys
Machine users
GitHub Apps
GITHUB_TOKEN

Indirect (public repo):

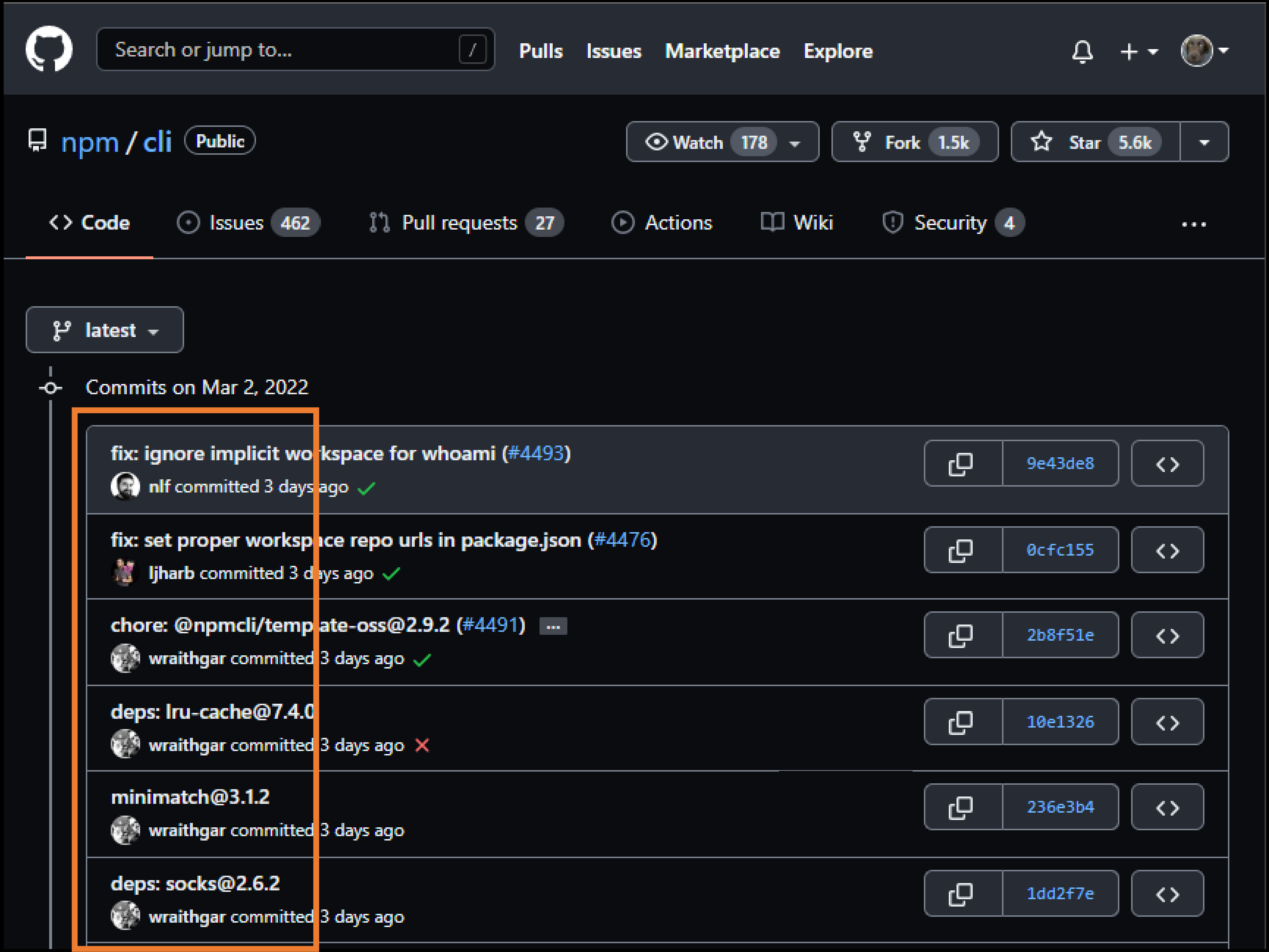
– anyone can send in a Pull Request

How do you push code?

```
$ git config --global user.name “Some name”
$ git config --global user.email some-name@example.com
```

GitHub uses **this** info to match the user!

Not the authentication method!



Commits on Mar 2, 2022

fix: ignore implicit workspace for whoami (#4493)
nlf committed 3 days ago ✓
9e43de8

fix: set proper workspace repo urls in package.json (#4476)
ljharb committed 3 days ago ✓
0cfc155

chore: @npmcli/template-oss@2.9.2 (#4491) …
wraithgar committed 3 days ago ✓
2b8f51e

deps: lru-cache@7.4.0
wraithgar committed 3 days ago ✗
10e1326

minimatch@3.1.2
wraithgar committed 3 days ago
236e3b4

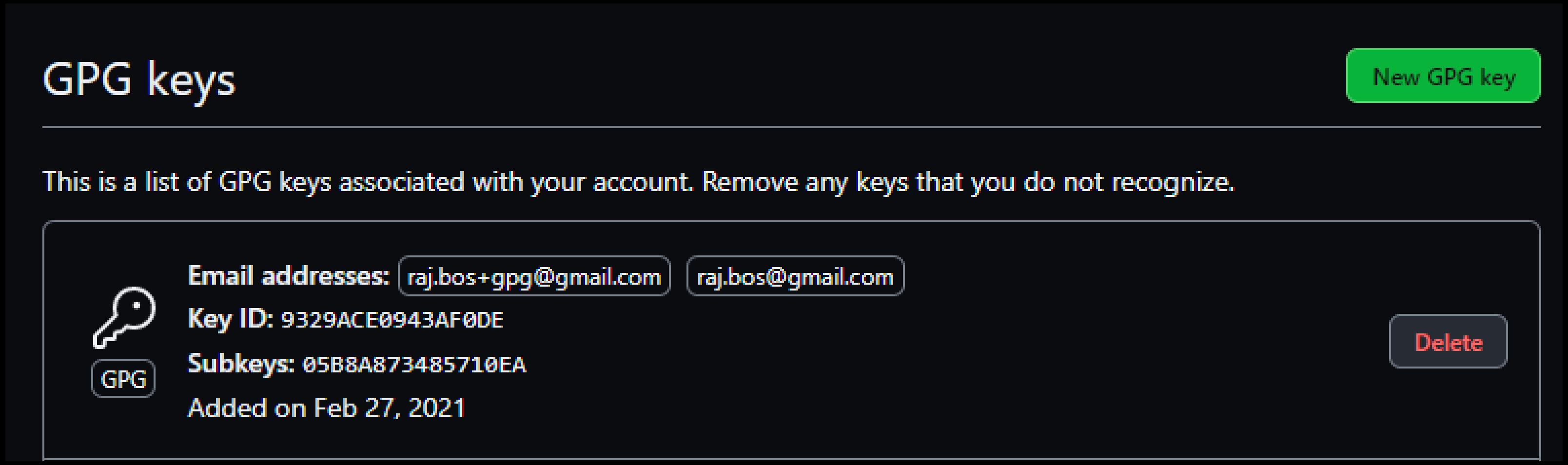
deps: socks@2.6.2
wraithgar committed 3 days ago
1dd2f7e

What’s so bad?

- I can automate your commits!
- Default setup (Linux/Windows/https/ssh):

```
git add .
git commit –m ‘doing the commit for you’
git push
```

Commit signing



GPG keys

This is a list of GPG keys associated with your account. Remove any keys that you do not recognize.

Email addresses: raj.bos+gpg@gmail.com raj.bos@gmail.com
Key ID: 9329ACE0943AF0DE
Subkeys: 05B8A873485710EA
Added on Feb 27, 2021

You have your private key to sign with

→

GitHub has public key to verify the commit with

https://xpir.it/commit-signing

Commit signing

- GPG keys (most common)
- S/MIME
- SSH keys (since September 2022)

Always configure commit signing

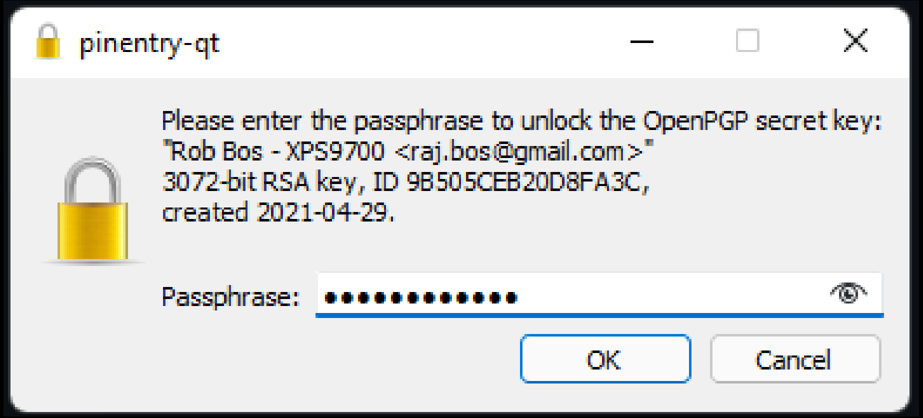
```
git commit -S -m "your commit message“
```

```
git config commit.gpgsign true
```

Demo / example

Demo – Commit signing

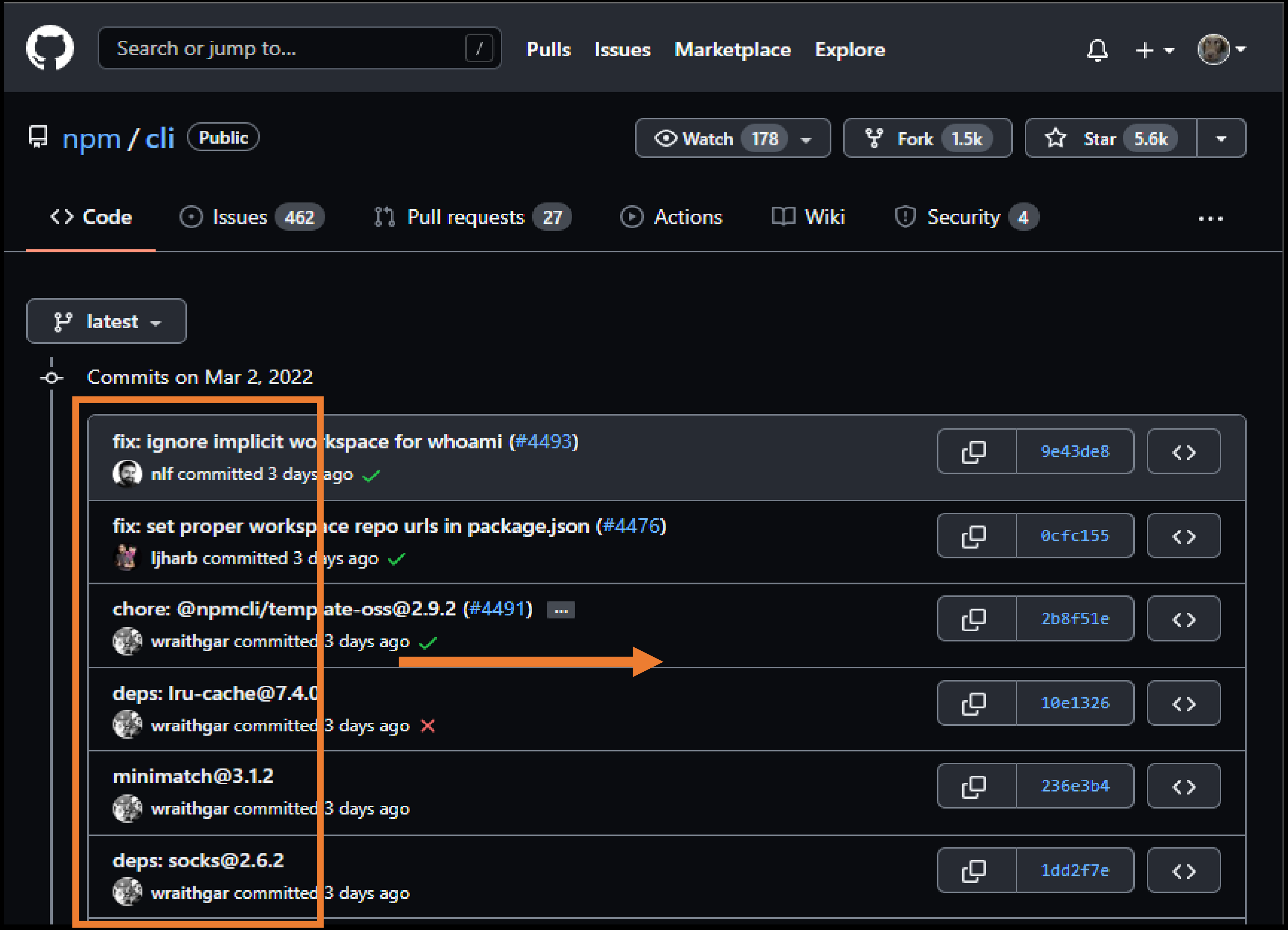
git commit –m ‘my commit’



Please enter the passphrase to unlock the OpenPGP secret key:
"Rob Bos - XPS9700 <raj.bos@gmail.com>"
3072-bit RSA key, ID 9B505CEB20D8FA3C,
created 2021-04-29.

