GitHub

GitHub Advanced Security Features and Demo

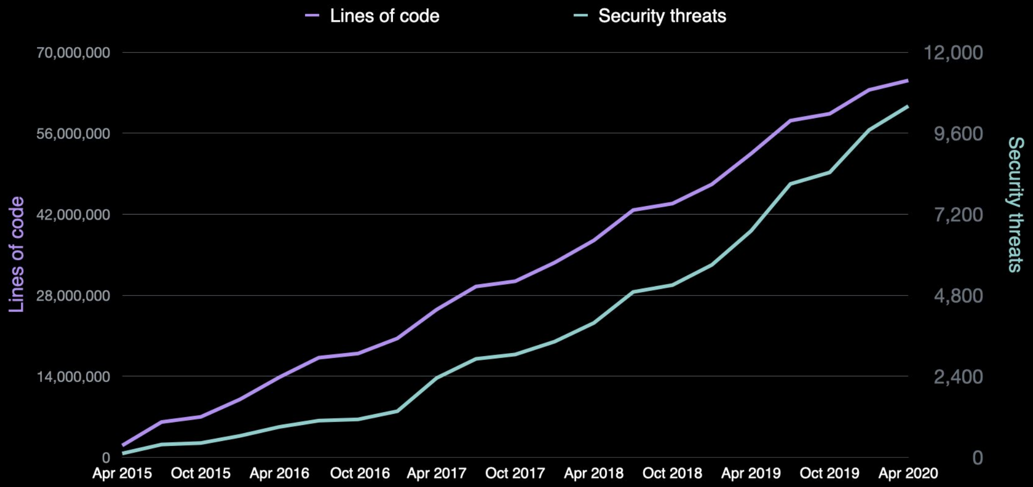
@joshjohanning | February 2022

Agenda

- What is GitHub Advanced Security (GHAS), and why?
- Demo
- Questions

What is GitHub Advanced Security?

More code = more technical debt & exposure

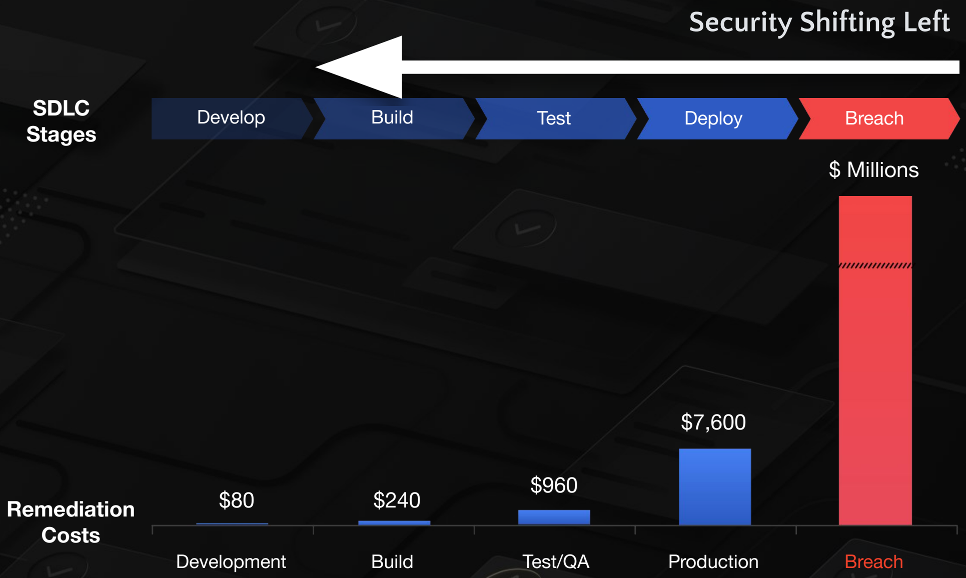


Source: GitHub Data Science Team analysis of 70 million lines of code in major OSS projects added over a 5 year period

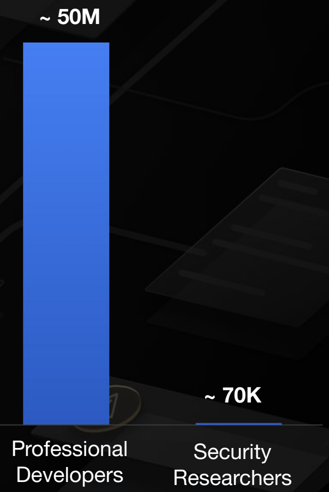
Flaws in applications are consistently the #1 attack vector for breaches

Source: Verizon Data Breach Investigations reports 2016, 2017, 2018, 2019 and 2020.

Solution: Shift security left, but how?