Passphrase: ●●●●●●●●●●●●●

Commit signing



Commits on Mar 2, 2022

fix: ignore implicit workspace for whoami (#4493)
nlf committed 3 days ago ✓
9e43de8

fix: set proper workspace repo urls in package.json (#4476)
ljharb committed 3 days ago ✓
0cfc155

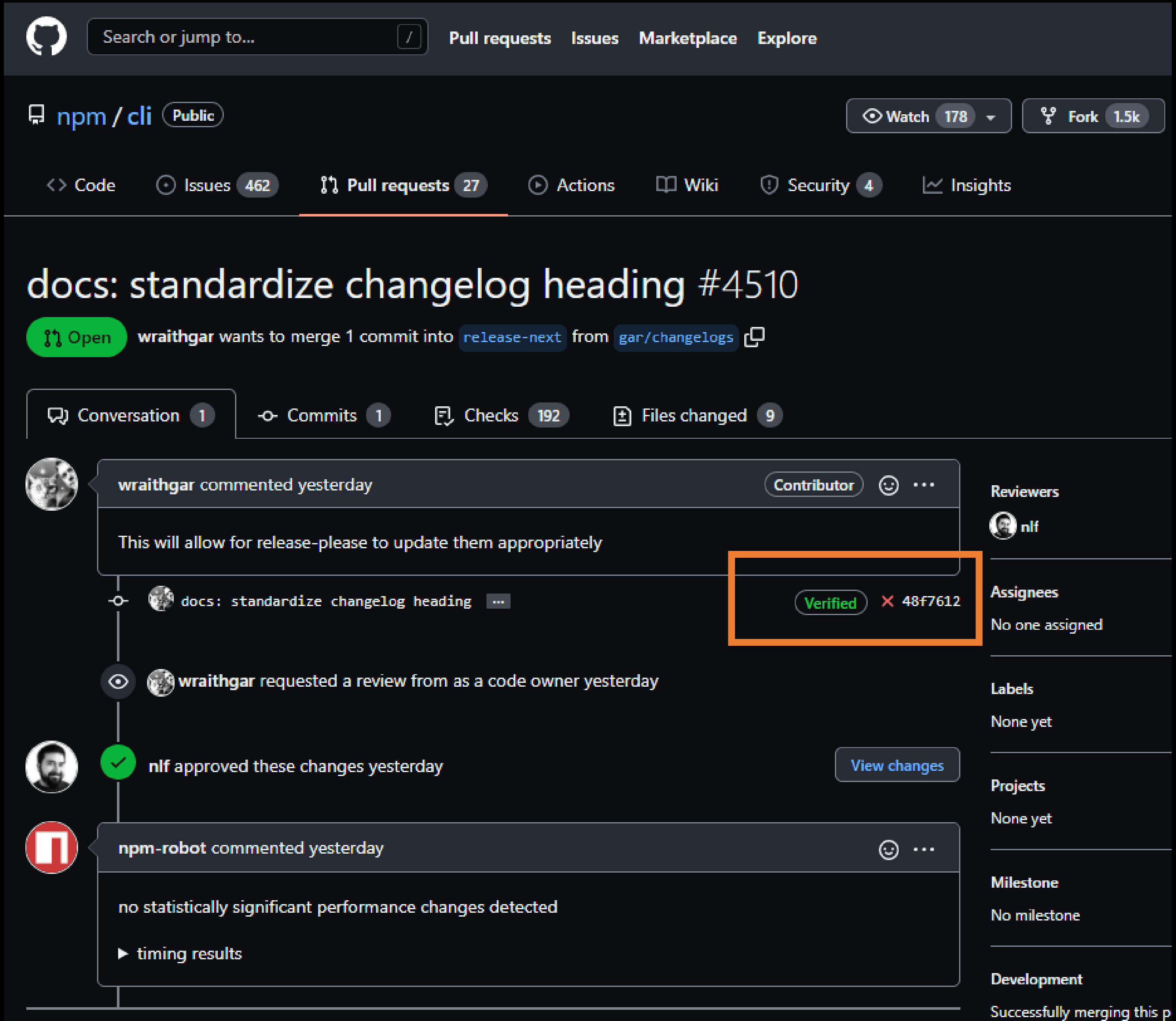
chore: @npmcli/template-oss@2.9.2 (#4491) …
wraithgar committed 3 days ago ✓
2b8f51e

deps: lru-cache@7.4.0
wraithgar committed 3 days ago ✗
10e1326

minimatch@3.1.2
wraithgar committed 3 days ago
236e3b4

deps: socks@2.6.2
wraithgar committed 3 days ago
1dd2f7e

Commit signing



npm / cli Public

docs: standardize changelog heading #4510

Open wraithgar wants to merge 1 commit into `release-next` from `gar/changelogs`

wraithgar commented yesterday

This will allow for release-please to update them appropriately

`docs: standardize changelog heading` … Verified ✕ 48f7612

wraithgar requested a review from as a code owner yesterday

nlf approved these changes yesterday

npm-robot commented yesterday

no statistically significant performance changes detected

▶ timing results

Reviewers: nlf

Assignees: No one assigned

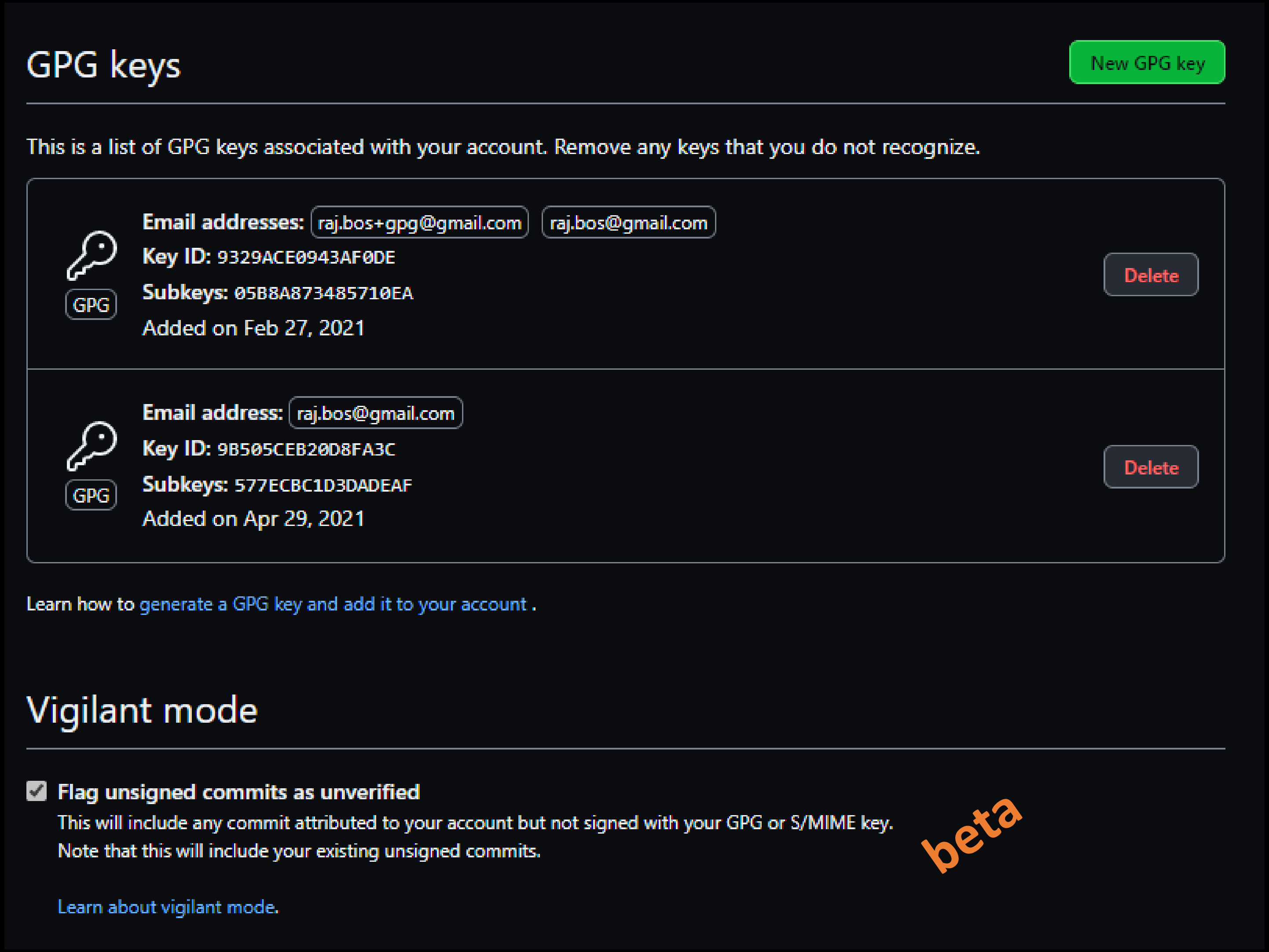
Labels: None yet

Projects: None yet

Milestone: No milestone

Development: Successfully merging this p

Vigilant mode



GPG keys

This is a list of GPG keys associated with your account. Remove any keys that you do not recognize.

Email addresses: raj.bos+gpg@gmail.com raj.bos@gmail.com
Key ID: 9329ACE0943AF0DE
Subkeys: 05B8A873485710EA
Added on Feb 27, 2021

Email address: raj.bos@gmail.com
Key ID: 9B505CEB20D8FA3C
Subkeys: 577ECBC1D3DADEAF
Added on Apr 29, 2021

Learn how to generate a GPG key and add it to your account .

Vigilant mode

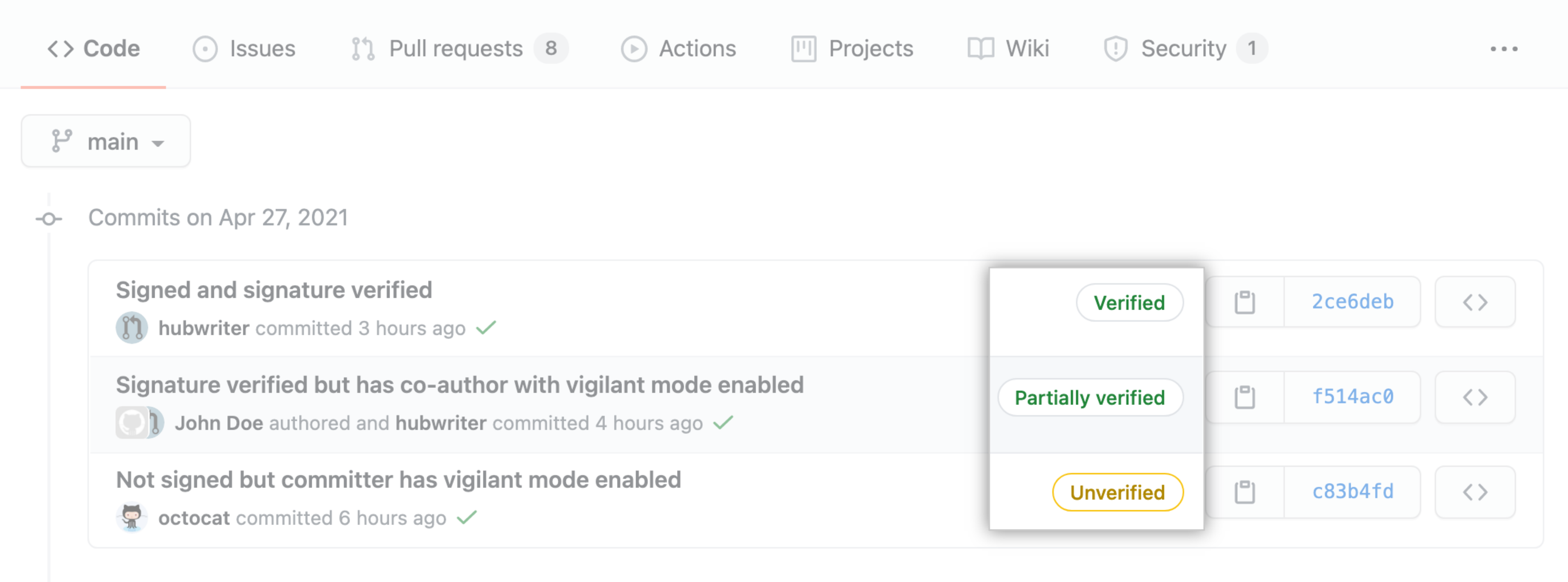
☑ **Flag unsigned commits as unverified**
This will include any commit attributed to your account but not signed with your GPG or S/MIME key.
Note that this will include your existing unsigned commits.

Learn about vigilant mode.

beta

@robbos81 https://xpir.it/vigilant-mode

Vigilant mode



Commits on Apr 27, 2021

Signed and signature verified
hubwriter committed 3 hours ago ✓
Verified
2ce6deb

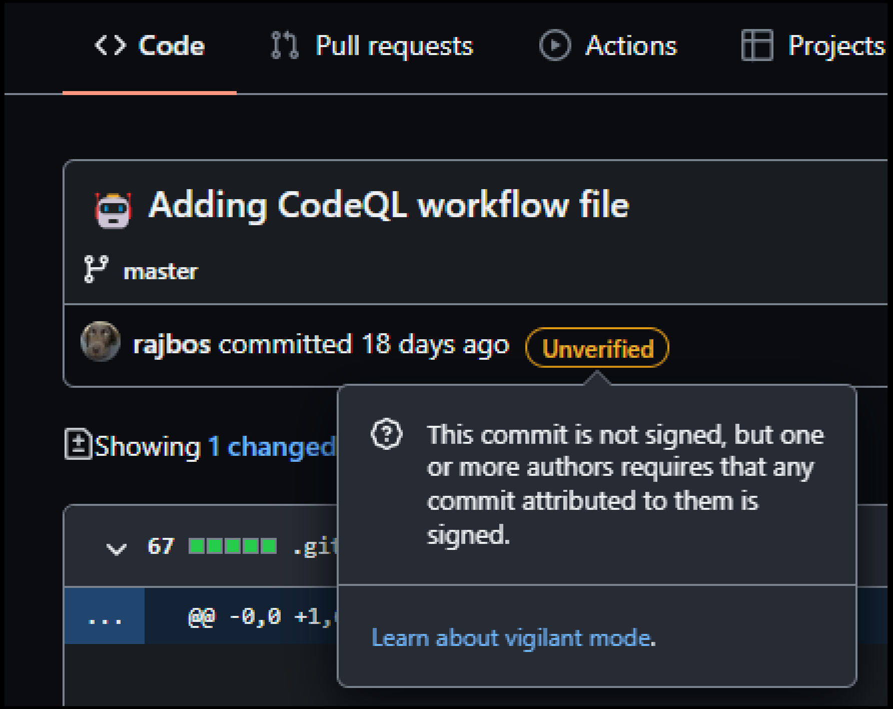
Signature verified but has co-author with vigilant mode enabled
John Doe authored and hubwriter committed 4 hours ago ✓
Partially verified
f514ac0

Not signed but committer has vigilant mode enabled
octocat committed 6 hours ago ✓
Unverified
c83b4fd

Vigilant mode

Status	Commit signed?	Signature verified?	Commit matches author?
Verified	☑	☑	☑
Partially verified	☑	☑	✗
Unverified	☑	✗	
	✗		

Vigilant mode



Adding CodeQL workflow file

master

rajbos committed 18 days ago Unverified

Showing 1 changed

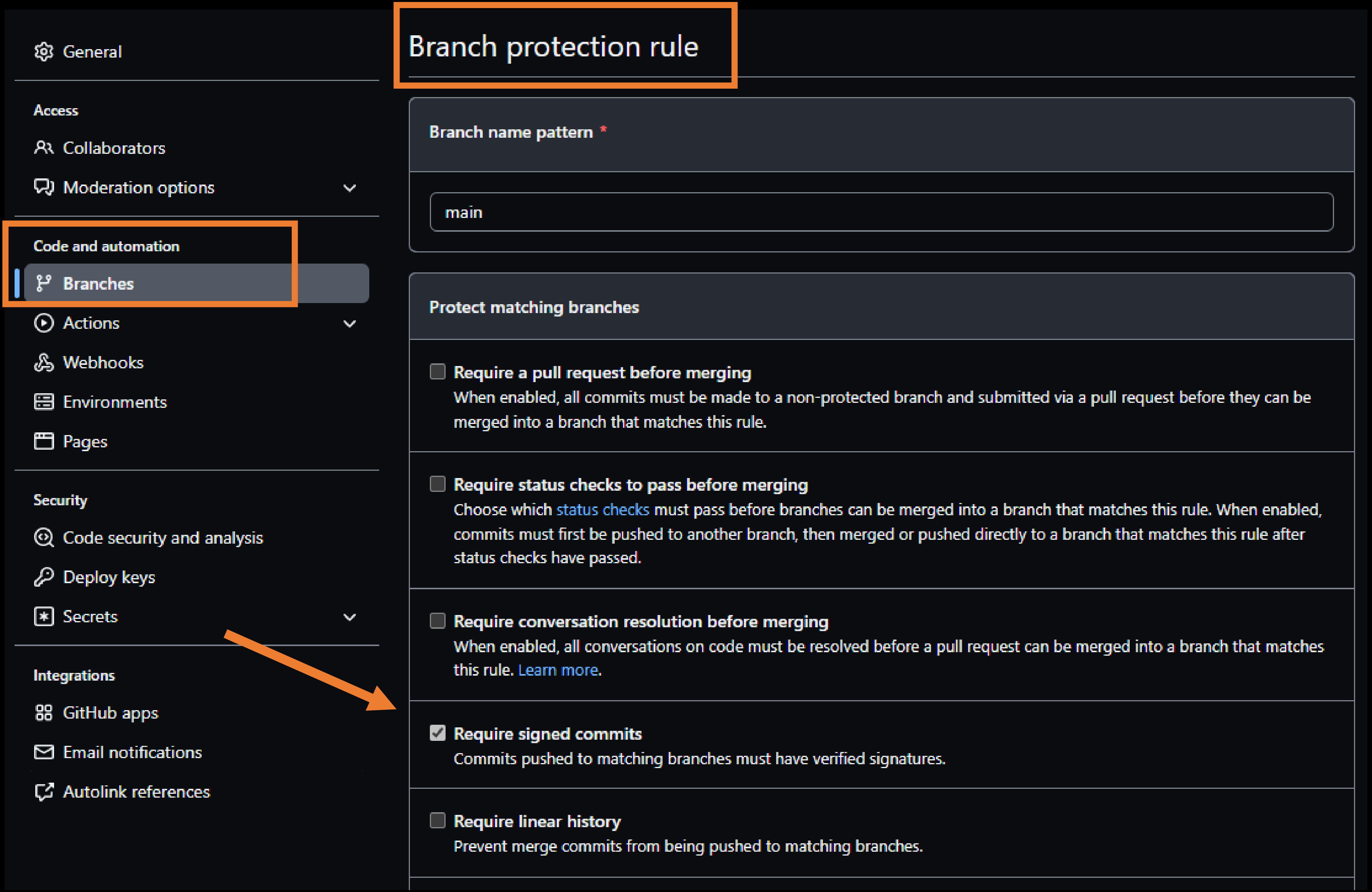
67 .gi

@@ -0,0 +1,

This commit is not signed, but one or more authors requires that any commit attributed to them is signed.

Learn about vigilant mode.

Next step:



Branch protection rule

Branch name pattern *

main

Protect matching branches

□ **Require a pull request before merging**
When enabled, all commits must be made to a non-protected branch and submitted via a pull request before they can be merged into a branch that matches this rule.

□ **Require status checks to pass before merging**
Choose which status checks must pass before branches can be merged into a branch that matches this rule. When enabled, commits must first be pushed to another branch, then merged or pushed directly to a branch that matches this rule after status checks have passed.

□ **Require conversation resolution before merging**
When enabled, all conversations on code must be resolved before a pull request can be merged into a branch that matches this rule. Learn more.

☑ **Require signed commits**
Commits pushed to matching branches must have verified signatures.

□ **Require linear history**
Prevent merge commits from being pushed to matching branches.

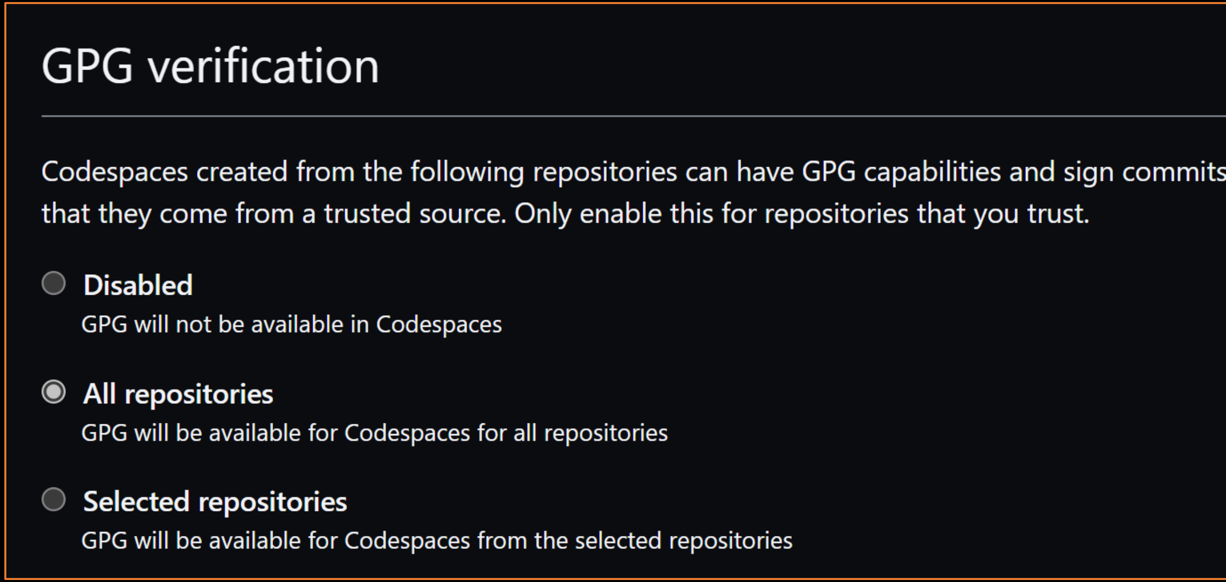
Require signed commits – impact

Users' setup: needs to install/configure tools

Automation:

- Dependabot – will sign automatically
- GitHub Apps
- Personal Access Tokens

Codespaces



GPG verification

Codespaces created from the following repositories can have GPG capabilities and sign commits
that they come from a trusted source. Only enable this for repositories that you trust.

○ **Disabled**
GPG will not be available in Codespaces

● **All repositories**
GPG will be available for Codespaces for all repositories

○ **Selected repositories**
GPG will be available for Codespaces from the selected repositories

Security features

Commit signing

Dependabot

Security alerts on dependencies

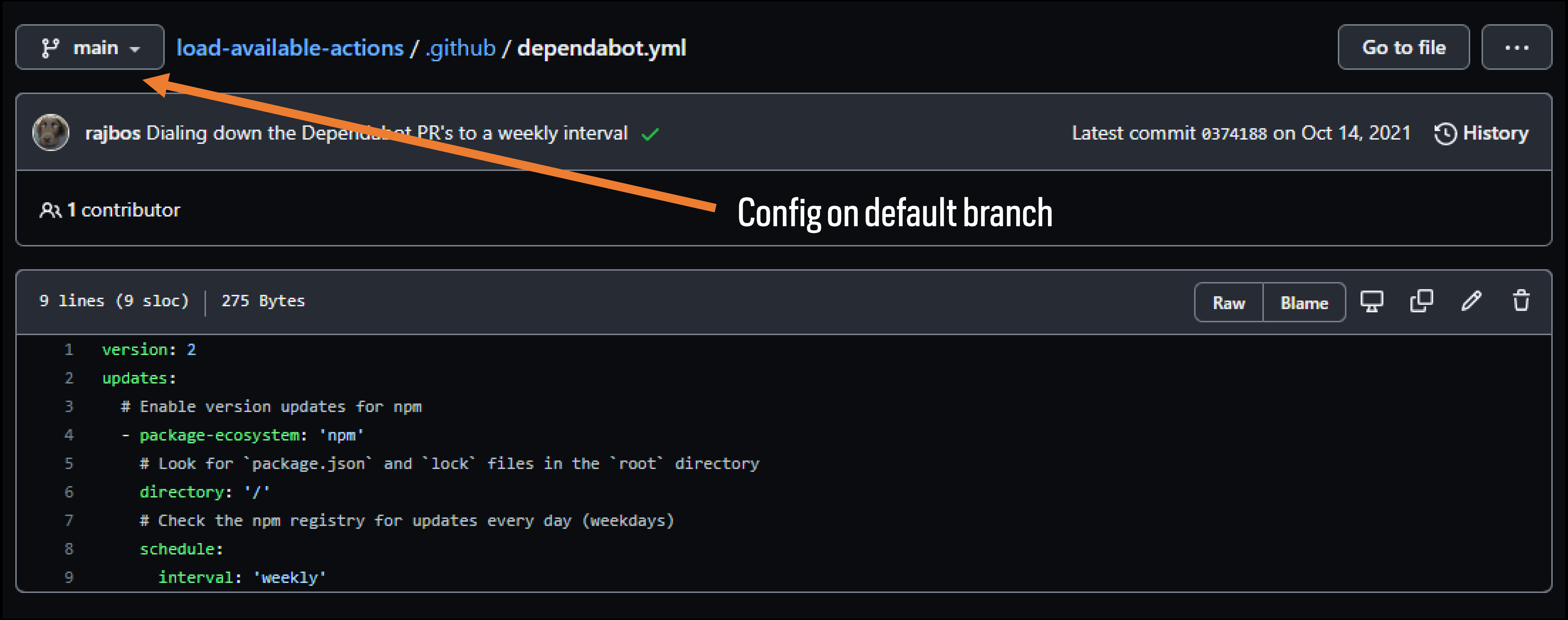
Secret scanning

CodeQL

Stay up to date

- Dependabot + updates
  - Why
  - What to do
  - How
- Free for public repos

Dependabot config



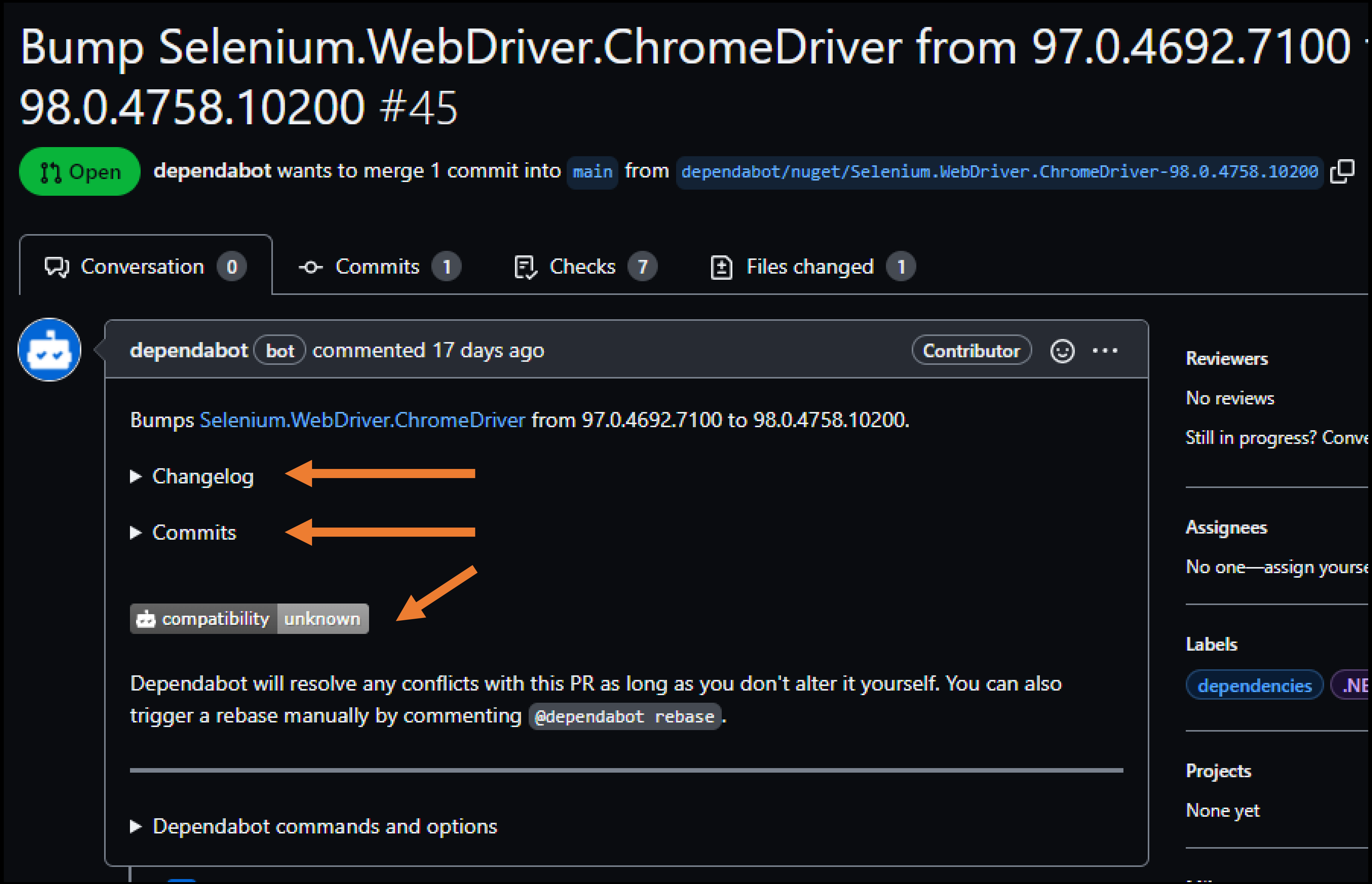
main
load-available-actions / .github / dependabot.yml
Go to file
rajbos Dialing down the Depend...ot PR's to a weekly interval ✓
Latest commit 0374188 on Oct 14, 2021
History
1 contributor
9 lines (9 sloc) | 275 Bytes
Raw
Blame

```yaml
version: 2
updates:
  # Enable version updates for npm
  - package-ecosystem: 'npm'
    # Look for `package.json` and `lock` files in the `root` directory
    directory: '/'
    # Check the npm registry for updates every day (weekdays)
    schedule:
      interval: 'weekly'
```

Config on default branch

Dependabot demo

https://github.com/devops-actions/load-runner-info/pull/98



Bump Selenium.WebDriver.ChromeDriver from 97.0.4692.7100 98.0.4758.10200 #45

Open **dependabot** wants to merge 1 commit into `main` from `dependabot/nuget/Selenium.WebDriver.ChromeDriver-98.0.4758.10200`

dependabot bot commented 17 days ago

Bumps Selenium.WebDriver.ChromeDriver from 97.0.4692.7100 to 98.0.4758.10200.