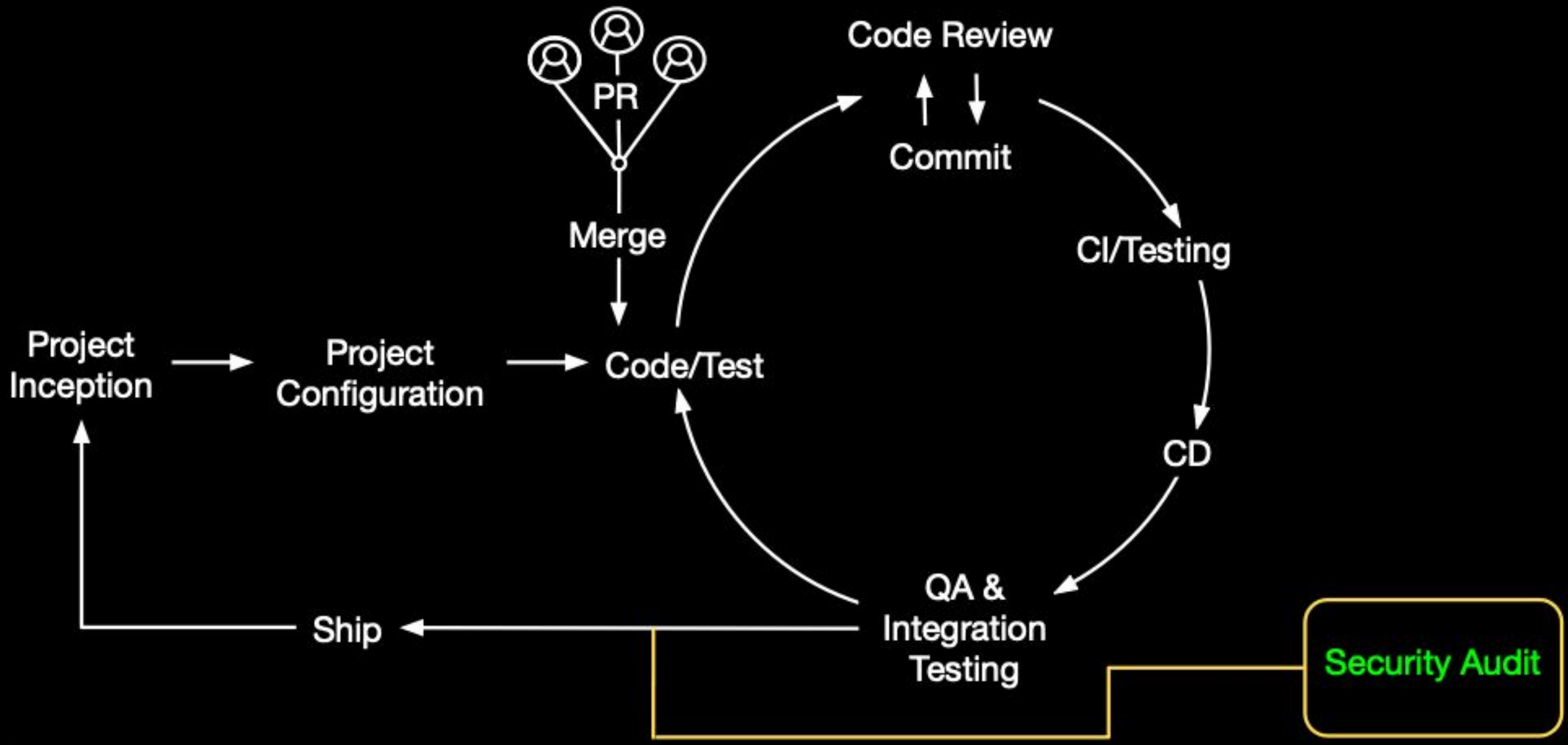


Vastly more cost effective to remediate during development

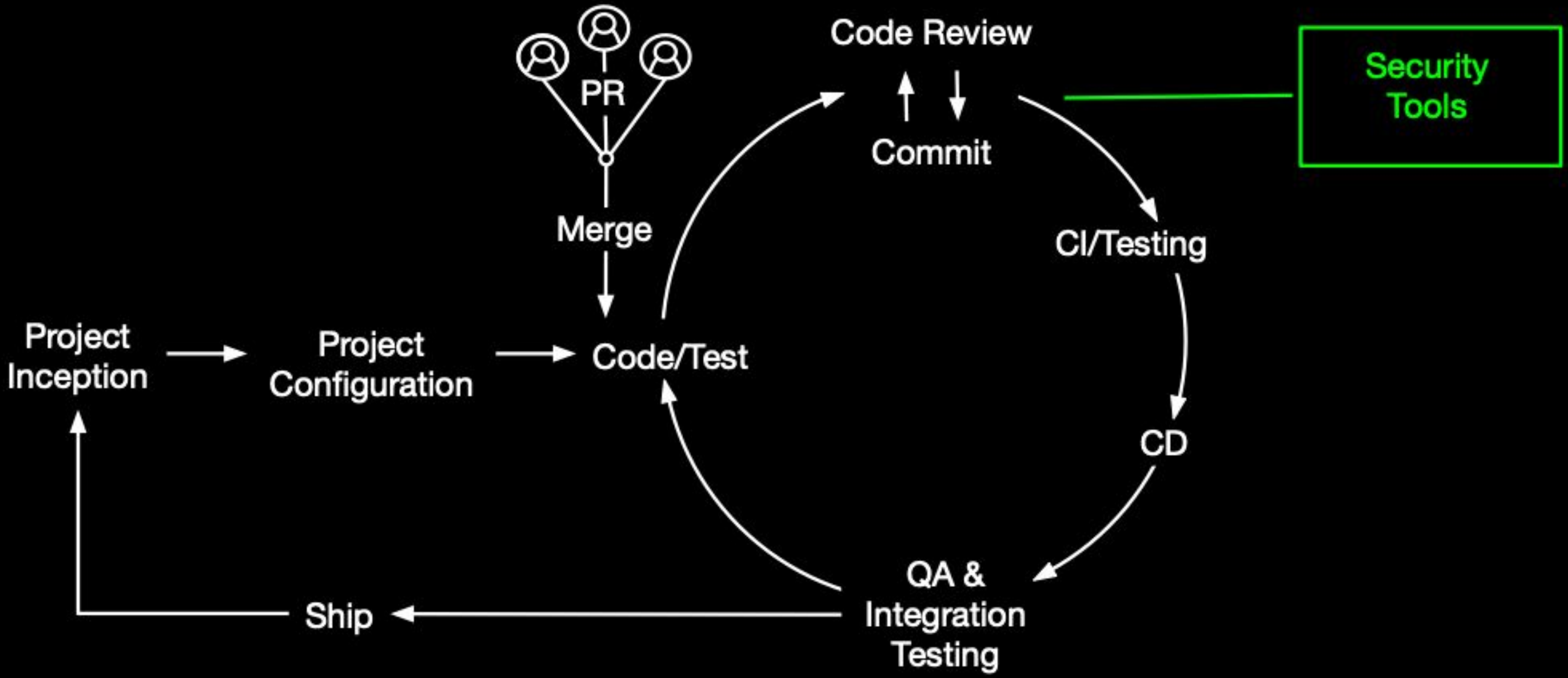


570x more developers than security researchers

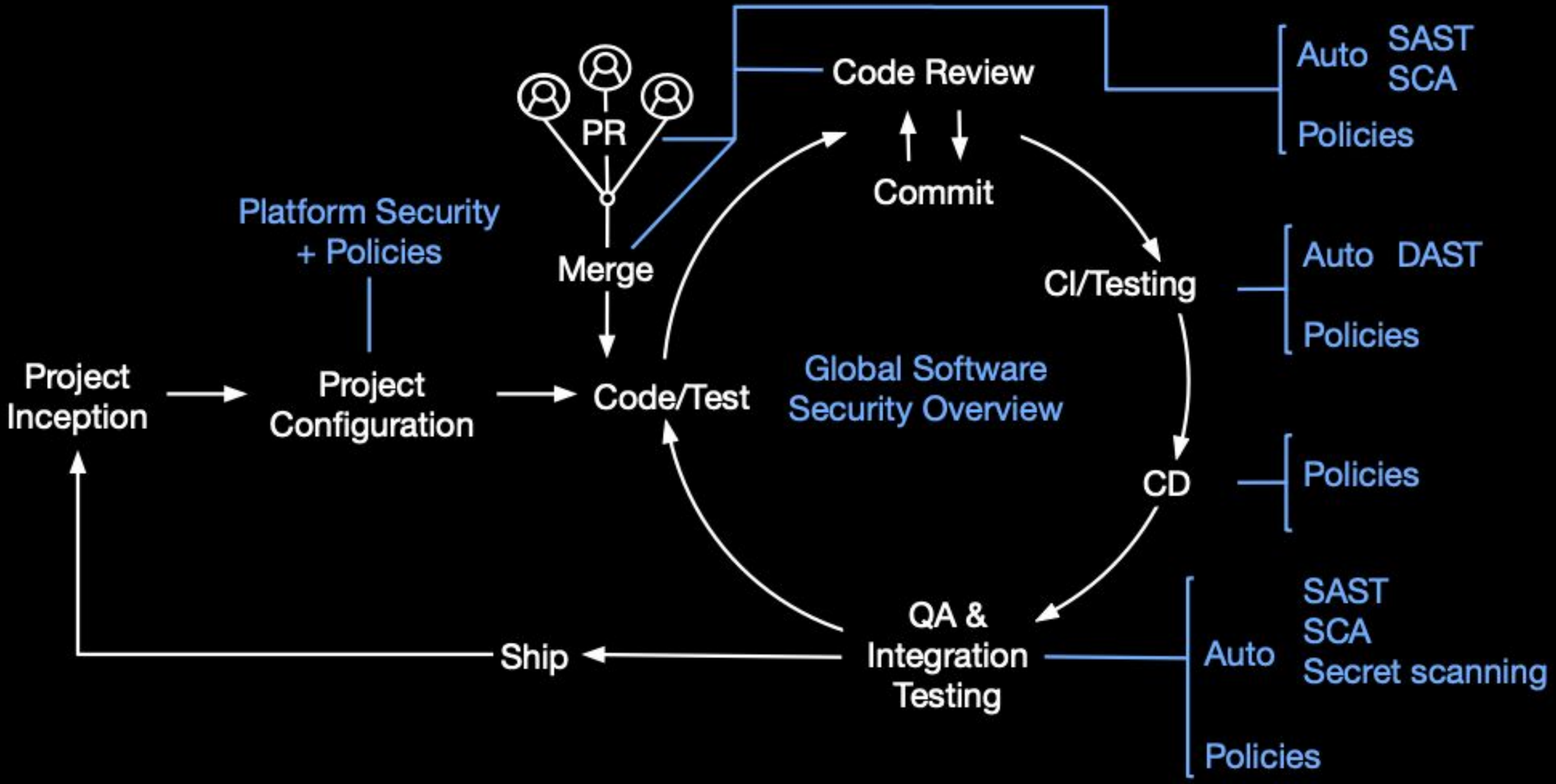
Basic application security scenario



Improved application security scenario



Application security - Targeted State



GitHub delivers **complete application security**

1. Developer-first
2. Native
3. Automated

GitHub secures your complete software lifecycle

Supply Chain

Code

Development Lifecycle

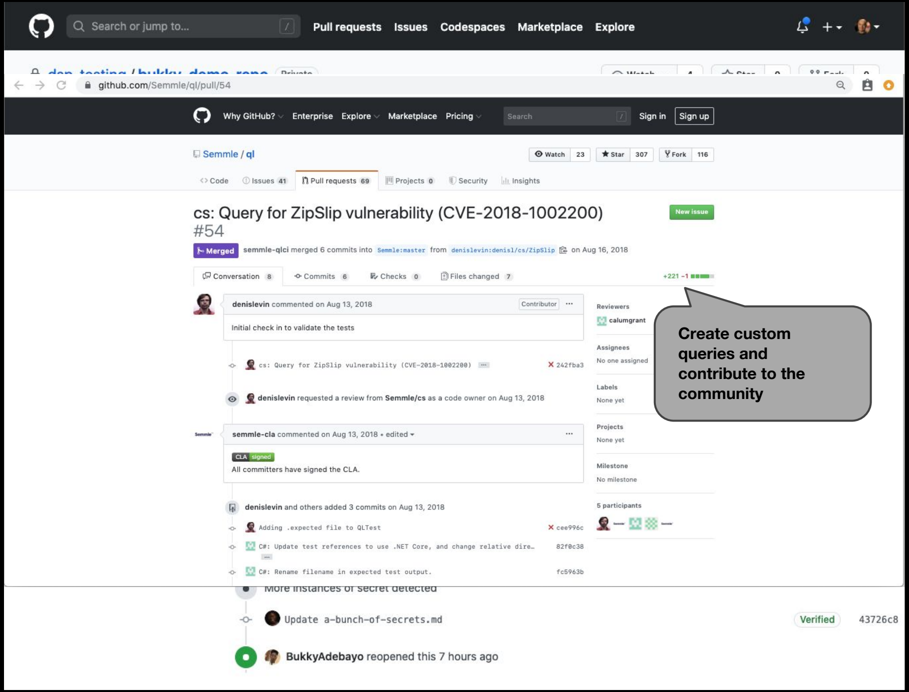
Platform for Security Governance

Secure your source code

Fail fast by finding vulnerabilities
as code is developed

Find hard-coded secrets
in code base

Set coding standards
across your entire
organisation



cs: Query for ZipSlip vulnerability (CVE-2018-1002200) #54

Merged semmle-qlci merged 6 commits into `Semmle:master` from `denislevin:denisl/cs/ZipSlip` on Aug 16, 2018

denislevin commented on Aug 13, 2018

Initial check in to validate the tests

```
cs: Query for ZipSlip vulnerability (CVE-2018-1002200)    ✕ 242fba3
```

denislevin requested a review from Semmle/cs as a code owner on Aug 13, 2018

semmle-cla commented on Aug 13, 2018 • edited

All committers have signed the CLA.

denislevin and others added 3 commits on Aug 13, 2018

```
Adding .expected file to QLTest    ✕ cee996c
C#: Update test references to use .NET Core, and change relative dire…    82f0c38
C#: Rename filename in expected test output.    fc5963b
```

More instances of secret detected

```
Update a-bunch-of-secrets.md    Verified    43726c8
```

BukkyAdebayo reopened this 7 hours ago

Create custom queries and contribute to the community

72%

Fix rate of vulnerabilities identified by CodeQL during a pull request

15% → **45%**

Fix rate after 7 days
Industry norm

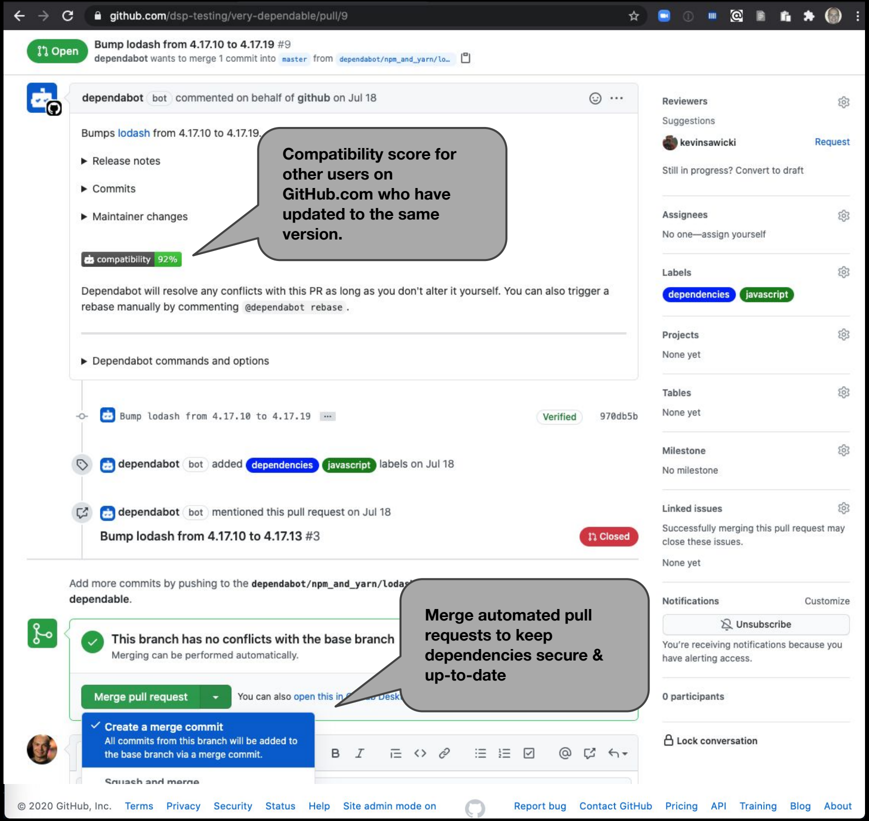
Fix rate after 90 days
Industry norm

Secure your supply chain

Know
your environment

Manage
your dependencies

Fix and publish
vulnerability information



github.com/dsp-testing/very-dependable/pull/9

Open **Bump lodash from 4.17.10 to 4.17.19** #9
dependabot wants to merge 1 commit into `master` from `dependabot/npm_and_yarn/lo…`

dependabot bot commented on behalf of **github** on Jul 18

Bumps lodash from 4.17.10 to 4.17.19.

- ▶ Release notes
- ▶ Commits
- ▶ Maintainer changes

compatibility 92%

Compatibility score for other users on GitHub.com who have updated to the same version.

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 lodash from 4.17.10 to 4.17.19` … Verified 970db5b

dependabot bot added dependencies javascript labels on Jul 18

dependabot bot mentioned this pull request on Jul 18
Bump lodash from 4.17.10 to 4.17.13 #3 Closed

Add more commits by pushing to the **`dependabot/npm_and_yarn/lodas`**
dependable.

This branch has no conflicts with the base branch
Merging can be performed automatically.

Merge pull request ▾ You can also open this in

✓ **Create a merge commit**
All commits from this branch will be added to the base branch via a merge commit.

Squash and merge

Merge automated pull requests to keep dependencies secure & up-to-date

Reviewers
Suggestions
kevinsawicki Request
Still in progress? Convert to draft

Assignees
No one—assign yourself

Labels
dependencies javascript

Projects
None yet

Tables
None yet

Milestone
No milestone

Linked issues
Successfully merging this pull request may close these issues.
None yet

Notifications Customize
Unsubscribe
You're receiving notifications because you have alerting access.

0 participants

Lock conversation

© 2020 GitHub, Inc. Terms Privacy Security Status Help Site admin mode on Report bug Contact GitHub Pricing API Training Blog About

40 days

Mean time to remediate (MTTR)
for repos with Dependabot security updates

180+ days

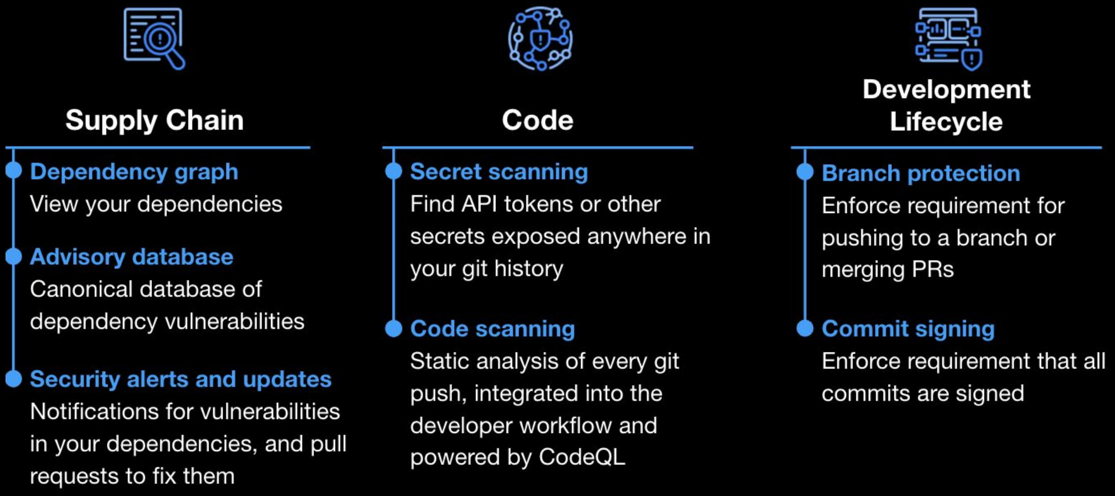
Mean time to remediate (MTTR)
Industry norm

Next steps...