▶ Changelog

▶ Commits

compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

▶ Dependabot commands and options

Reviewers

No reviews

Still in progress? Conve

Assignees

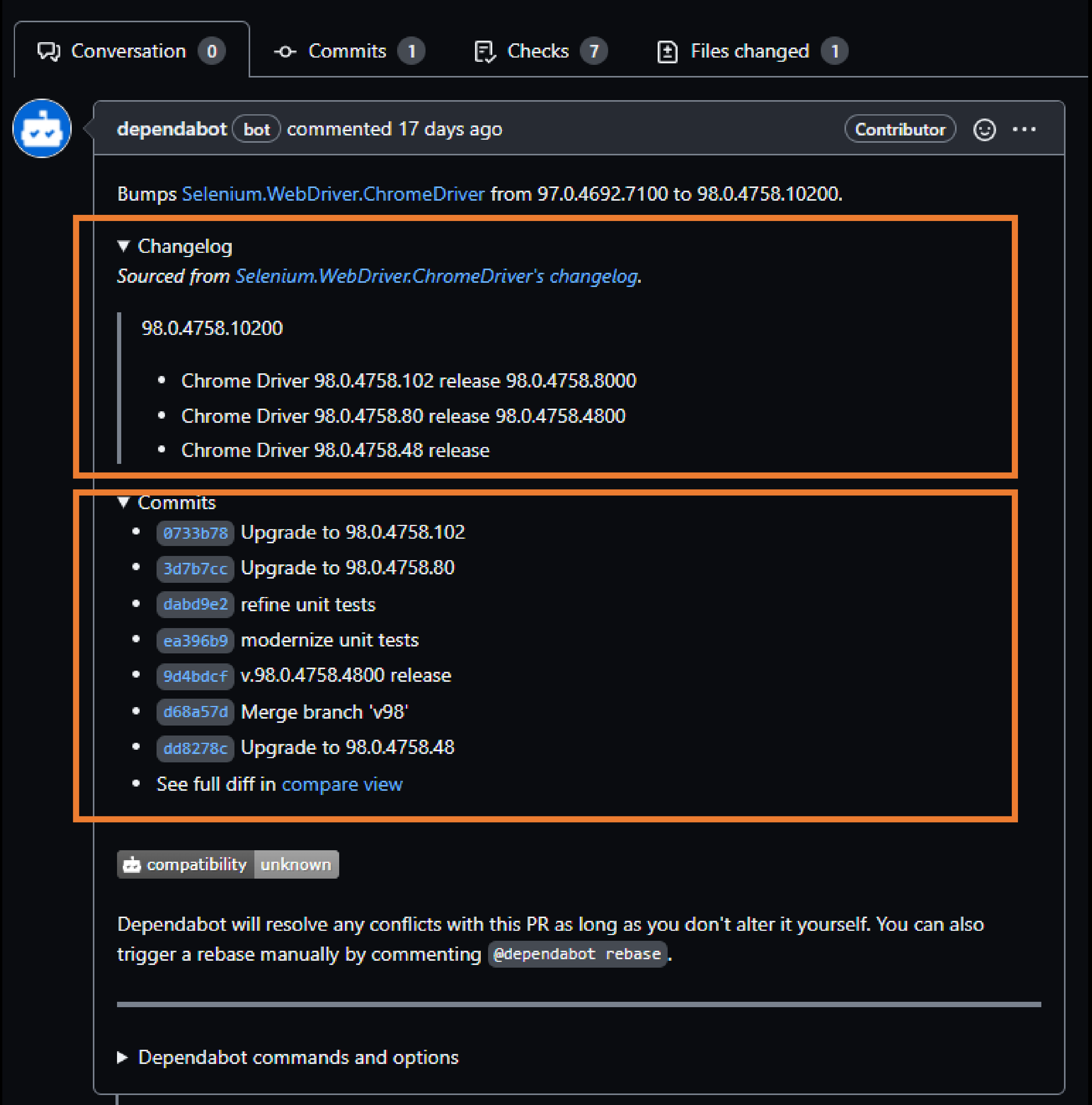
No one—assign yourse

Labels

dependencies .NE

Projects

None yet



dependabot bot commented 17 days ago

Bumps Selenium.WebDriver.ChromeDriver from 97.0.4692.7100 to 98.0.4758.10200.

▼ Changelog

Sourced from Selenium.WebDriver.ChromeDriver's changelog.

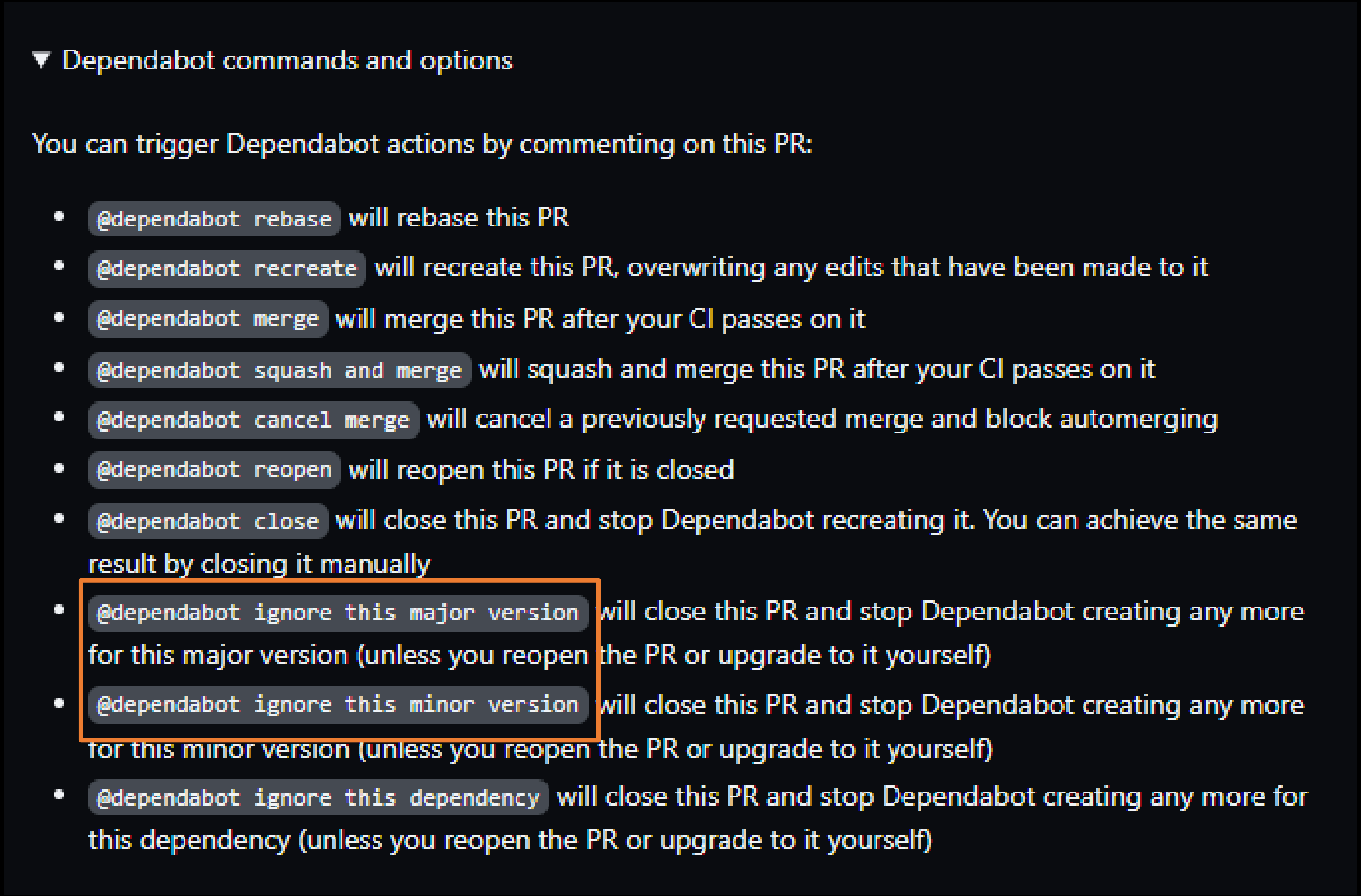
> 98.0.4758.10200
>
> - Chrome Driver 98.0.4758.102 release 98.0.4758.8000
> - Chrome Driver 98.0.4758.80 release 98.0.4758.4800
> - Chrome Driver 98.0.4758.48 release

▼ Commits

- `0733b78` Upgrade to 98.0.4758.102
- `3d7b7cc` Upgrade to 98.0.4758.80
- `dabd9e2` refine unit tests
- `ea396b9` modernize unit tests
- `9d4bdcf` v.98.0.4758.4800 release
- `d68a57d` Merge branch 'v98'
- `dd8278c` Upgrade to 98.0.4758.48
- See full diff in compare view

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

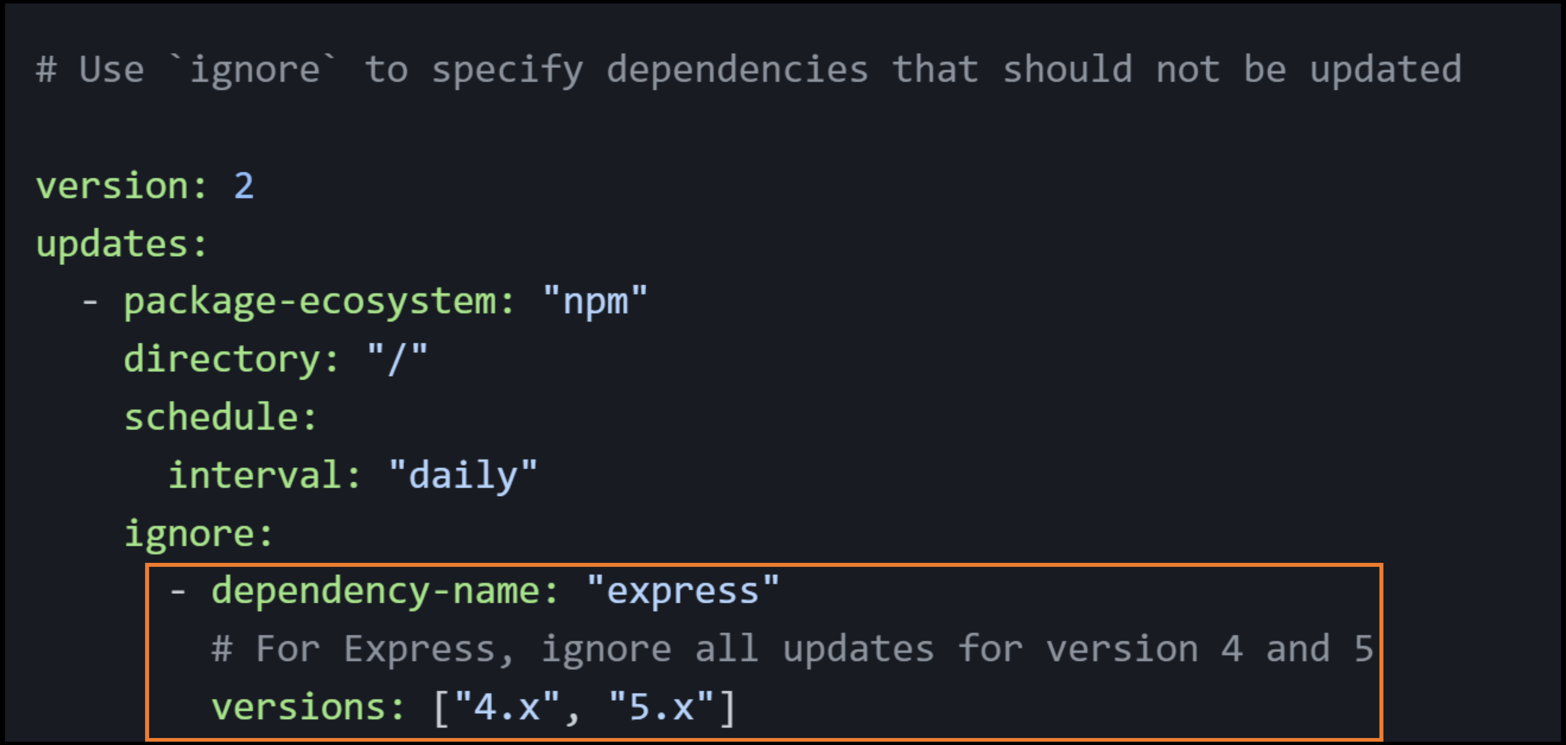
▶ Dependabot commands and options



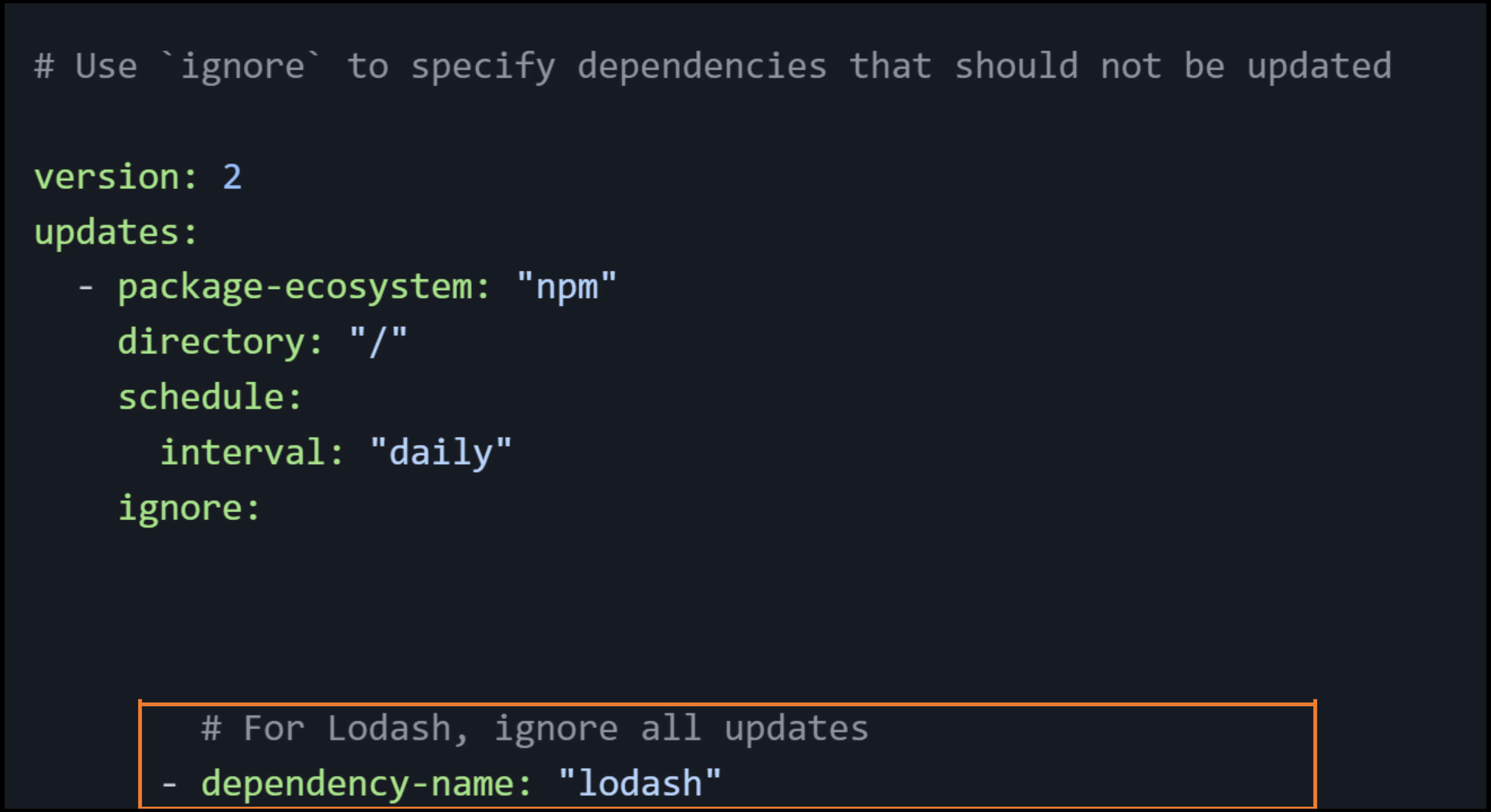
▼ Dependabot commands and options

You can trigger Dependabot actions by commenting on this PR:

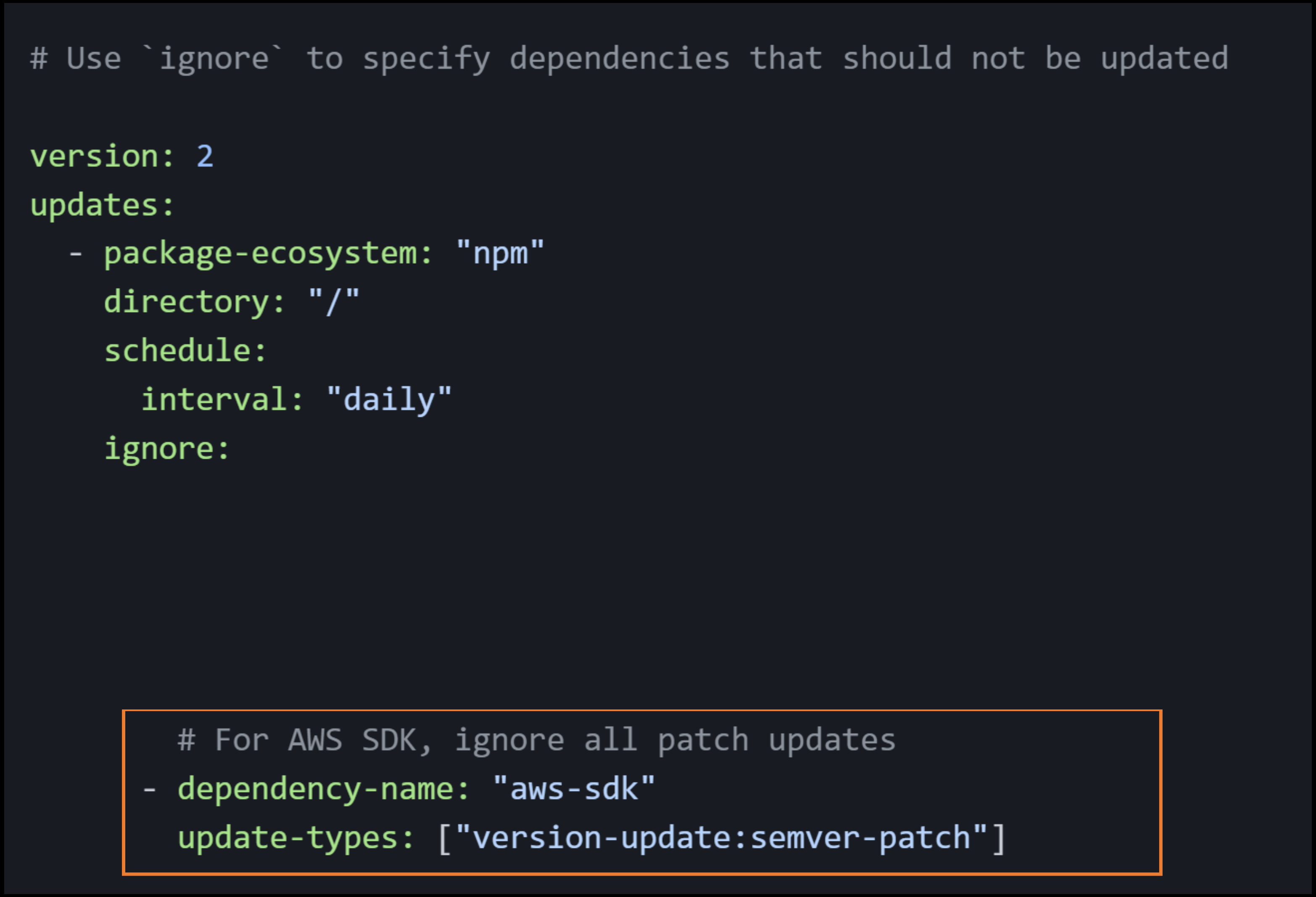
- `@dependabot rebase` will rebase this PR
- `@dependabot recreate` will recreate this PR, overwriting any edits that have been made to it
- `@dependabot merge` will merge this PR after your CI passes on it
- `@dependabot squash and merge` will squash and merge this PR after your CI passes on it
- `@dependabot cancel merge` will cancel a previously requested merge and block automerging
- `@dependabot reopen` will reopen this PR if it is closed
- `@dependabot close` will close this PR and stop Dependabot recreating it. You can achieve the same result by closing it manually
- `@dependabot ignore this major version` will close this PR and stop Dependabot creating any more for this major version (unless you reopen the PR or upgrade to it yourself)
- `@dependabot ignore this minor version` will close this PR and stop Dependabot creating any more for this minor version (unless you reopen the PR or upgrade to it yourself)
- `@dependabot ignore this dependency` will close this PR and stop Dependabot creating any more for this dependency (unless you reopen the PR or upgrade to it yourself)



```yaml
# Use `ignore` to specify dependencies that should not be updated

version: 2
updates:
  - package-ecosystem: "npm"
    directory: "/"
    schedule:
      interval: "daily"
    ignore:
      - dependency-name: "express"
        # For Express, ignore all updates for version 4 and 5
        versions: ["4.x", "5.x"]
```



```yaml
# Use `ignore` to specify dependencies that should not be updated

version: 2
updates:
  - package-ecosystem: "npm"
    directory: "/"
    schedule:
      interval: "daily"
    ignore:



        # For Lodash, ignore all updates
      - dependency-name: "lodash"
```



```yaml
# Use `ignore` to specify dependencies that should not be updated

version: 2
updates:
  - package-ecosystem: "npm"
    directory: "/"
    schedule:
      interval: "daily"
    ignore:




        # For AWS SDK, ignore all patch updates
      - dependency-name: "aws-sdk"
        update-types: ["version-update:semver-patch"]
```

Security features

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

CodeQL

Security alerts on dependencies

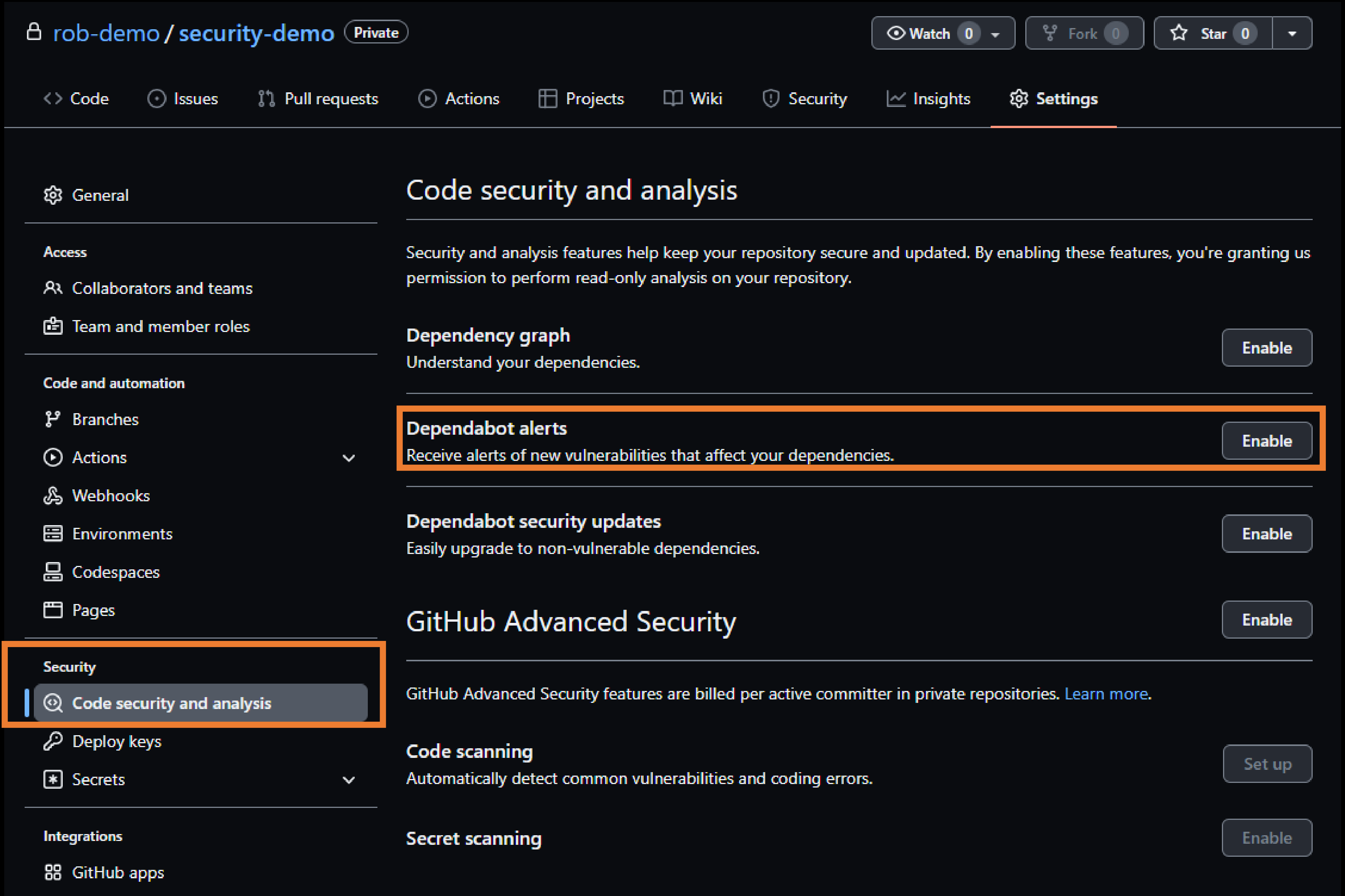
Security updates from Dependabot

    Free for public repos

Dependabot knows your dependency graph

Dependency has vulnerability? Alert!

Alerts on dependencies



rob-demo / security-demo Private

Code security and analysis

Security and analysis features help keep your repository secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your repository.

Dependency graph
Understand your dependencies. Enable

Dependabot alerts
Receive alerts of new vulnerabilities that affect your dependencies. Enable

Dependabot security updates
Easily upgrade to non-vulnerable dependencies. Enable

GitHub Advanced Security

Enable

GitHub Advanced Security features are billed per active committer in private repositories. Learn more.