Demo

Demo Overview

- Configure GitHub Advanced Security
  - Difference between public repo / Enterprise
- Secret Scanning
  - Committing secrets to source
  - Managing secrets in repositories
  - Custom patterns
- Code Scanning / CodeQL
  - Alerts
  - Creating workflow and my workflow
  - Other partners (ie: IaaC scans)
- Dependabot
  - Security Alerts and Updates
  - Dependency Graph
  - Version Updates
- Security Overview
- Vulnerability Database



Supply Chain

Dependency graph
View your dependencies

Advisory database
Canonical database of dependency vulnerabilities

Security alerts and updates
Notifications for vulnerabilities in your dependencies, and pull requests to fix them

Code

Secret scanning
Find API tokens or other secrets exposed anywhere in your git history

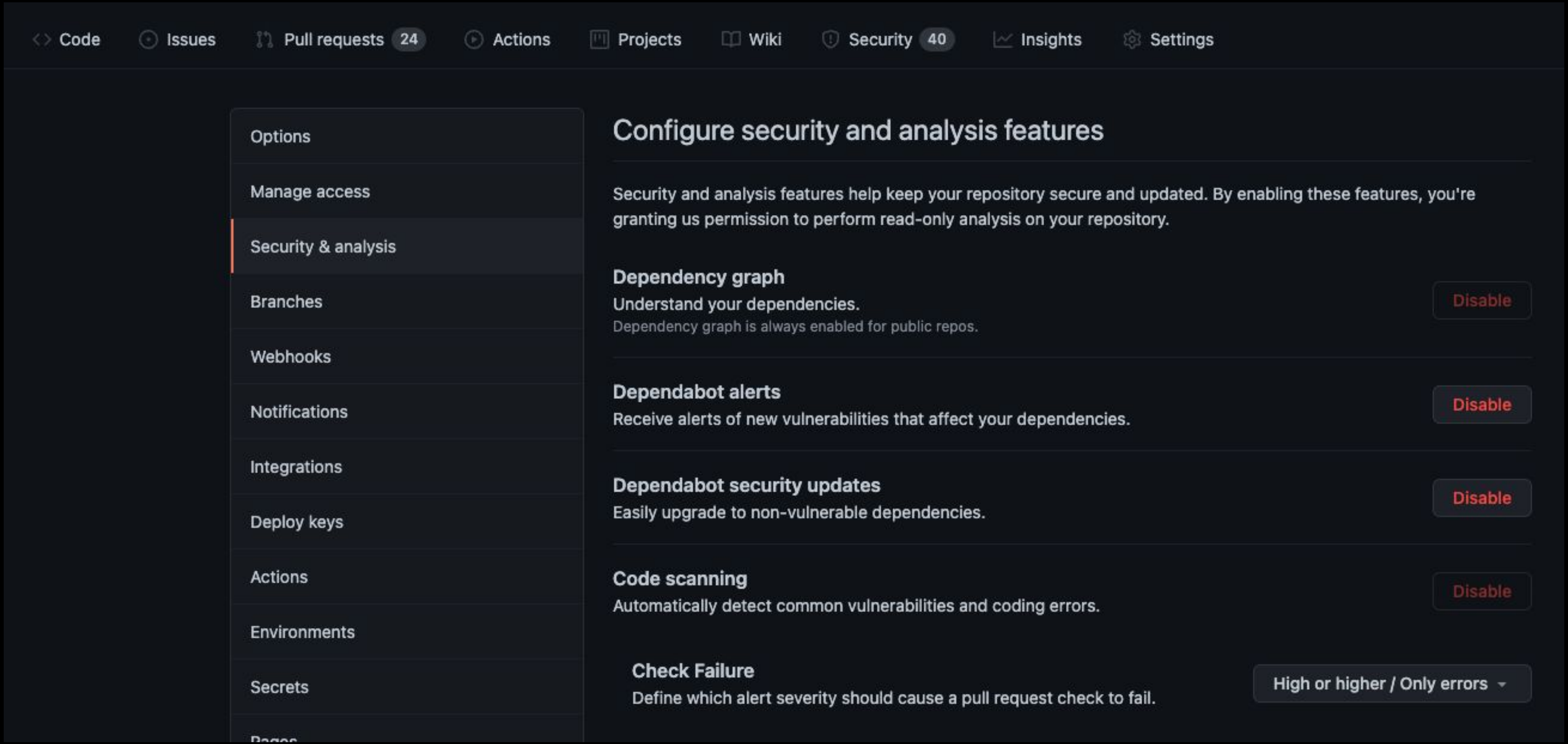
Code scanning
Static analysis of every git push, integrated into the developer workflow and powered by CodeQL

Development Lifecycle

Branch protection
Enforce requirement for pushing to a branch or merging PRs

Commit signing
Enforce requirement that all commits are signed

GHAS Setup - GitHub.com (public repo)



Configure security and analysis features

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.
Dependency graph is always enabled for public repos.
Disable

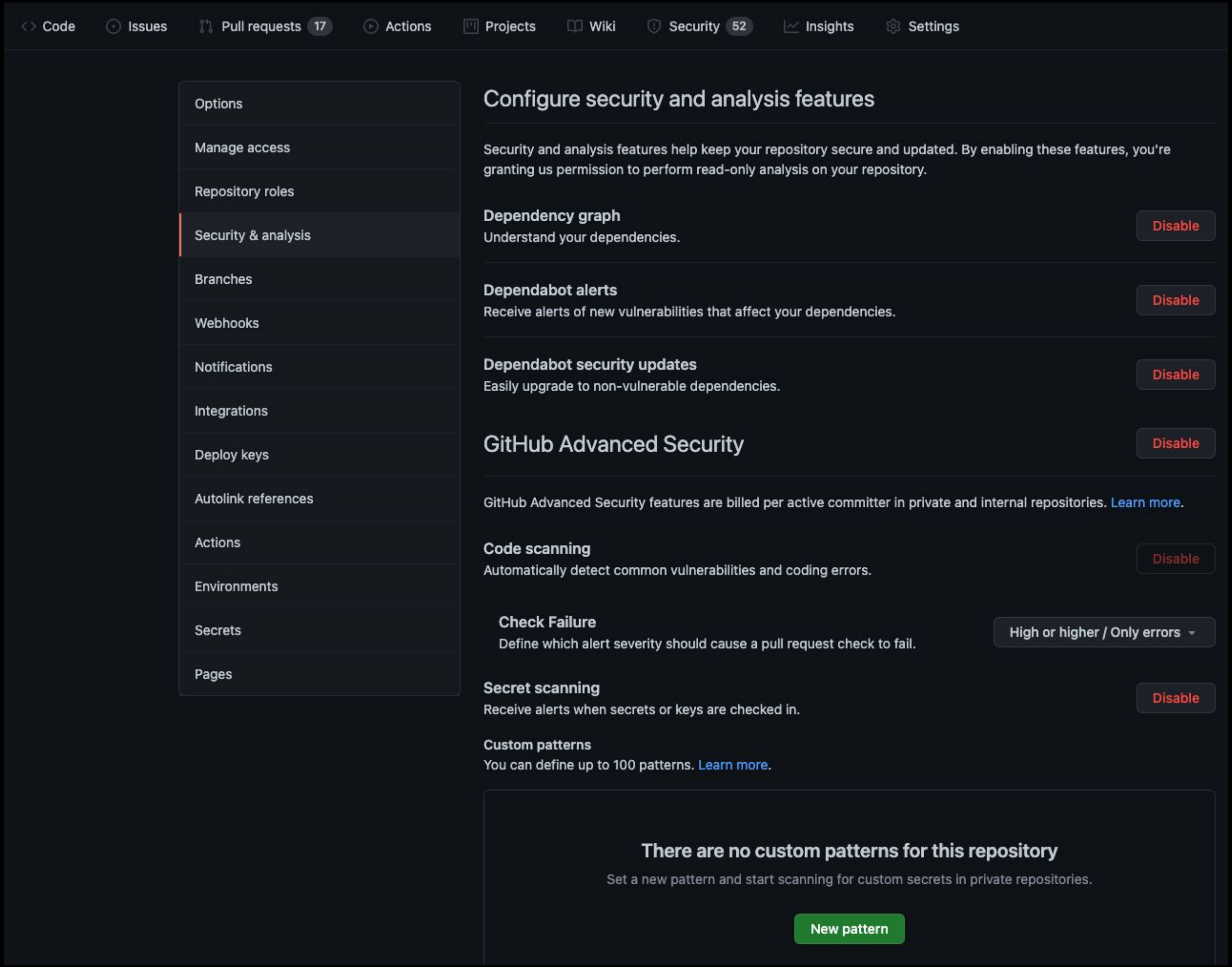
Dependabot alerts
Receive alerts of new vulnerabilities that affect your dependencies.
Disable

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

Code scanning
Automatically detect common vulnerabilities and coding errors.
Disable

Check Failure
Define which alert severity should cause a pull request check to fail.
High or higher / Only errors ▾

GHAS Setup - GitHub Enterprise Cloud



Configure security and analysis features

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 Disable
Understand your dependencies.

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

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

GitHub Advanced Security Disable

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

Code scanning Disable
Automatically detect common vulnerabilities and coding errors.

Check Failure High or higher / Only errors
Define which alert severity should cause a pull request check to fail.

Secret scanning Disable
Receive alerts when secrets or keys are checked in.

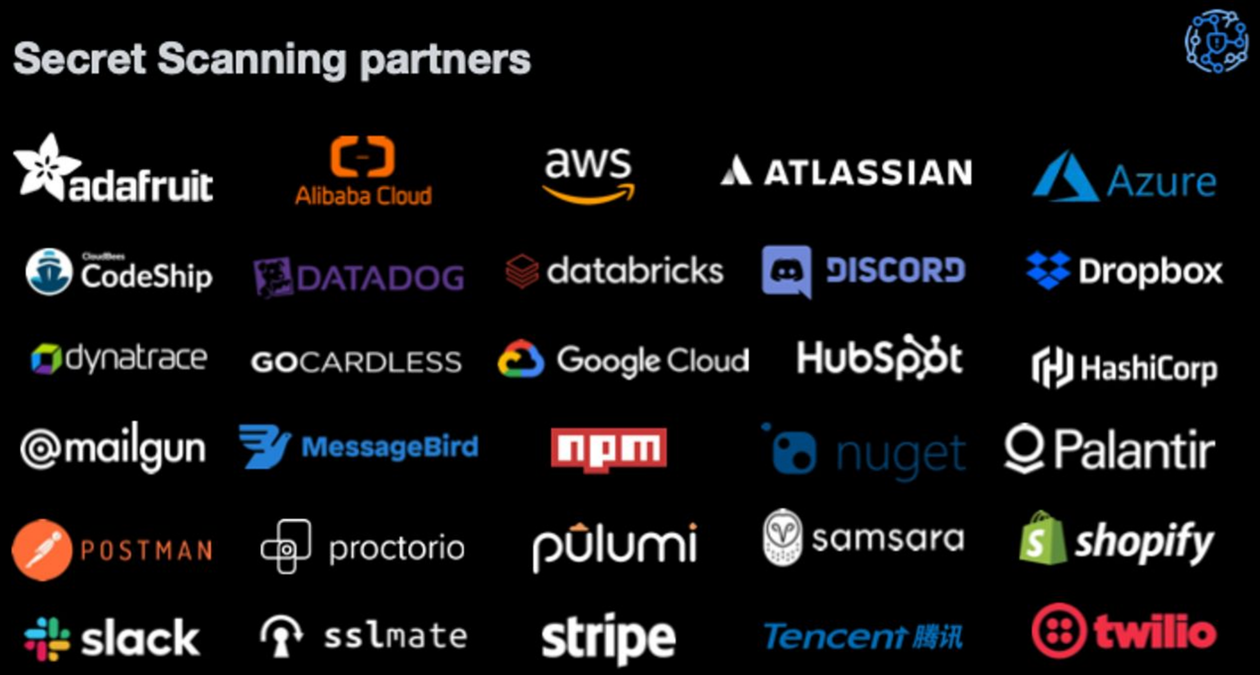
Custom patterns
You can define up to 100 patterns. Learn more.

There are no custom patterns for this repository

Set a new pattern and start scanning for custom secrets in private repositories.

New pattern

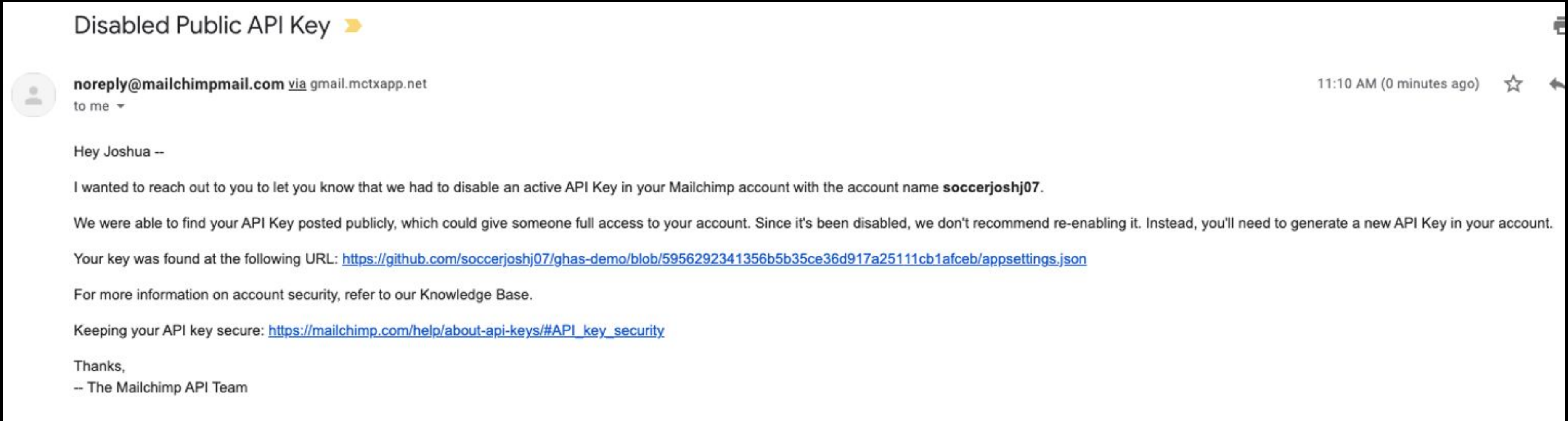
Secret Scanning - Partners



Secret Scanning partners

https://docs.github.com/en/code-security/secret-scanning/about-secret-scanning

Secret Scanning - Revoked API Key Email (public .com)



Disabled Public API Key

noreply@mailchimpmail.com via gmail.mctxapp.net
to me

11:10 AM (0 minutes ago)

Hey Joshua --

I wanted to reach out to you to let you know that we had to disable an active API Key in your Mailchimp account with the account name **soccerjoshj07**.