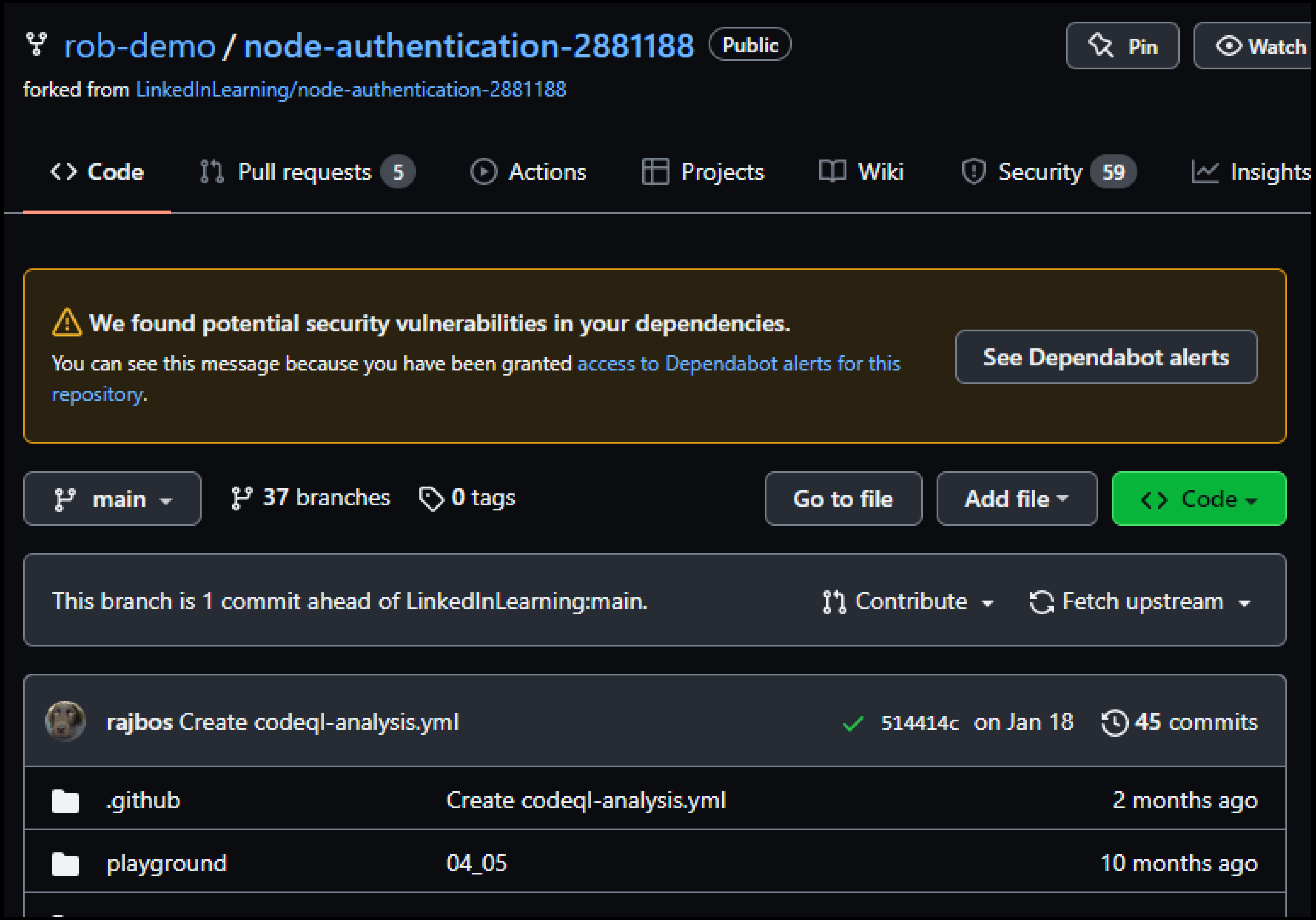
Code scanning
Automatically detect common vulnerabilities and coding errors. Set up

Secret scanning
Enable

Demo

https://github.com/rob-demo/node-authentication-2881188

DEMO: Security alerts on dependencies



rob-demo / node-authentication-2881188 Public

forked from LinkedInLearning/node-authentication-2881188

⚠ We found potential security vulnerabilities in your dependencies.

You can see this message because you have been granted access to Dependabot alerts for this repository.

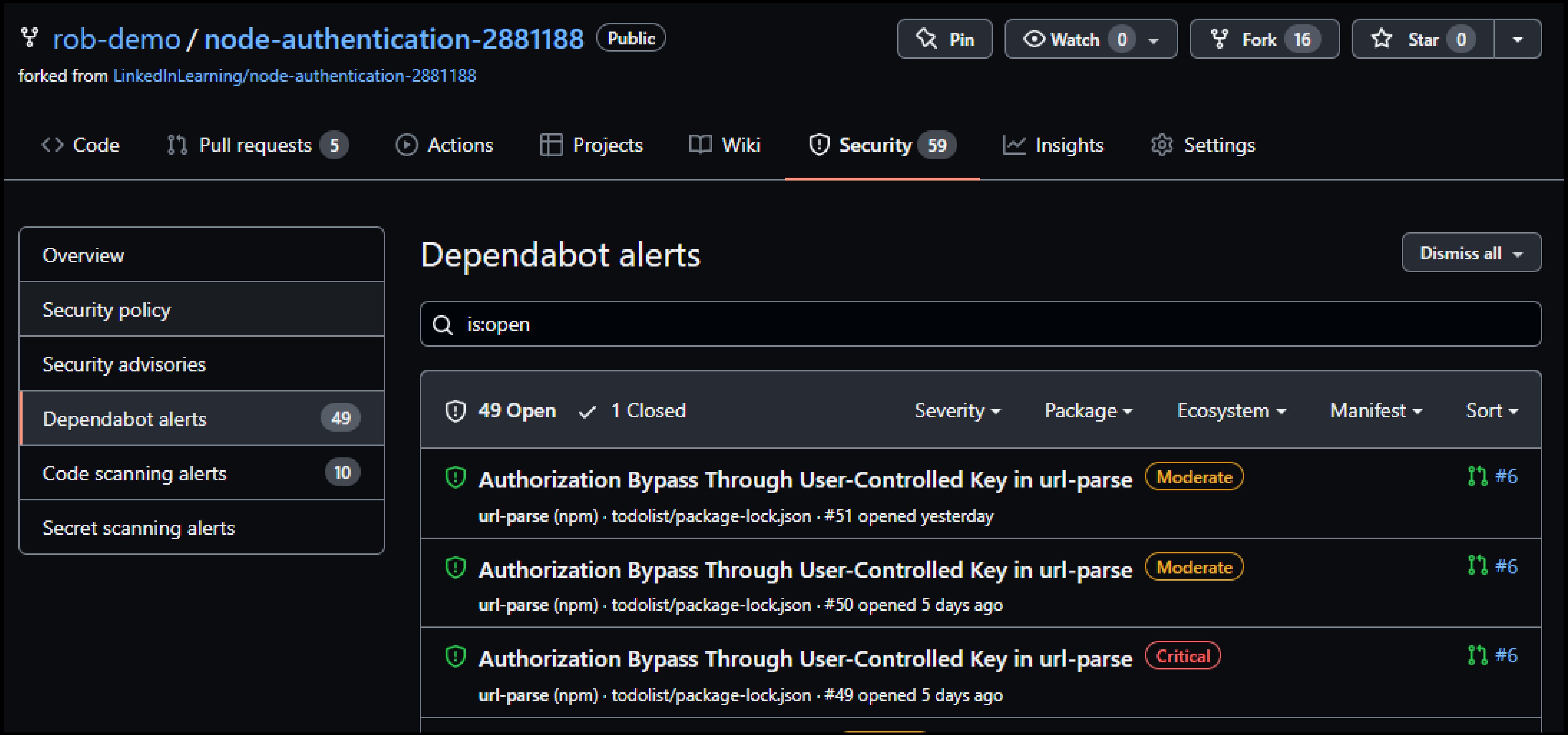
main · 37 branches · 0 tags

This branch is 1 commit ahead of LinkedInLearning:main.

rajbos Create codeql-analysis.yml ✓ 514414c on Jan 18 · 45 commits

.github	Create codeql-analysis.yml	2 months ago
playground	04_05	10 months ago

DEMO: Security alerts on dependencies



rob-demo / node-authentication-2881188 Public

forked from LinkedInLearning/node-authentication-2881188

Dependabot alerts

is:open

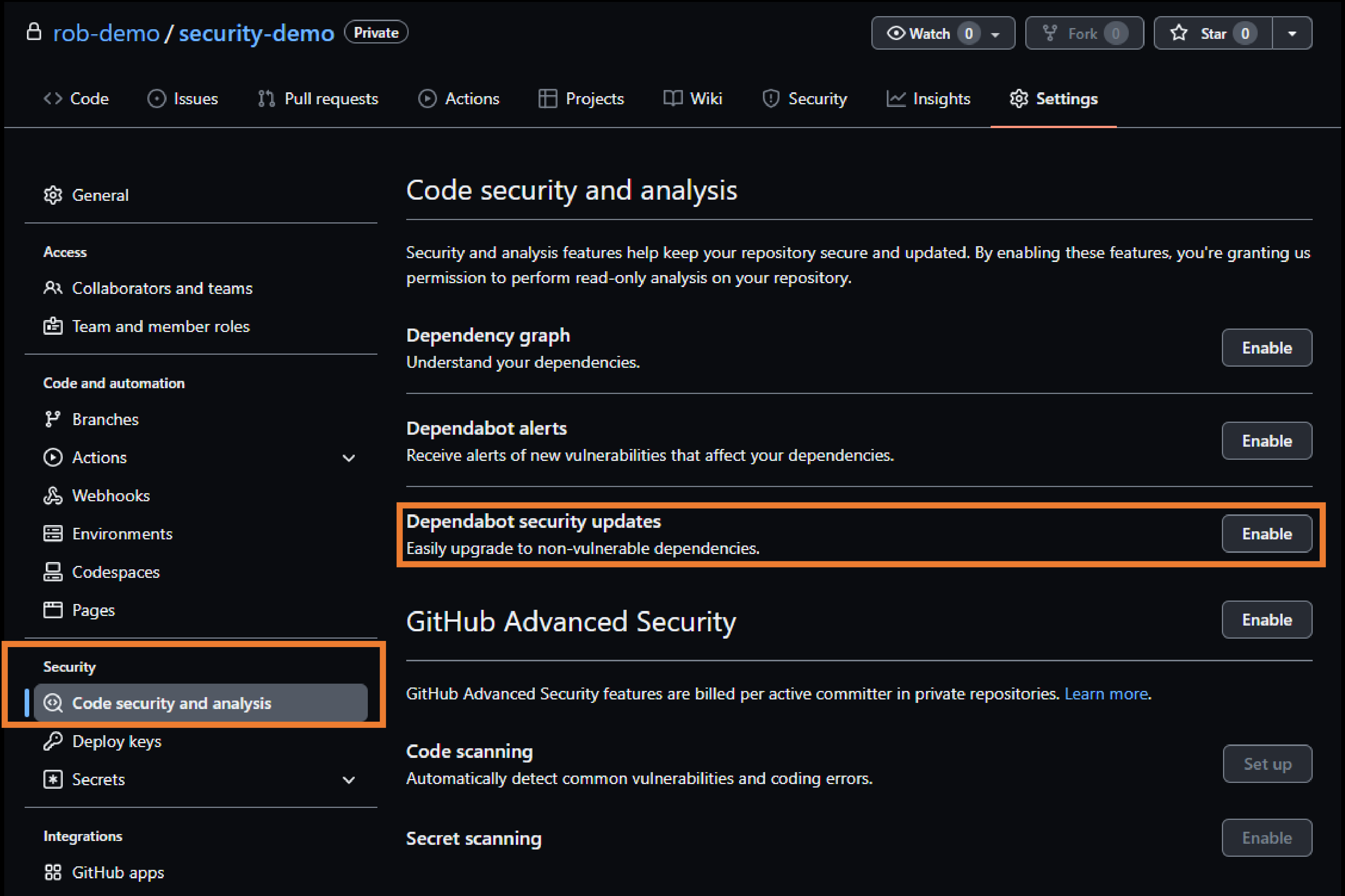
49 Open ✓ 1 Closed

Authorization Bypass Through User-Controlled Key in url-parse Moderate #6
url-parse (npm) · todolist/package-lock.json · #51 opened yesterday

Authorization Bypass Through User-Controlled Key in url-parse Moderate #6
url-parse (npm) · todolist/package-lock.json · #50 opened 5 days ago

Authorization Bypass Through User-Controlled Key in url-parse Critical #6
url-parse (npm) · todolist/package-lock.json · #49 opened 5 days ago

DEMO: Security alerts on dependencies



Code security and analysis

Security and analysis features help keep your repository secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your repository.