We were able to find your API Key posted publicly, which could give someone full access to your account. Since it's been disabled, we don't recommend re-enabling it. Instead, you'll need to generate a new API Key in your account.

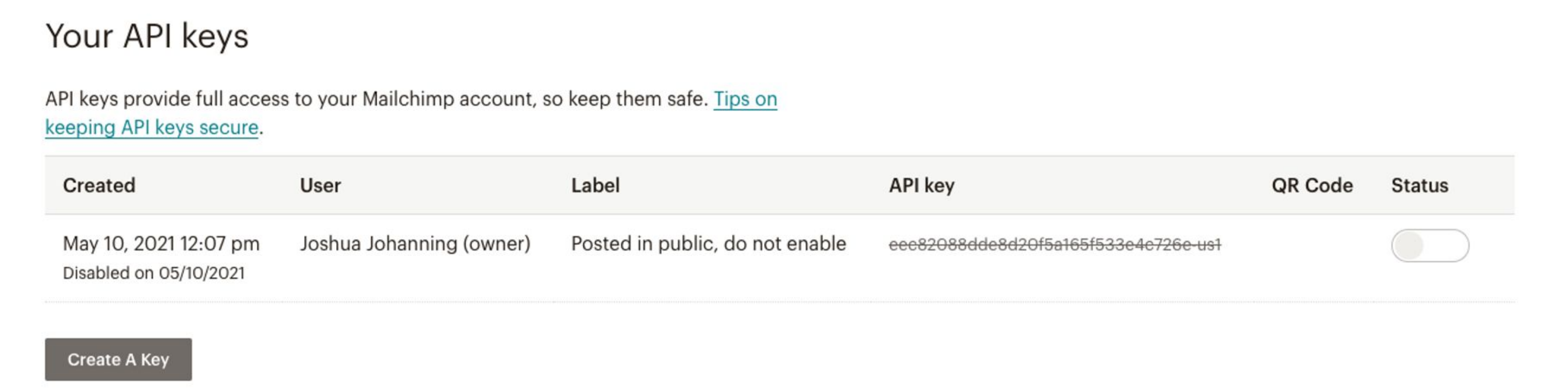
Your key was found at the following URL: https://github.com/soccerjoshj07/ghas-demo/blob/5956292341356b5b35ce36d917a25111cb1afceb/appsettings.json

For more information on account security, refer to our Knowledge Base.

Keeping your API key secure: https://mailchimp.com/help/about-api-keys/#API_key_security

Thanks,
-- The Mailchimp API Team

Secret Scanning - Revoked API Key (public .com)

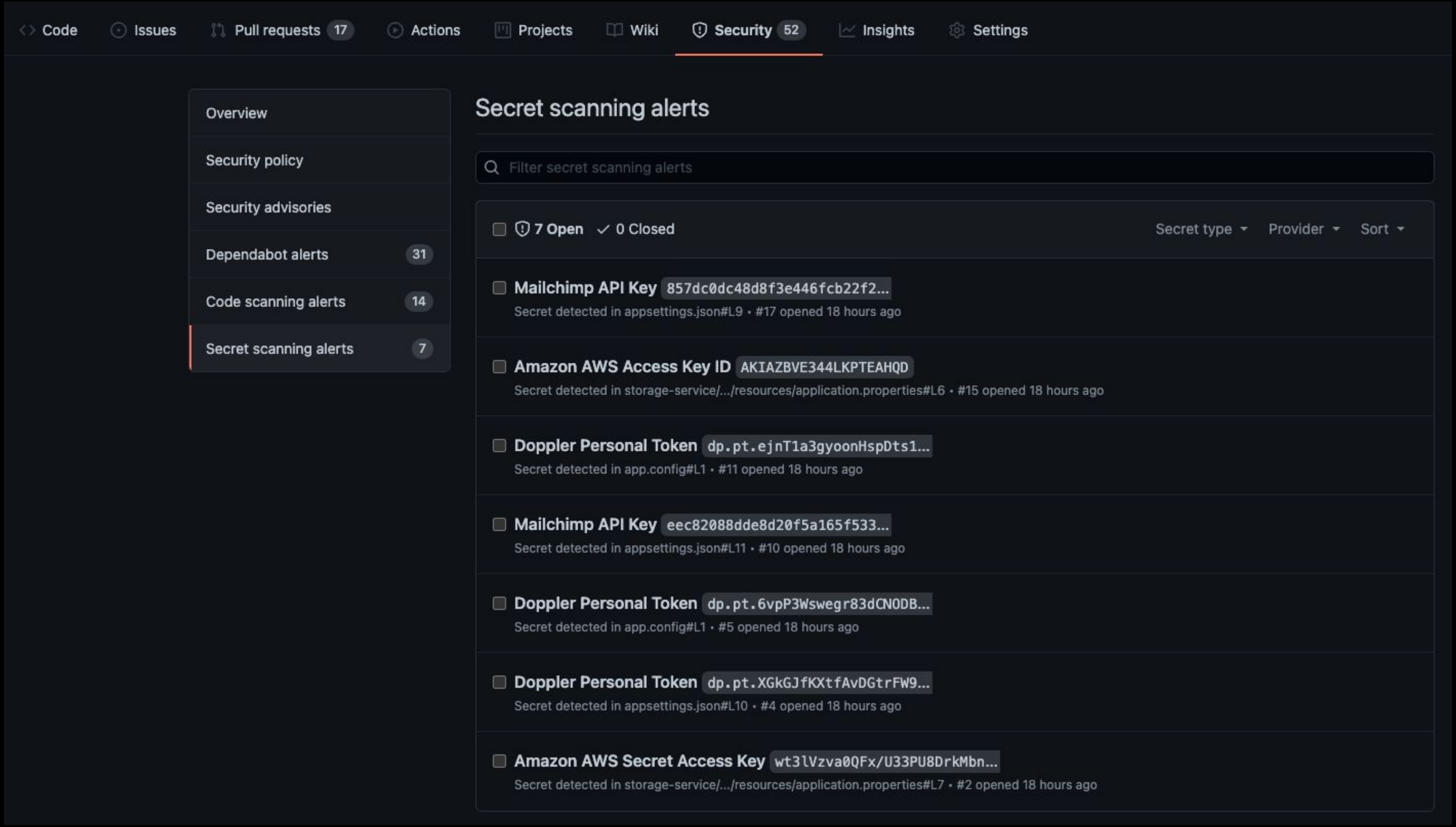


Your API keys

API keys provide full access to your Mailchimp account, so keep them safe. Tips on keeping API keys secure.

Created	User	Label	API key	QR Code	Status
May 10, 2021 12:07 pm Disabled on 05/10/2021	Joshua Johanning (owner)	Posted in public, do not enable	~~eec82088dde8d20f5a165f533e4c726e-us1~~		○

Secret Scanning - GitHub Enterprise Cloud



Secret scanning alerts

□ 7 Open ✓ 0 Closed

□ **Mailchimp API Key** `857dc0dc48d8f3e446fcb22f2...`
Secret detected in appsettings.json#L9 • #17 opened 18 hours ago

□ **Amazon AWS Access Key ID** `AKIAZBVE344LKPTEAHQD`
Secret detected in storage-service/.../resources/application.properties#L6 • #15 opened 18 hours ago

□ **Doppler Personal Token** `dp.pt.ejnT1a3gyoonHspDts1...`
Secret detected in app.config#L1 • #11 opened 18 hours ago

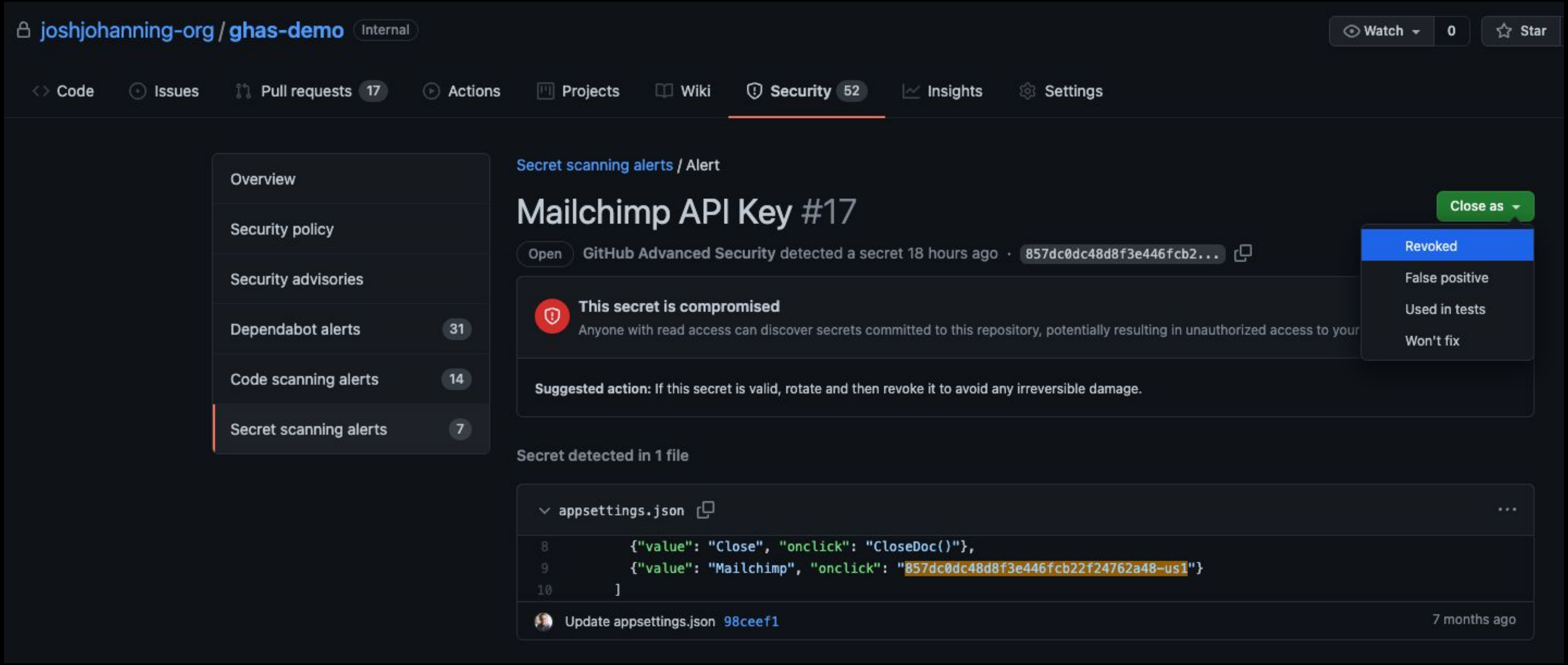
□ **Mailchimp API Key** `eec82088dde8d20f5a165f533...`
Secret detected in appsettings.json#L11 • #10 opened 18 hours ago

□ **Doppler Personal Token** `dp.pt.6vpP3Wswegr83dCNODB...`
Secret detected in app.config#L1 • #5 opened 18 hours ago

□ **Doppler Personal Token** `dp.pt.XGkGJfKXtfAvDGtrFW9...`
Secret detected in appsettings.json#L10 • #4 opened 18 hours ago

□ **Amazon AWS Secret Access Key** `wt3lVzva0QFx/U33PU8DrkMbn...`
Secret detected in storage-service/.../resources/application.properties#L7 • #2 opened 18 hours ago

Secret Scanning - GitHub Enterprise Cloud



Secret scanning alerts / Alert

Mailchimp API Key #17

Open GitHub Advanced Security detected a secret 18 hours ago · `857dc0dc48d8f3e446fcb2...`

This secret is compromised

Anyone with read access can discover secrets committed to this repository, potentially resulting in unauthorized access to your

Suggested action: If this secret is valid, rotate and then revoke it to avoid any irreversible damage.

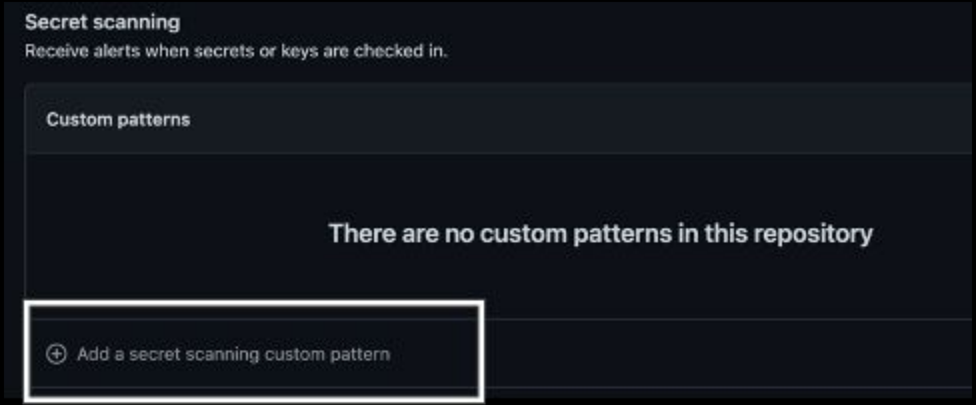
Secret detected in 1 file

appsettings.json

```
        {"value": "Close", "onclick": "CloseDoc()"},
        {"value": "Mailchimp", "onclick": "857dc0dc48d8f3e446fcb22f24762a48-us1"}
      ]
```

Update appsettings.json 98ceef1 7 months ago

Secret Scanning - GitHub Enterprise Cloud - Custom Patterns

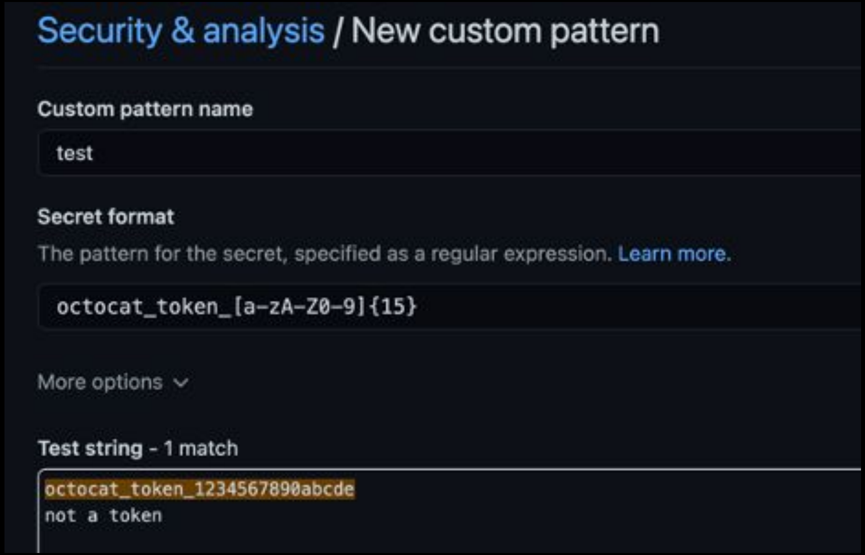


Secret scanning

Receive alerts when secrets or keys are checked in.

Custom patterns

There are no custom patterns in this repository



Security & analysis / New custom pattern

Custom pattern name

test

Secret format

The pattern for the secret, specified as a regular expression. Learn more.

```
octocat_token_[a-zA-Z0-9]{15}
```

Test string - 1 match

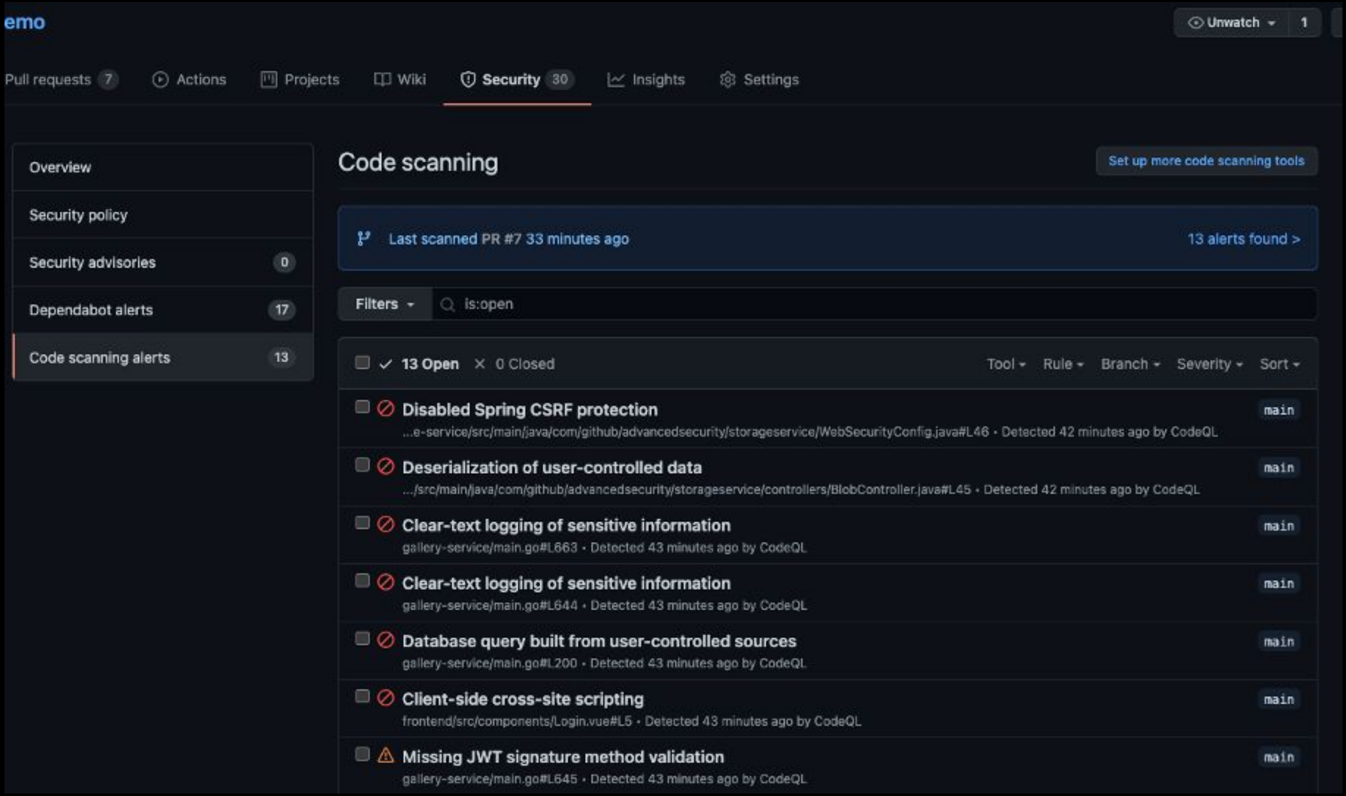
```
octocat_token_1234567890abcde
not a token
```

Code Scanning - CodeQL

CodeQL analysis consists of three steps:

1) Preparing the code, by creating a CodeQL database
2) Running CodeQL queries against the database
3) Interpreting the query results

Code Scanning - Open Alerts



Code scanning

Last scanned PR #7 33 minutes ago — 13 alerts found >

is:open

□ ✓ 13 Open ✕ 0 Closed

□ ⊘ **Disabled Spring CSRF protection** `main`
...e-service/src/main/java/com/github/advancedsecurity/storageservice/WebSecurityConfig.java#L46 • Detected 42 minutes ago by CodeQL

□ ⊘ **Deserialization of user-controlled data** `main`
.../src/main/java/com/github/advancedsecurity/storageservice/controllers/BlobController.java#L45 • Detected 42 minutes ago by CodeQL

□ ⊘ **Clear-text logging of sensitive information** `main`
gallery-service/main.go#L663 • Detected 43 minutes ago by CodeQL

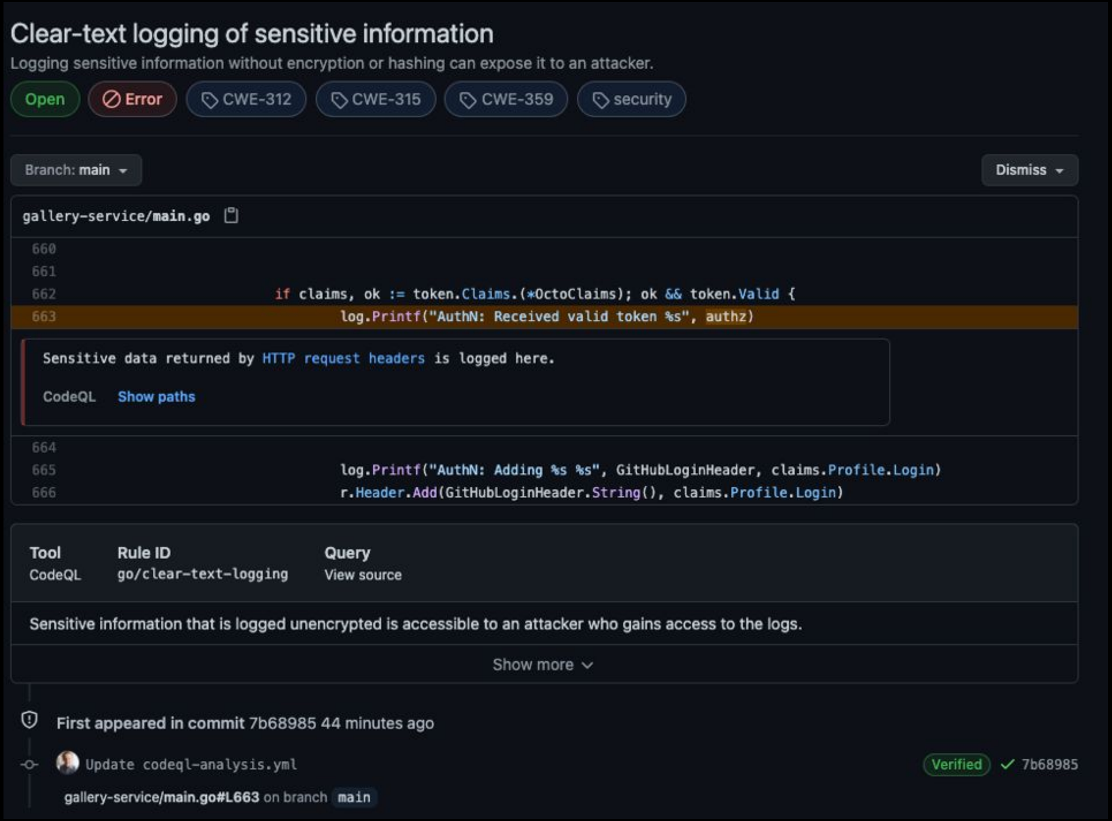
□ ⊘ **Clear-text logging of sensitive information** `main`
gallery-service/main.go#L644 • Detected 43 minutes ago by CodeQL

□ ⊘ **Database query built from user-controlled sources** `main`
gallery-service/main.go#L200 • Detected 43 minutes ago by CodeQL

□ ⊘ **Client-side cross-site scripting** `main`
frontend/src/components/Login.vue#L5 • Detected 43 minutes ago by CodeQL

□ ⚠ **Missing JWT signature method validation** `main`
gallery-service/main.go#L645 • Detected 43 minutes ago by CodeQL

Code Scanning - Example Alert



Clear-text logging of sensitive information

Logging sensitive information without encryption or hashing can expose it to an attacker.

gallery-service/main.go

```
            if claims, ok := token.Claims.(*OctoClaims); ok && token.Valid {
                log.Printf("AuthN: Received valid token %s", authz)
```

Sensitive data returned by HTTP request headers is logged here.

```

                log.Printf("AuthN: Adding %s %s", GitHubLoginHeader, claims.Profile.Login)
                r.Header.Add(GitHubLoginHeader.String(), claims.Profile.Login)
```

Tool	Rule ID	Query
CodeQL	go/clear-text-logging	View source

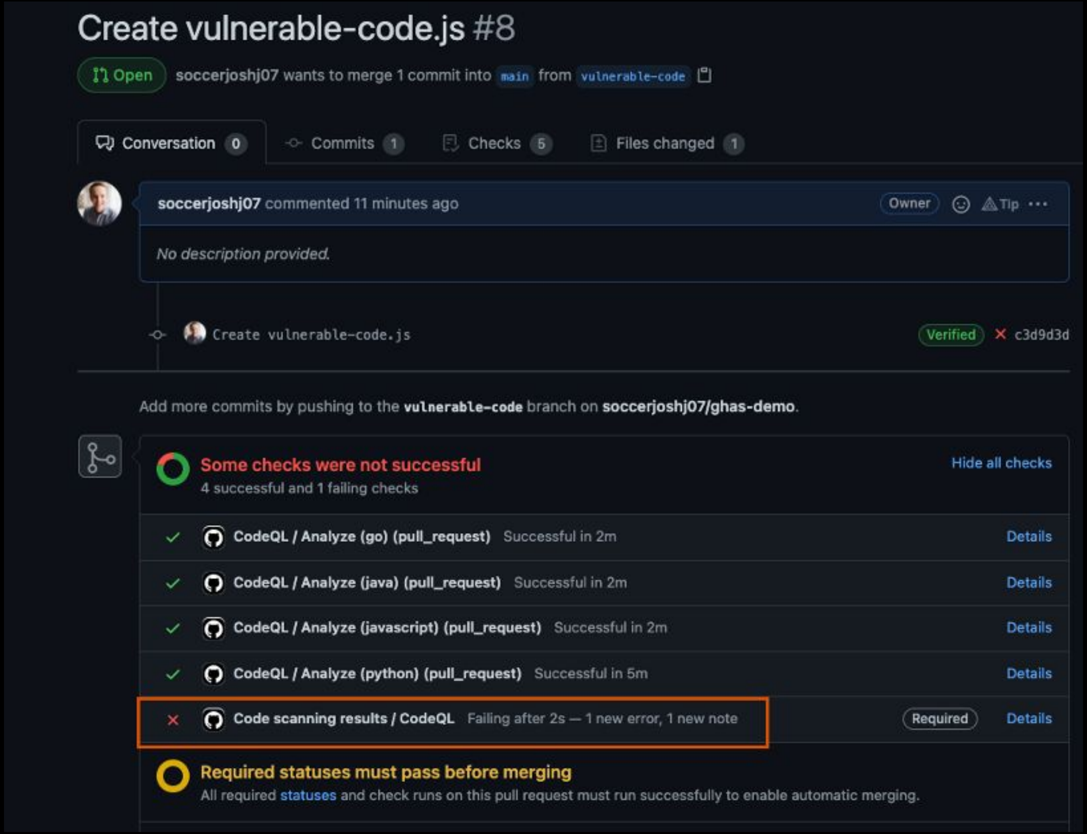
Sensitive information that is logged unencrypted is accessible to an attacker who gains access to the logs.