Dependency graph
Understand your dependencies. Enable

Dependabot alerts
Receive alerts of new vulnerabilities that affect your dependencies. Enable

Dependabot security updates
Easily upgrade to non-vulnerable dependencies. Enable

GitHub Advanced Security

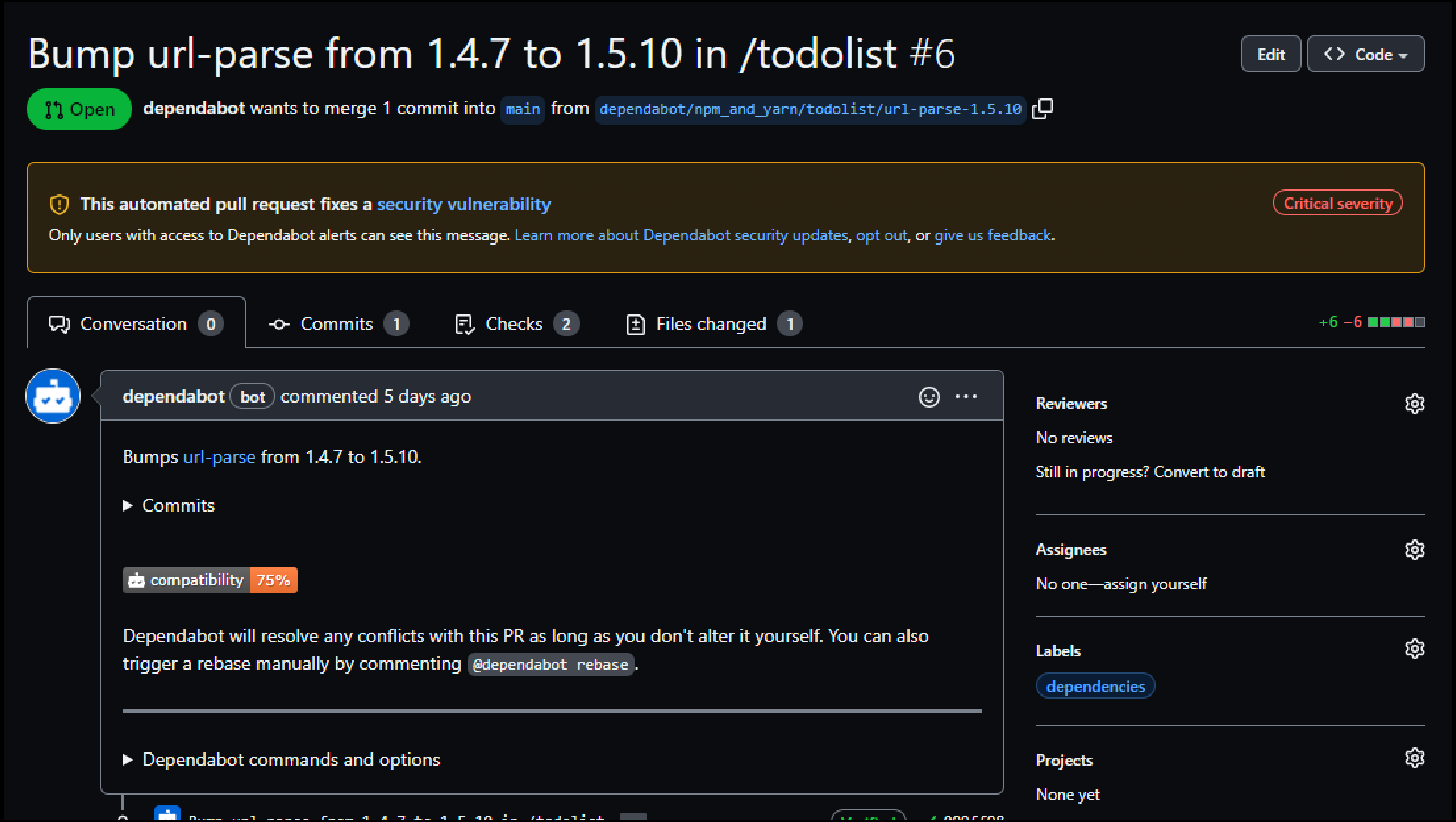
Enable

GitHub Advanced Security features are billed per active committer in private repositories. Learn more.

Code scanning
Automatically detect common vulnerabilities and coding errors. Set up

Secret scanning
Enable

DEMO: Security alerts on dependencies



Bump url-parse from 1.4.7 to 1.5.10 in /todolist #6

Open **dependabot** wants to merge 1 commit into `main` from `dependabot/npm_and_yarn/todolist/url-parse-1.5.10`

This automated pull request fixes a security vulnerability

Critical severity

Only users with access to Dependabot alerts can see this message. Learn more about Dependabot security updates, opt out, or give us feedback.

dependabot bot commented 5 days ago

Bumps url-parse from 1.4.7 to 1.5.10.

▶ Commits

compatibility 75%

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

▶ Dependabot commands and options

Bump url-parse from 1.4.7 to 1.5.10 in /todolist

Reviewers

No reviews

Still in progress? Convert to draft

Assignees

No one—assign yourself

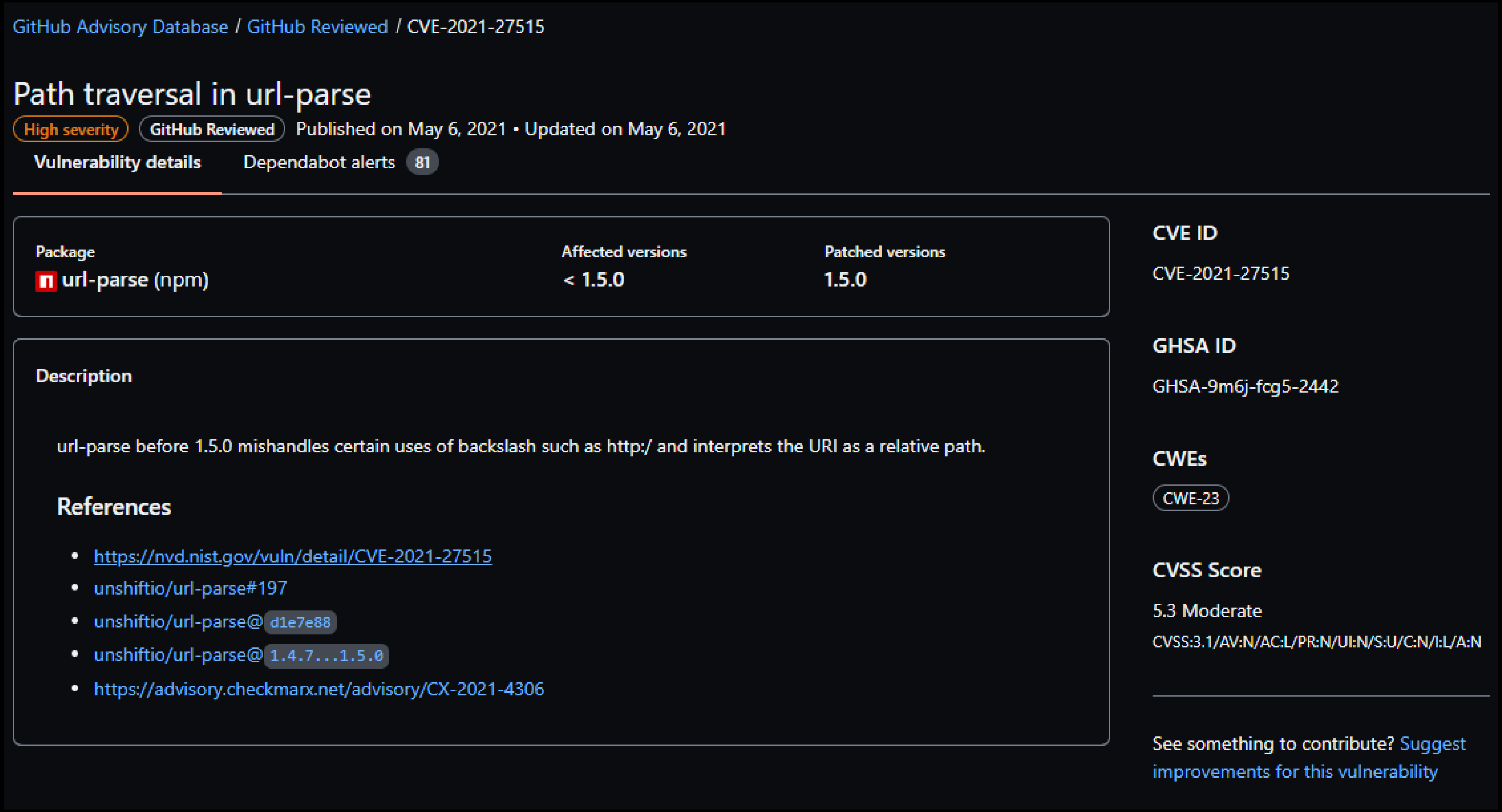
Labels

dependencies

Projects

None yet

DEMO: Security alerts on dependencies



GitHub Advisory Database / GitHub Reviewed / CVE-2021-27515

Path traversal in url-parse

High severity GitHub Reviewed Published on May 6, 2021 • Updated on May 6, 2021

Vulnerability details Dependabot alerts 81

Package	Affected versions	Patched versions
url-parse (npm)	< 1.5.0	1.5.0

Description

url-parse before 1.5.0 mishandles certain uses of backslash such as http:/ and interprets the URI as a relative path.

References

- https://nvd.nist.gov/vuln/detail/CVE-2021-27515
- unshiftio/url-parse#197
- unshiftio/url-parse@`d1e7e88`
- unshiftio/url-parse@`1.4.7...1.5.0`
- https://advisory.checkmarx.net/advisory/CX-2021-4306

CVE ID

CVE-2021-27515

GHSA ID

GHSA-9m6j-fcg5-2442

CWEs

CWE-23

CVSS Score

5.3 Moderate

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

See something to contribute? Suggest improvements for this vulnerability

Security features

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

CodeQL

Secret scanning

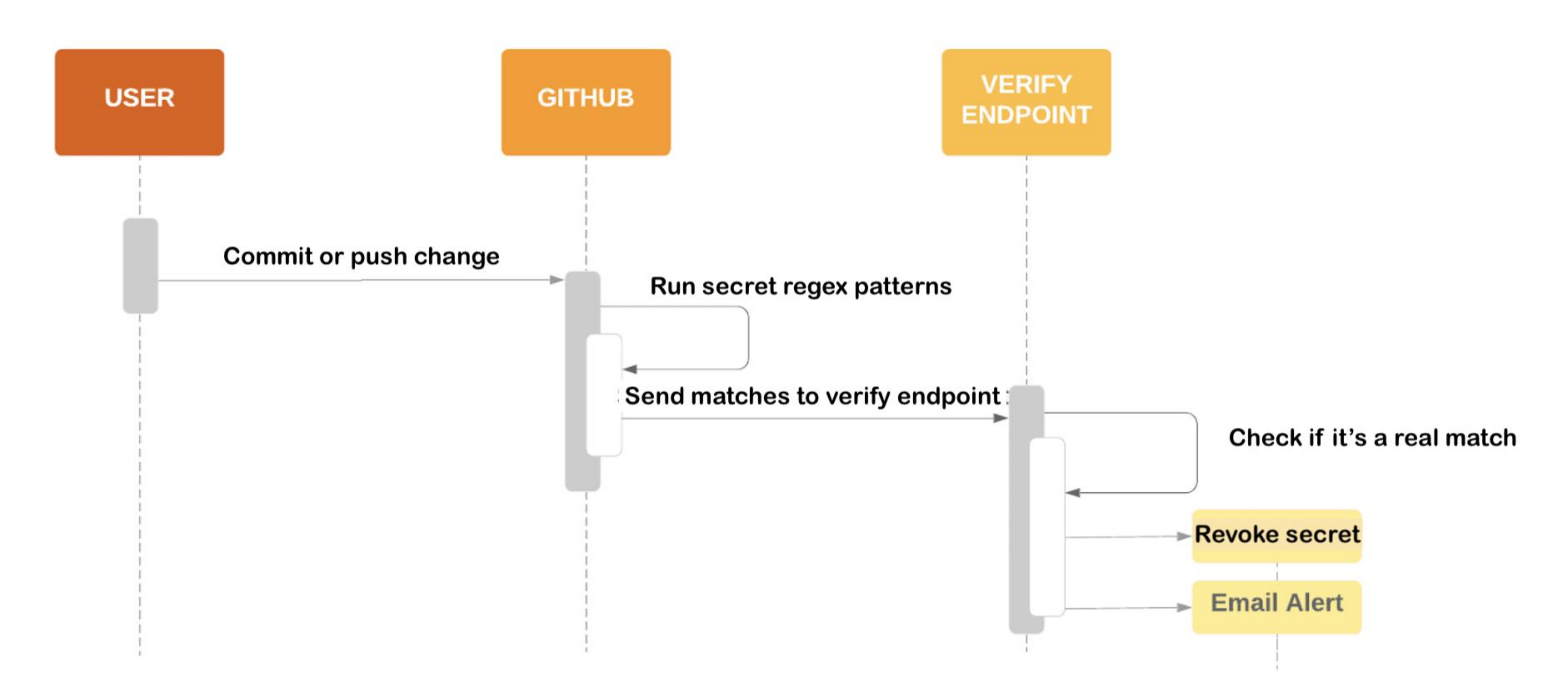
Secrets have a high risk!

Enabled by default on public repos

80+ secret scanning partners

- AWS / GCP/ Azure
- Discord
- npm
- NuGet
- Postman
- Twillio

Secret scanning


USER
GITHUB
VERIFY ENDPOINT
Commit or push change
Run secret regex patterns
Send matches to verify endpoint
Check if it's a real match
Revoke secret
Email Alert

Secret scanning

Runs after a push event (scanning issues/ PR's is on the roadmap)

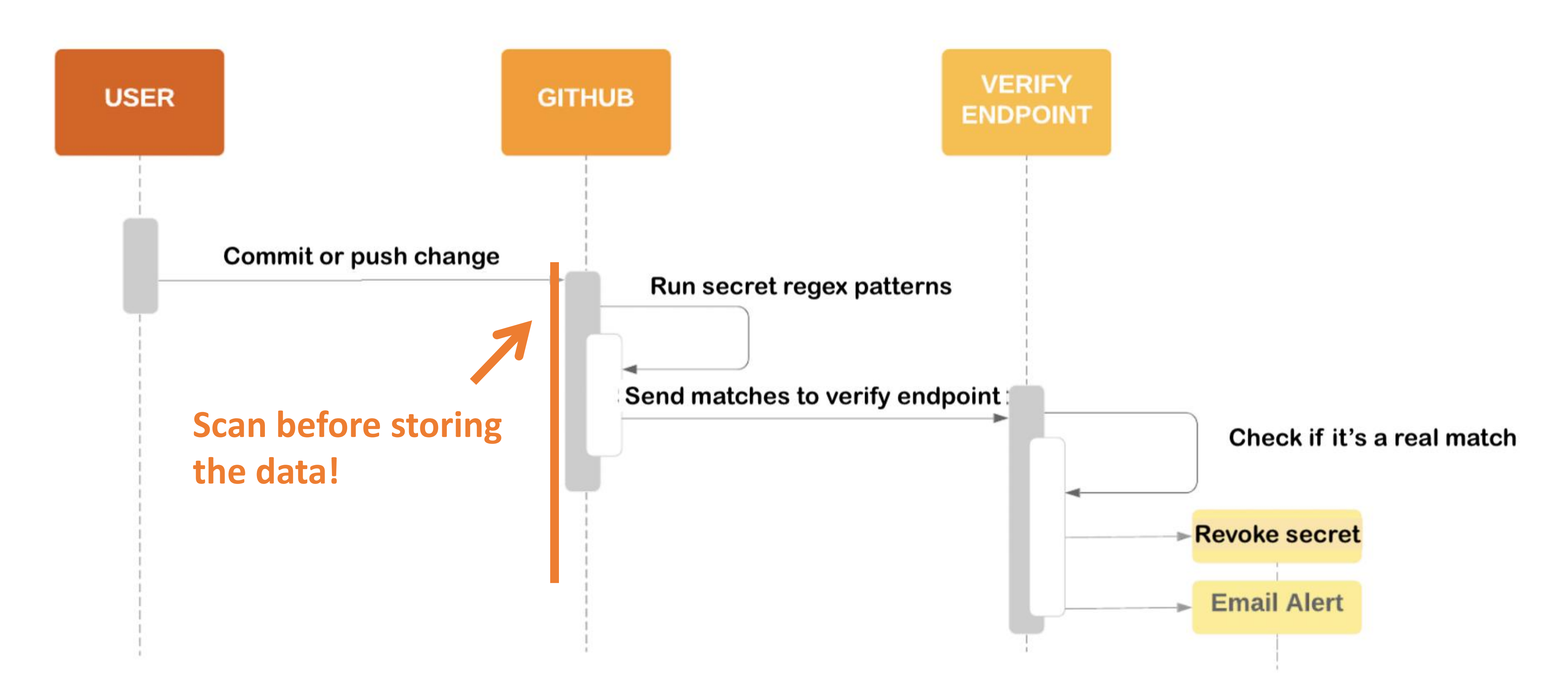
Scans the entire history of the repo as well

Public repo + actionable secret = high probability of revoking

Demo with an example repository:

- https://github.com/Microsoft-Bootcamp/attendee-rajbos

Secret scanning – push protection [PAID]



USER
GITHUB
VERIFY ENDPOINT
Commit or push change
Run secret regex patterns
Send matches to verify endpoint
Check if it's a real match
Revoke secret
Email Alert

Scan before storing the data!