First appeared in commit 7b68985 44 minutes ago

Update codeql-analysis.yml

gallery-service/main.go#L663 on branch main

Code Scanning - Pull Request



Create vulnerable-code.js #8

Open soccerjoshj07 wants to merge 1 commit into `main` from `vulnerable-code`

soccerjoshj07 commented 11 minutes ago

No description provided.

Create vulnerable-code.js

✕ c3d9d3d

Add more commits by pushing to the **`vulnerable-code`** branch on **soccerjoshj07/ghas-demo**.

Some checks were not successful

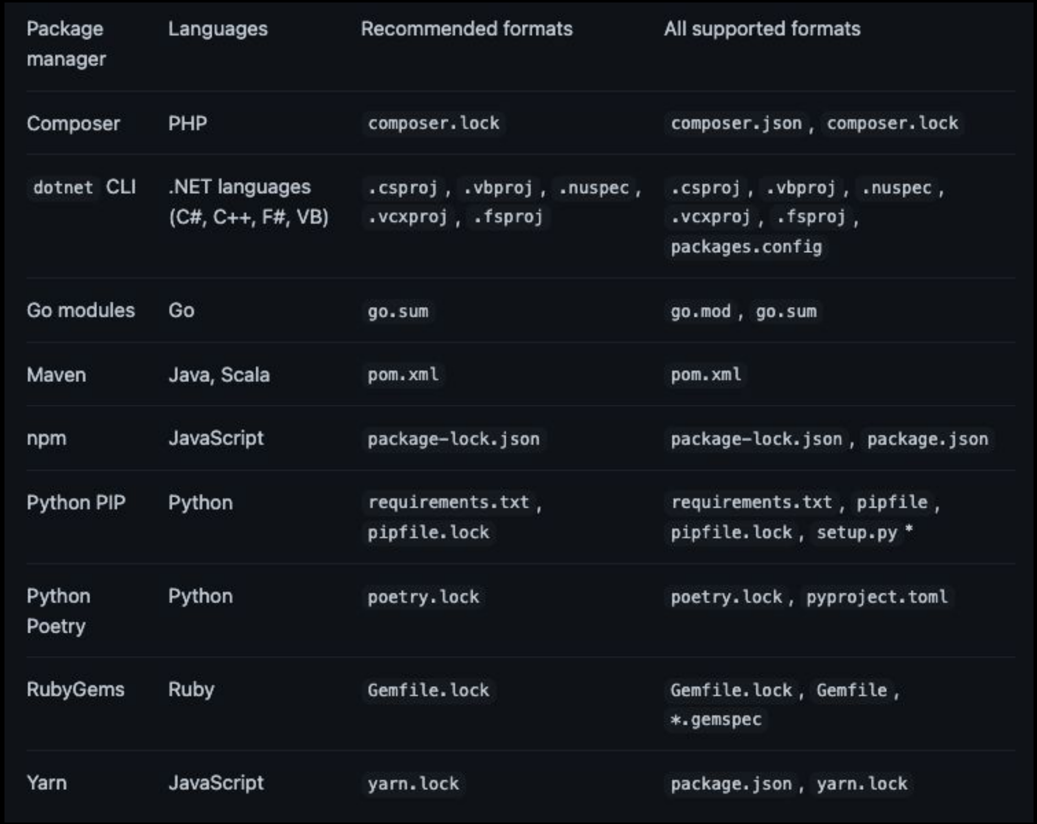
4 successful and 1 failing checks

✓	**CodeQL / Analyze (go) (pull_request)** Successful in 2m		Details
✓	**CodeQL / Analyze (java) (pull_request)** Successful in 2m		Details
✓	**CodeQL / Analyze (javascript) (pull_request)** Successful in 2m		Details
✓	**CodeQL / Analyze (python) (pull_request)** Successful in 5m		Details
✕	**Code scanning results / CodeQL** Failing after 2s — 1 new error, 1 new note	Required	Details

Required statuses must pass before merging

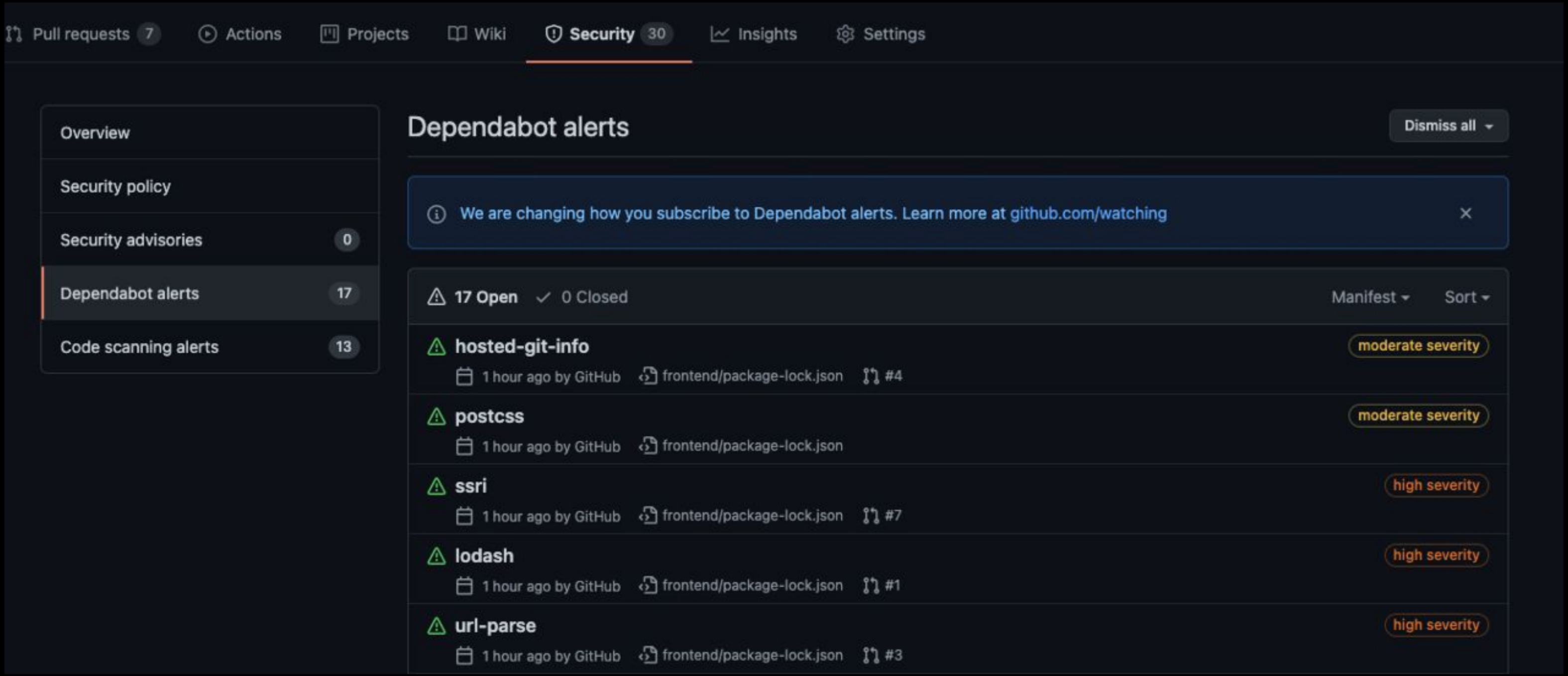
All required statuses and check runs on this pull request must run successfully to enable automatic merging.

Dependabot - Security Alerts - Supported Package Ecosystems



Package manager	Languages	Recommended formats	All supported formats
Composer	PHP	`composer.lock`	`composer.json`, `composer.lock`
`dotnet` CLI	.NET languages (C#, C++, F#, VB)	`.csproj`, `.vbproj`, `.nuspec`, `.vcxproj`, `.fsproj`	`.csproj`, `.vbproj`, `.nuspec`, `.vcxproj`, `.fsproj`, `packages.config`
Go modules	Go	`go.sum`	`go.mod`, `go.sum`
Maven	Java, Scala	`pom.xml`	`pom.xml`
npm	JavaScript	`package-lock.json`	`package-lock.json`, `package.json`
Python PIP	Python	`requirements.txt`, `pipfile.lock`	`requirements.txt`, `pipfile`, `pipfile.lock`, `setup.py` *
Python Poetry	Python	`poetry.lock`	`poetry.lock`, `pyproject.toml`
RubyGems	Ruby	`Gemfile.lock`	`Gemfile.lock`, `Gemfile`, `*.gemspec`
Yarn	JavaScript	`yarn.lock`	`package.json`, `yarn.lock`

Dependabot - Security Alerts - Open Alerts



Dependabot alerts

We are changing how you subscribe to Dependabot alerts. Learn more at github.com/watching

17 Open ✓ 0 Closed

hosted-git-info — moderate severity
1 hour ago by GitHub · frontend/package-lock.json · #4

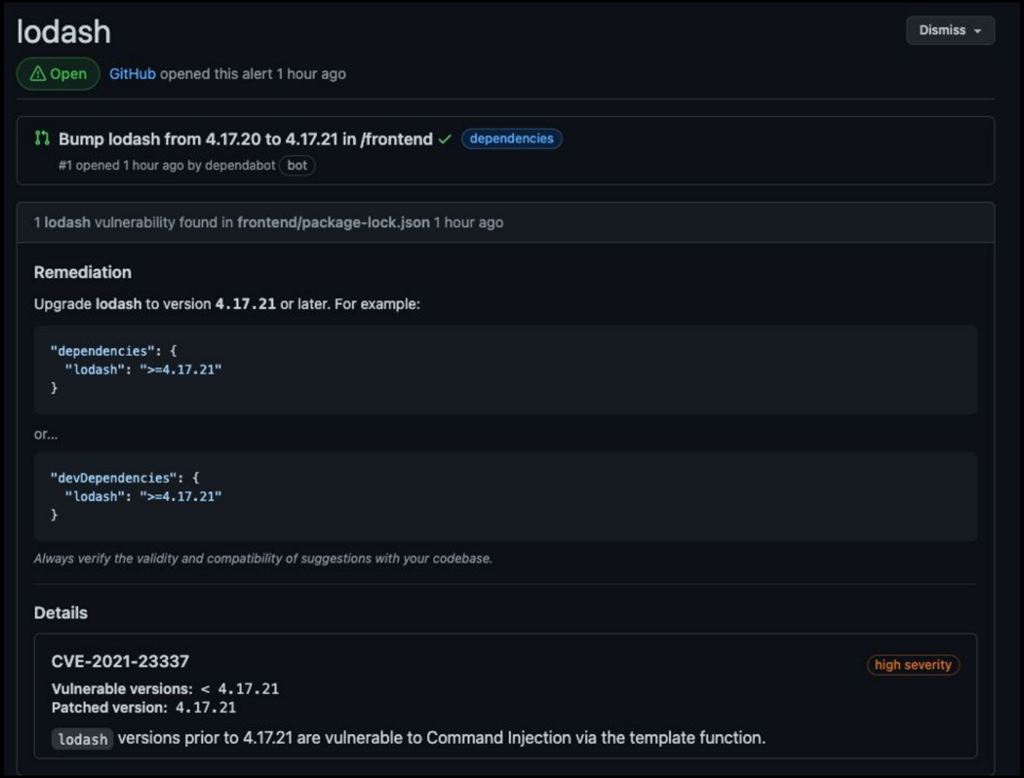
postcss — moderate severity
1 hour ago by GitHub · frontend/package-lock.json

ssri — high severity
1 hour ago by GitHub · frontend/package-lock.json · #7

lodash — high severity
1 hour ago by GitHub · frontend/package-lock.json · #1

url-parse — high severity
1 hour ago by GitHub · frontend/package-lock.json · #3

Dependabot - Security Alerts - Remediation



lodash

⚠ Open GitHub opened this alert 1 hour ago

Bump lodash from 4.17.20 to 4.17.21 in /frontend ✓ dependencies

#1 opened 1 hour ago by dependabot bot

1 **lodash** vulnerability found in **frontend/package-lock.json** 1 hour ago

Remediation

Upgrade **lodash** to version **`4.17.21`** or later. For example:

```
"dependencies": {
  "lodash": ">=4.17.21"
}
```

or...

```
"devDependencies": {
  "lodash": ">=4.17.21"
}
```

Always verify the validity and compatibility of suggestions with your codebase.

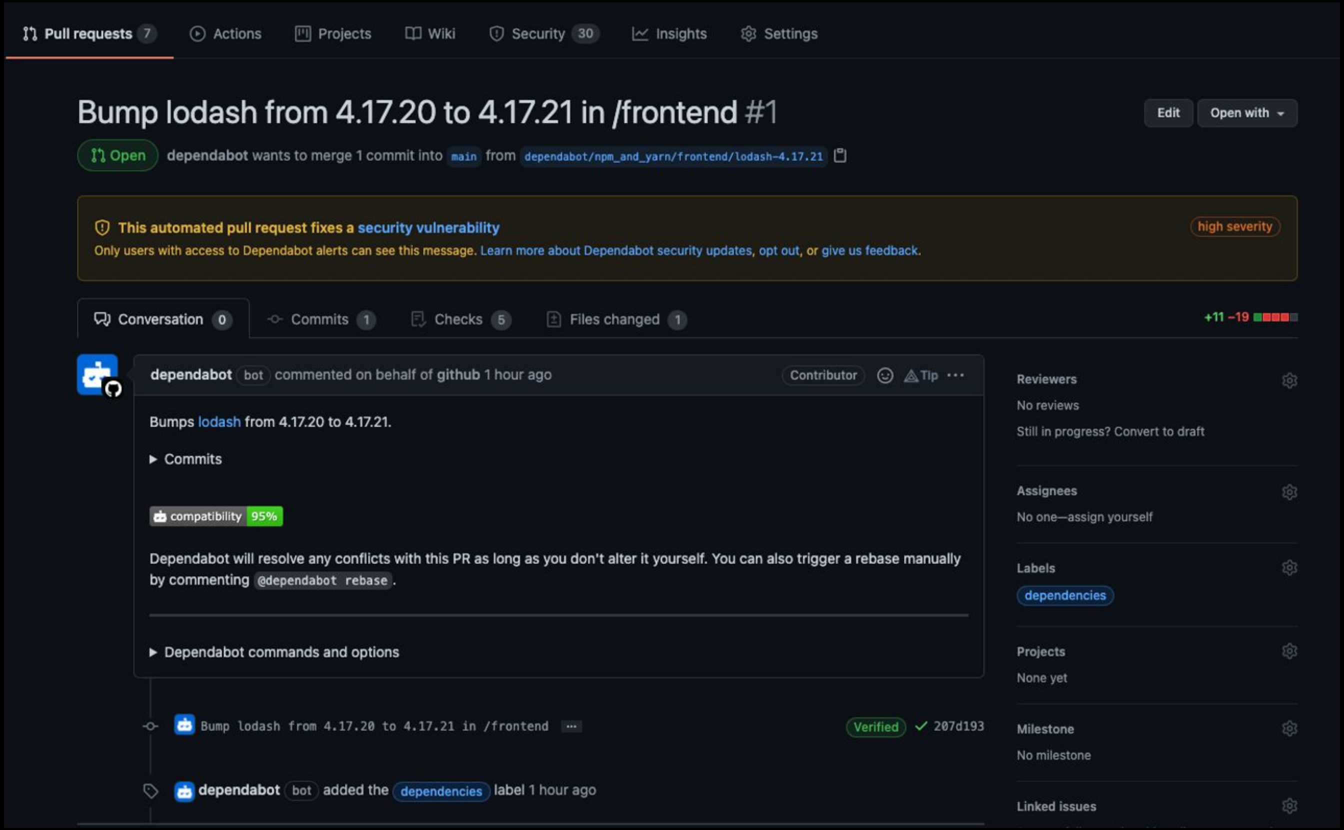
Details

CVE-2021-23337 high severity

Vulnerable versions: `< 4.17.21`
Patched version: `4.17.21`

`lodash` versions prior to 4.17.21 are vulnerable to Command Injection via the template function.

Dependabot - Security Alerts - Pull Request



Bump lodash from 4.17.20 to 4.17.21 in /frontend #1

Open dependabot wants to merge 1 commit into `main` from `dependabot/npm_and_yarn/frontend/lodash-4.17.21`

This automated pull request fixes a security vulnerability high 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 on behalf of **github** 1 hour ago Contributor

Bumps lodash from 4.17.20 to 4.17.21.

▶ Commits

compatibility 95%

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`.

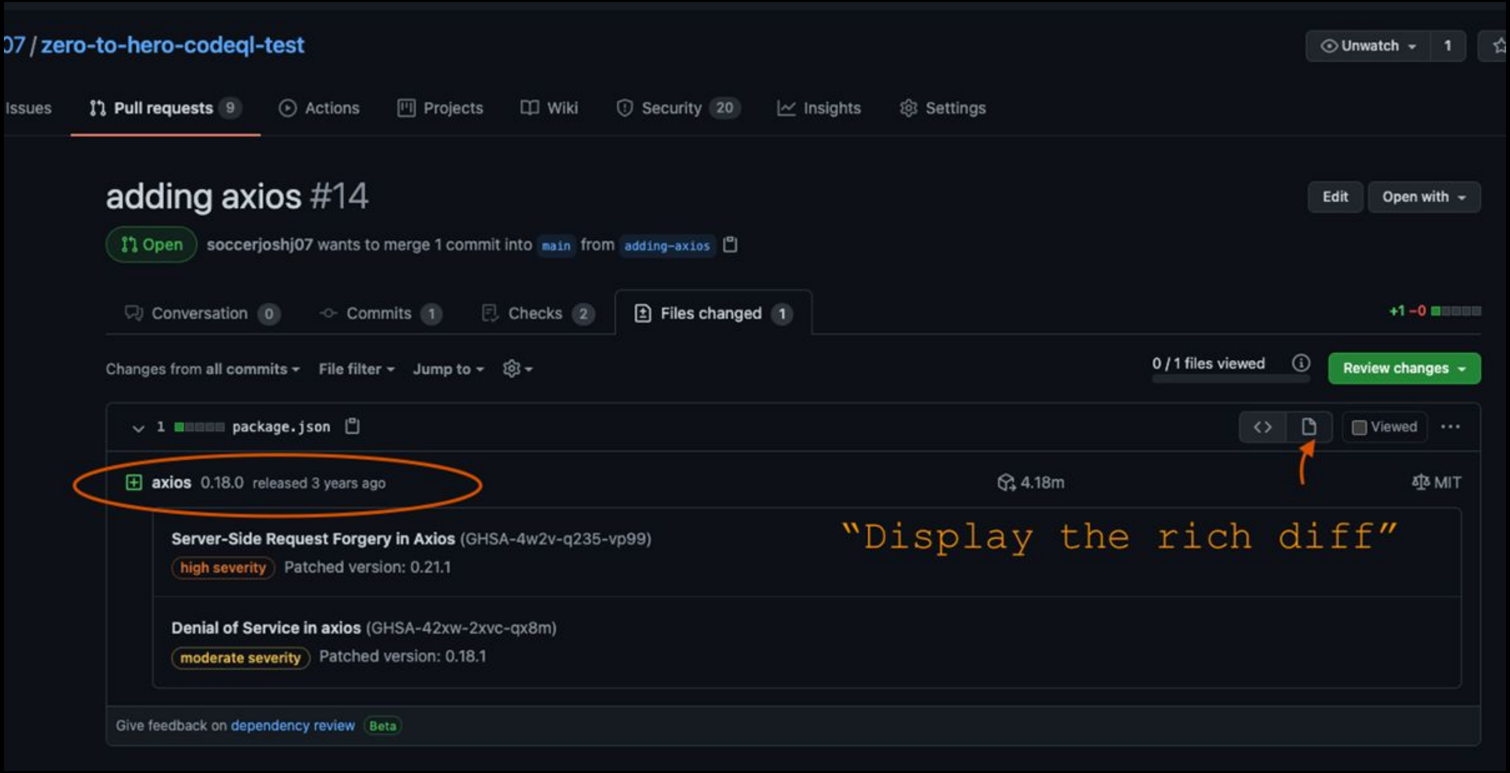
▶ Dependabot commands and options

`Bump lodash from 4.17.20 to 4.17.21 in /frontend` Verified ✓ 207d193

dependabot bot added the dependencies label 1 hour ago

Reviewers	No reviews Still in progress? Convert to draft
Assignees	No one—assign yourself
Labels	dependencies
Projects	None yet
Milestone	No milestone
Linked issues	

Dependabot - Security Alerts - Pull Request



adding axios #14

soccerjoshj07 wants to merge 1 commit into `main` from `adding-axios`

axios 0.18.0 released 3 years ago

"Display the rich diff"

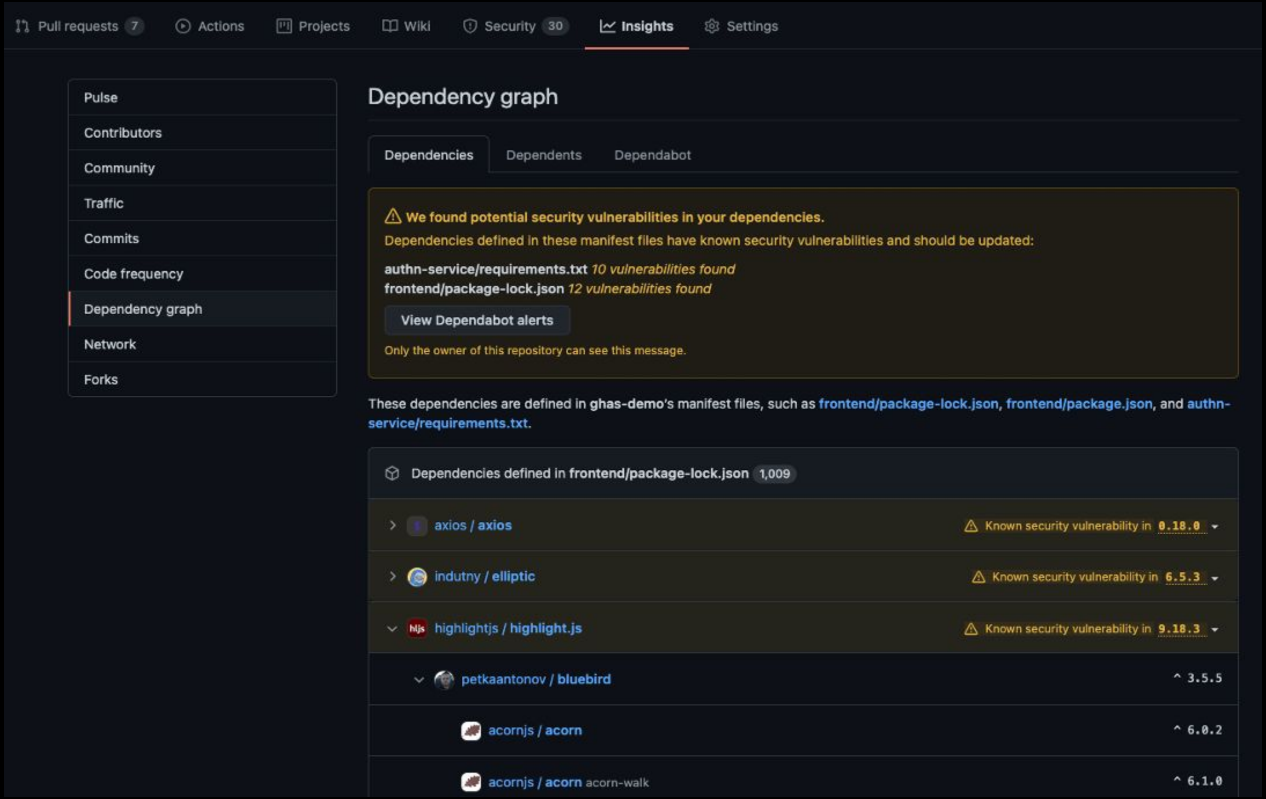
Server-Side Request Forgery in Axios (GHSA-4w2v-q235-vp99)
high severity Patched version: 0.21.1

Denial of Service in axios (GHSA-42xw-2xvc-qx8m)
moderate severity Patched version: 0.18.1

Give feedback on dependency review Beta

Introducing a vulnerable package that the PR catches

Dependabot - Dependency Graph



Dependency graph

We found potential security vulnerabilities in your dependencies.

Dependencies defined in these manifest files have known security vulnerabilities and should be updated:

authn-service/requirements.txt *10 vulnerabilities found*
frontend/package-lock.json *12 vulnerabilities found*

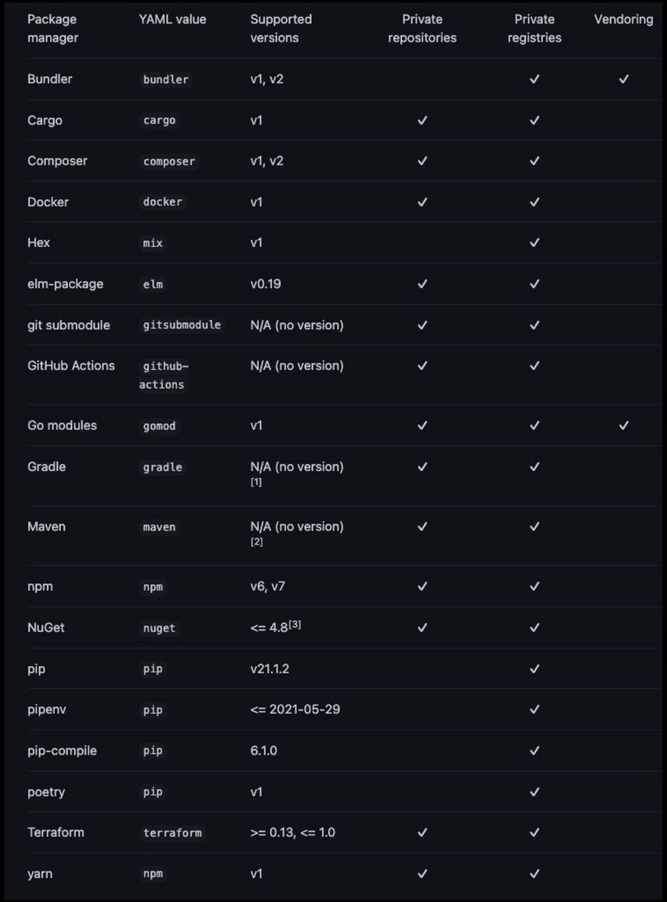
Only the owner of this repository can see this message.