Security features

Commit signing

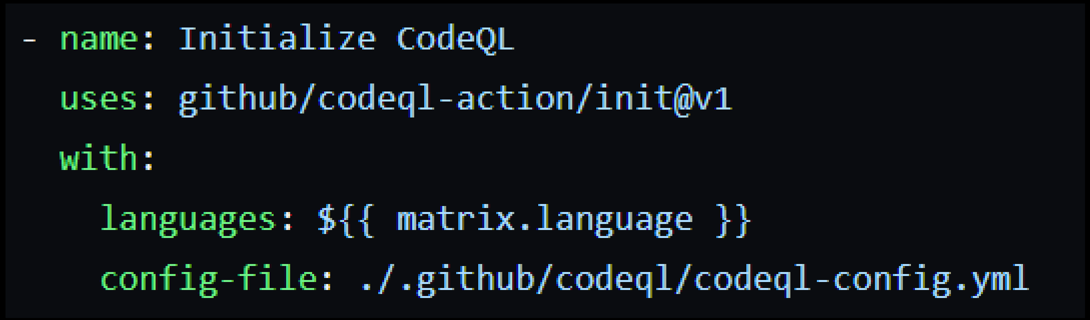
Dependabot

Security alerts on dependencies

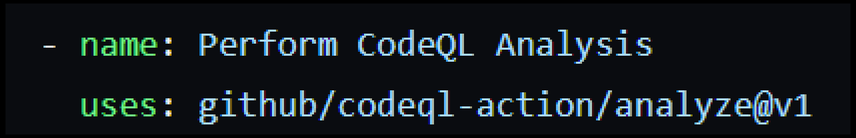
Secret scanning

CodeQL

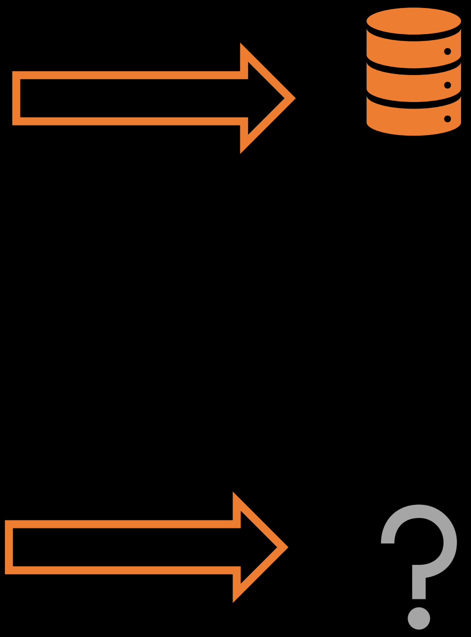
CodeQL – What is it?



```
- name: Initialize CodeQL
  uses: github/codeql-action/init@v1
  with:
    languages: ${{ matrix.language }}
    config-file: ./.github/codeql/codeql-config.yml
```



```
 - name: Perform CodeQL Analysis
   uses: github/codeql-action/analyze@v1
```



Database

Query

Using CodeQL

Free for public repos, uses your own Action minutes

CLI support

Open-source queries

Support for:

- javascript
- c#
- java
- c++
- go
- python
- ruby

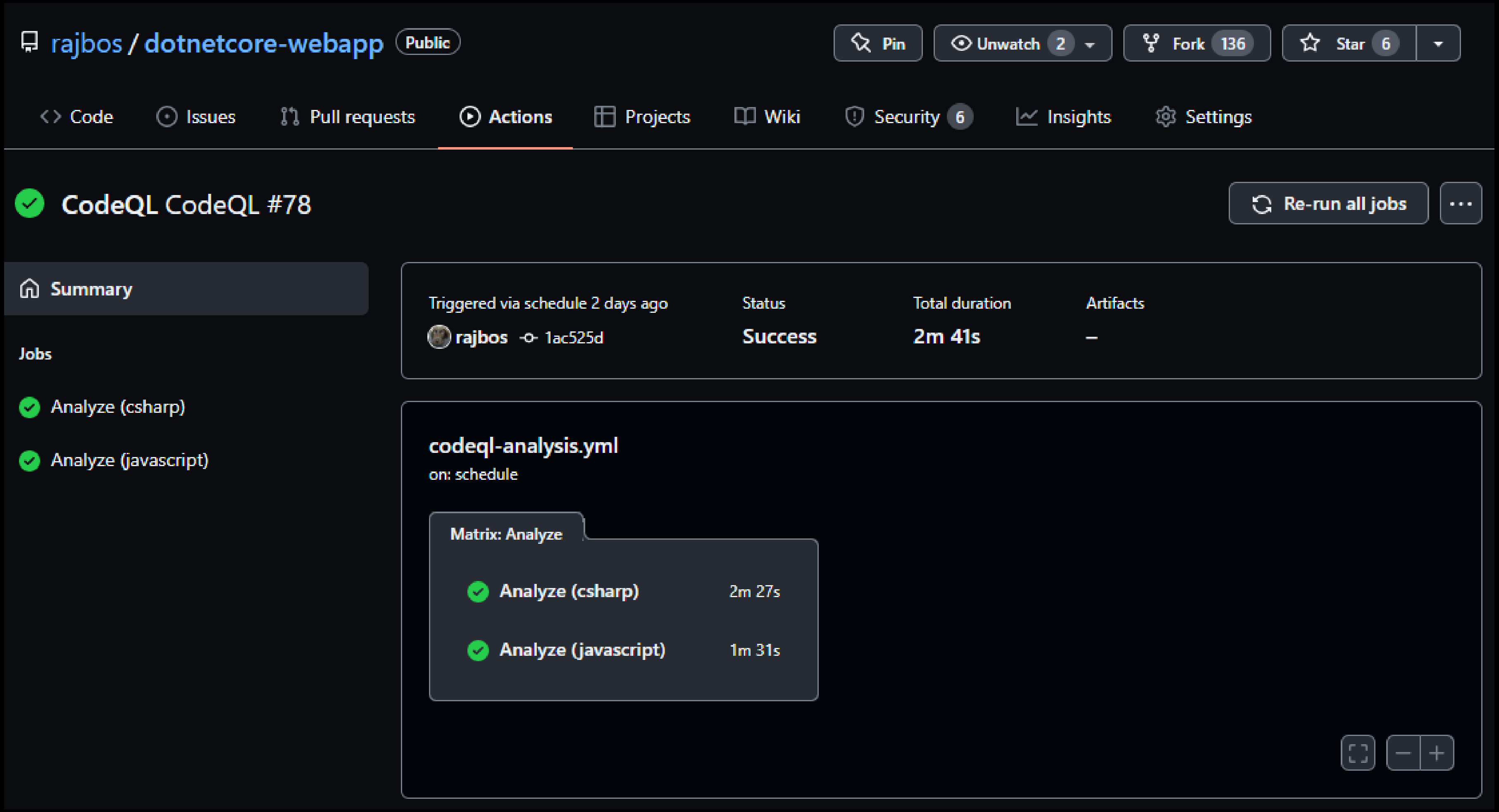
CodeQL - demo

a: https://github.com/rajbos/TailwindTraders-Website

b: https://github.com/github/codeql

c: https://sarifweb.azurewebsites.net/

CodeQL - demo



rajbos / dotnetcore-webapp Public

CodeQL CodeQL #78

Jobs

- Analyze (csharp)
- Analyze (javascript)

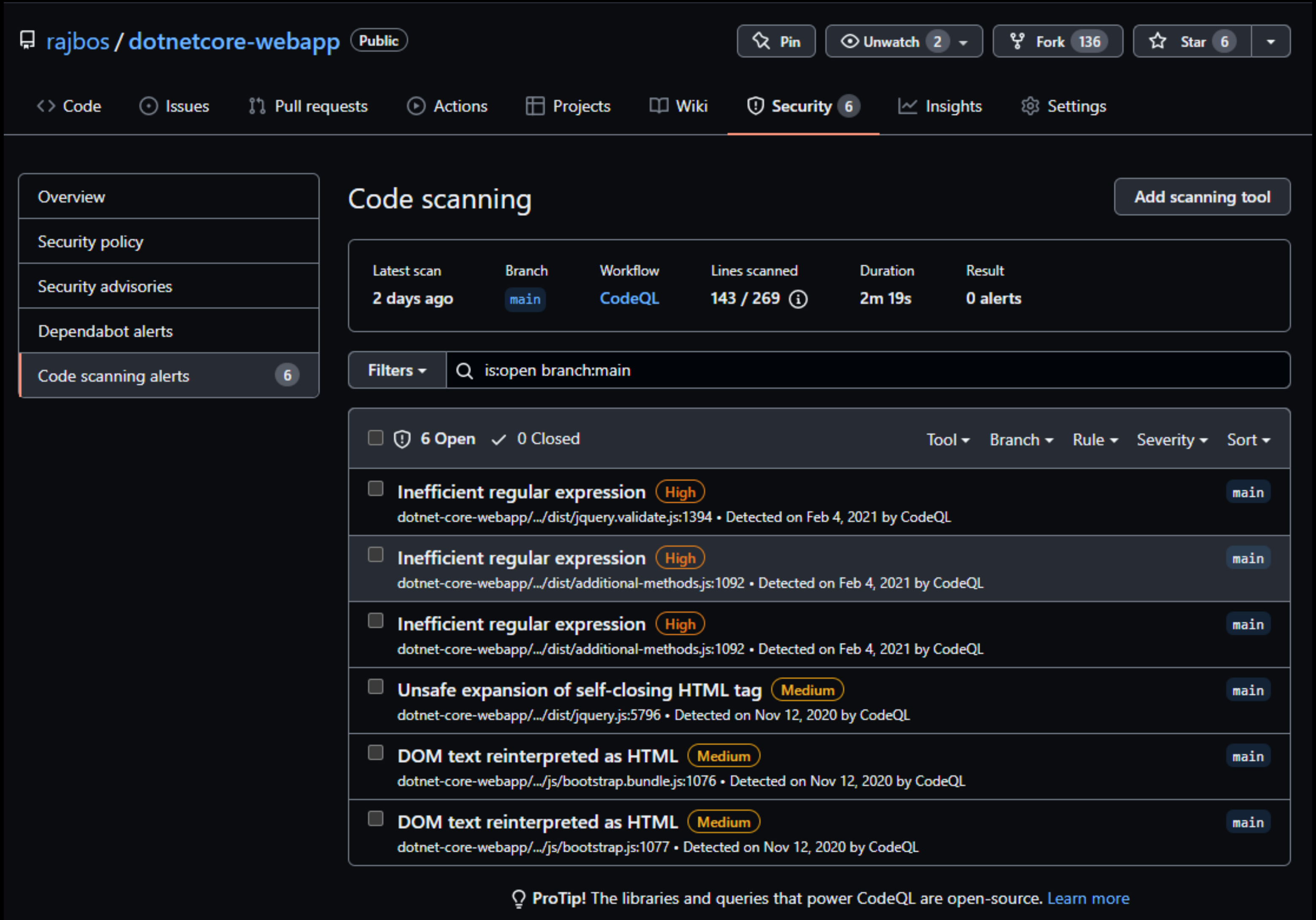
Triggered via schedule 2 days ago	Status	Total duration	Artifacts
rajbos 1ac525d	Success	2m 41s	–

codeql-analysis.yml
on: schedule

Matrix: Analyze

Analyze (csharp)	2m 27s
Analyze (javascript)	1m 31s

CodeQL - demo



Code scanning

Latest scan	Branch	Workflow	Lines scanned	Duration	Result
2 days ago	main	CodeQL	143 / 269	2m 19s	0 alerts

is:open branch:main

□ 6 Open ✓ 0 Closed

□ **Inefficient regular expression** High — main
dotnet-core-webapp/.../dist/jquery.validate.js:1394 • Detected on Feb 4, 2021 by CodeQL

□ **Inefficient regular expression** High — main
dotnet-core-webapp/.../dist/additional-methods.js:1092 • Detected on Feb 4, 2021 by CodeQL

□ **Inefficient regular expression** High — main
dotnet-core-webapp/.../dist/additional-methods.js:1092 • Detected on Feb 4, 2021 by CodeQL

□ **Unsafe expansion of self-closing HTML tag** Medium — main
dotnet-core-webapp/.../dist/jquery.js:5796 • Detected on Nov 12, 2020 by CodeQL

□ **DOM text reinterpreted as HTML** Medium — main
dotnet-core-webapp/.../js/bootstrap.bundle.js:1076 • Detected on Nov 12, 2020 by CodeQL

□ **DOM text reinterpreted as HTML** Medium — main
dotnet-core-webapp/.../js/bootstrap.js:1077 • Detected on Nov 12, 2020 by CodeQL

ProTip! The libraries and queries that power CodeQL are open-source. Learn more

Security features – overview

Commit signing

Dependabot

Security alerts on dependencies

Secret scanning

CodeQL

Protect your code with GitHub security features

dotnetsheff

Rob Bos

DevOps Consultant – Xpirit

The Netherlands

https://devopsjournal.io

@robbos81

https://myoctocat.com