These dependencies are defined in **ghas-demo**'s manifest files, such as frontend/package-lock.json, frontend/package.json, and authn-service/requirements.txt.

Dependencies defined in **frontend/package-lock.json** 1,009

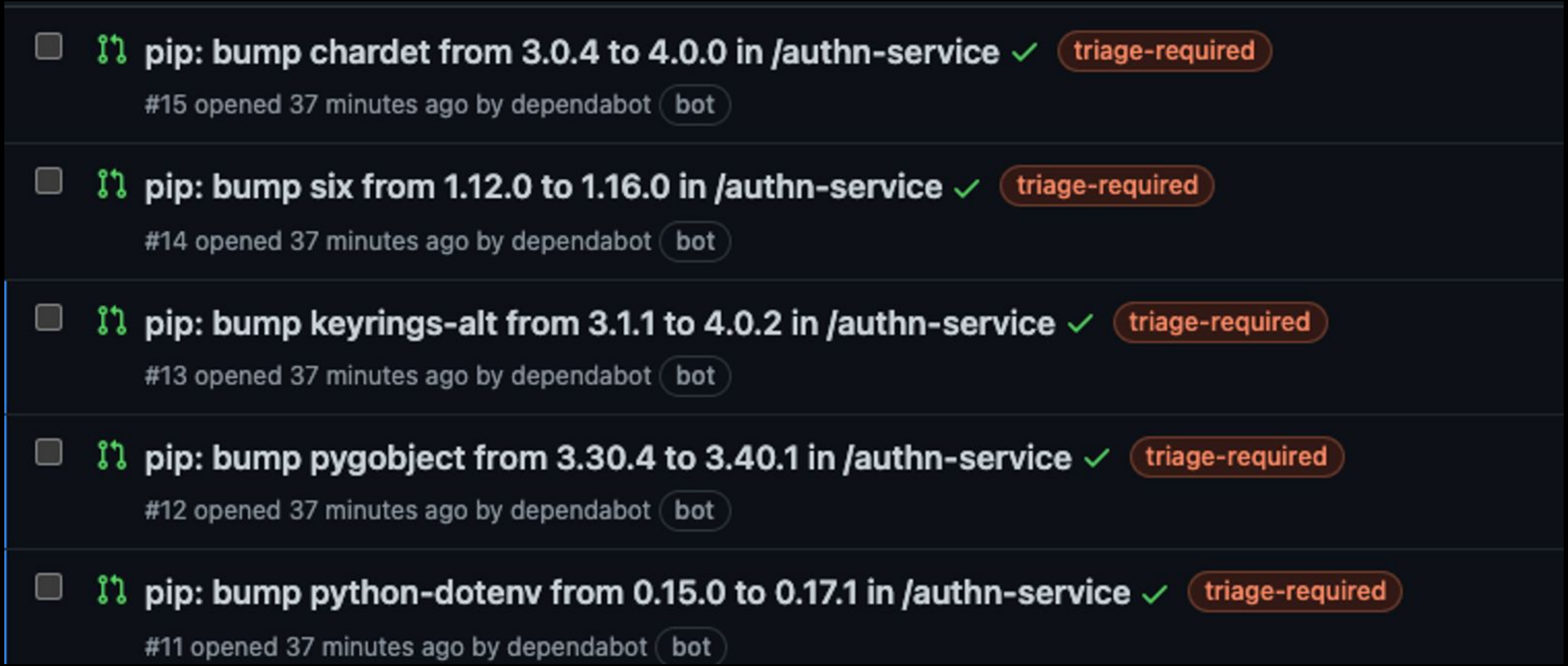
axios / **axios**	Known security vulnerability in `0.18.0`
indutny / **elliptic**	Known security vulnerability in `6.5.3`
highlightjs / **highlight.js**	Known security vulnerability in `9.18.3`
petkaantonov / **bluebird**	`^ 3.5.5`
acornjs / **acorn**	`^ 6.0.2`
acornjs / **acorn** acorn-walk	`^ 6.1.0`

Dependabot - Dependency Updates - Supported Manifests



Package manager	YAML value	Supported versions	Private repositories	Private registries	Vendoring
Bundler	`bundler`	v1, v2		✓	✓
Cargo	`cargo`	v1	✓	✓	
Composer	`composer`	v1, v2	✓	✓	
Docker	`docker`	v1	✓	✓	
Hex	`mix`	v1		✓	
elm-package	`elm`	v0.19	✓	✓	
git submodule	`gitsubmodule`	N/A (no version)	✓	✓	
GitHub Actions	`github-actions`	N/A (no version)	✓	✓	
Go modules	`gomod`	v1	✓	✓	✓
Gradle	`gradle`	N/A (no version) [1]	✓	✓	
Maven	`maven`	N/A (no version) [2]	✓	✓	
npm	`npm`	v6, v7	✓	✓	
NuGet	`nuget`	<= 4.8[3]	✓	✓	
pip	`pip`	v21.1.2		✓	
pipenv	`pip`	<= 2021-05-29		✓	
pip-compile	`pip`	6.1.0		✓	
poetry	`pip`	v1		✓	
Terraform	`terraform`	>= 0.13, <= 1.0	✓	✓	
yarn	`npm`	v1	✓	✓	

Dependabot - Dependency Updates



□ pip: bump chardet from 3.0.4 to 4.0.0 in /authn-service ✓ triage-required
#15 opened 37 minutes ago by dependabot bot

□ pip: bump six from 1.12.0 to 1.16.0 in /authn-service ✓ triage-required
#14 opened 37 minutes ago by dependabot bot

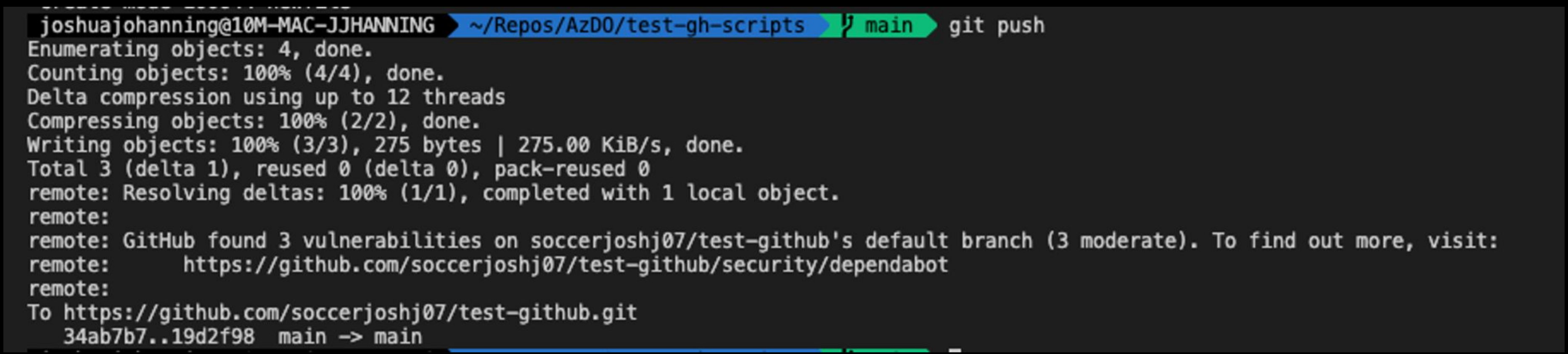
□ pip: bump keyrings-alt from 3.1.1 to 4.0.2 in /authn-service ✓ triage-required
#13 opened 37 minutes ago by dependabot bot

□ pip: bump pygobject from 3.30.4 to 3.40.1 in /authn-service ✓ triage-required
#12 opened 37 minutes ago by dependabot bot

□ pip: bump python-dotenv from 0.15.0 to 0.17.1 in /authn-service ✓ triage-required
#11 opened 37 minutes ago by dependabot bot

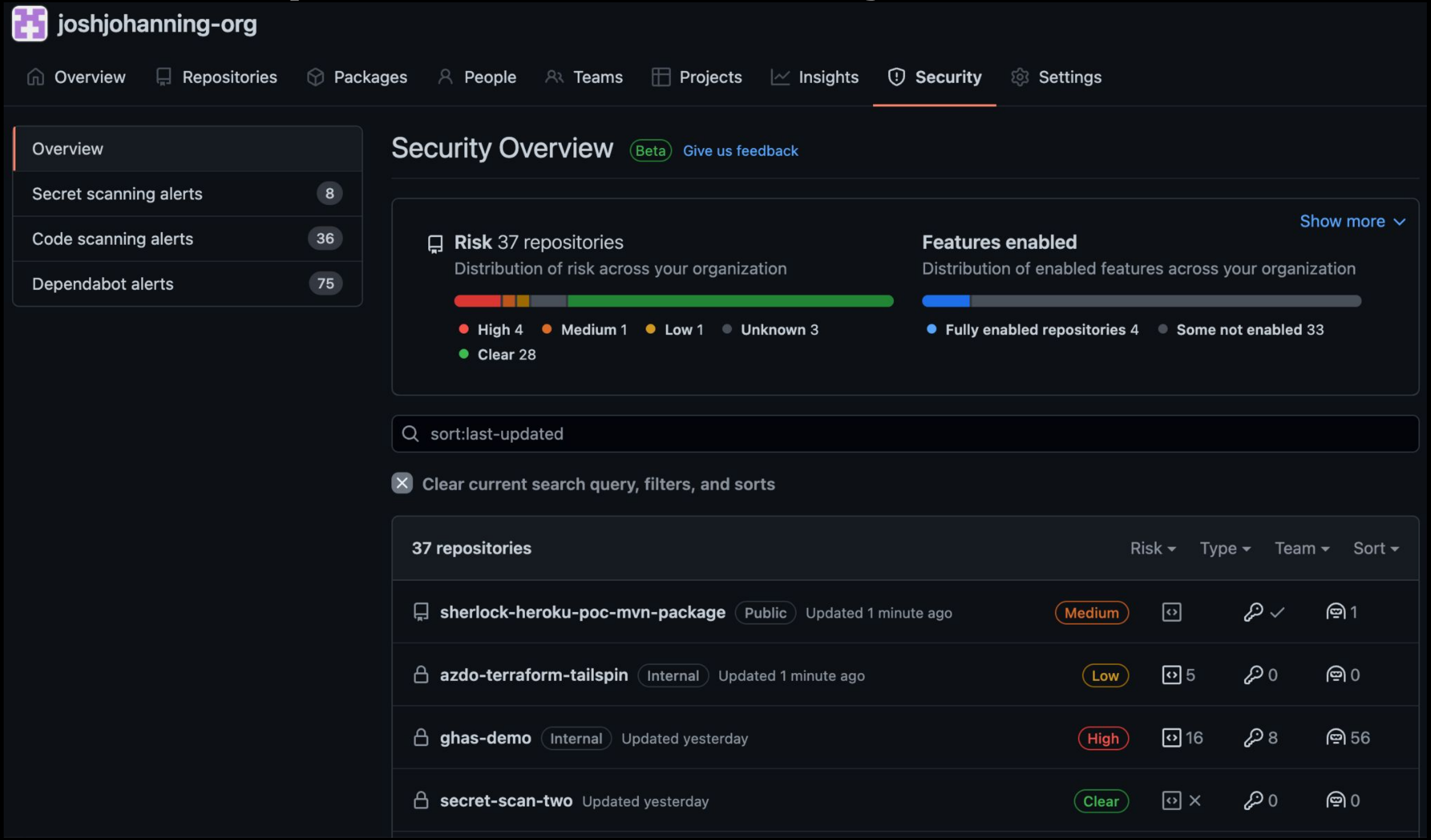
Packages that need to be updated – not necessarily security vulnerabilities

Dependency Vulnerabilities shown in local Git output



```
 joshuajohanning@10M-MAC-JJHANNING  ~/Repos/AzDO/test-gh-scripts  main  git push
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 12 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 275 bytes | 275.00 KiB/s, done.
Total 3 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), completed with 1 local object.
remote:
remote: GitHub found 3 vulnerabilities on soccerjoshj07/test-github's default branch (3 moderate). To find out more, visit:
remote:      https://github.com/soccerjoshj07/test-github/security/dependabot
remote:
To https://github.com/soccerjoshj07/test-github.git
   34ab7b7..19d2f98  main -> main
```

GitHub Enterprise Cloud - Security Overview for the Org



joshjohanning-org

Overview	
Secret scanning alerts	8
Code scanning alerts	36
Dependabot alerts	75

Security Overview

Beta Give us feedback

Show more

Risk 37 repositories

Distribution of risk across your organization

● High 4 ● Medium 1 ● Low 1 ● Unknown 3 ● Clear 28

Features enabled

Distribution of enabled features across your organization

● Fully enabled repositories 4 ● Some not enabled 33

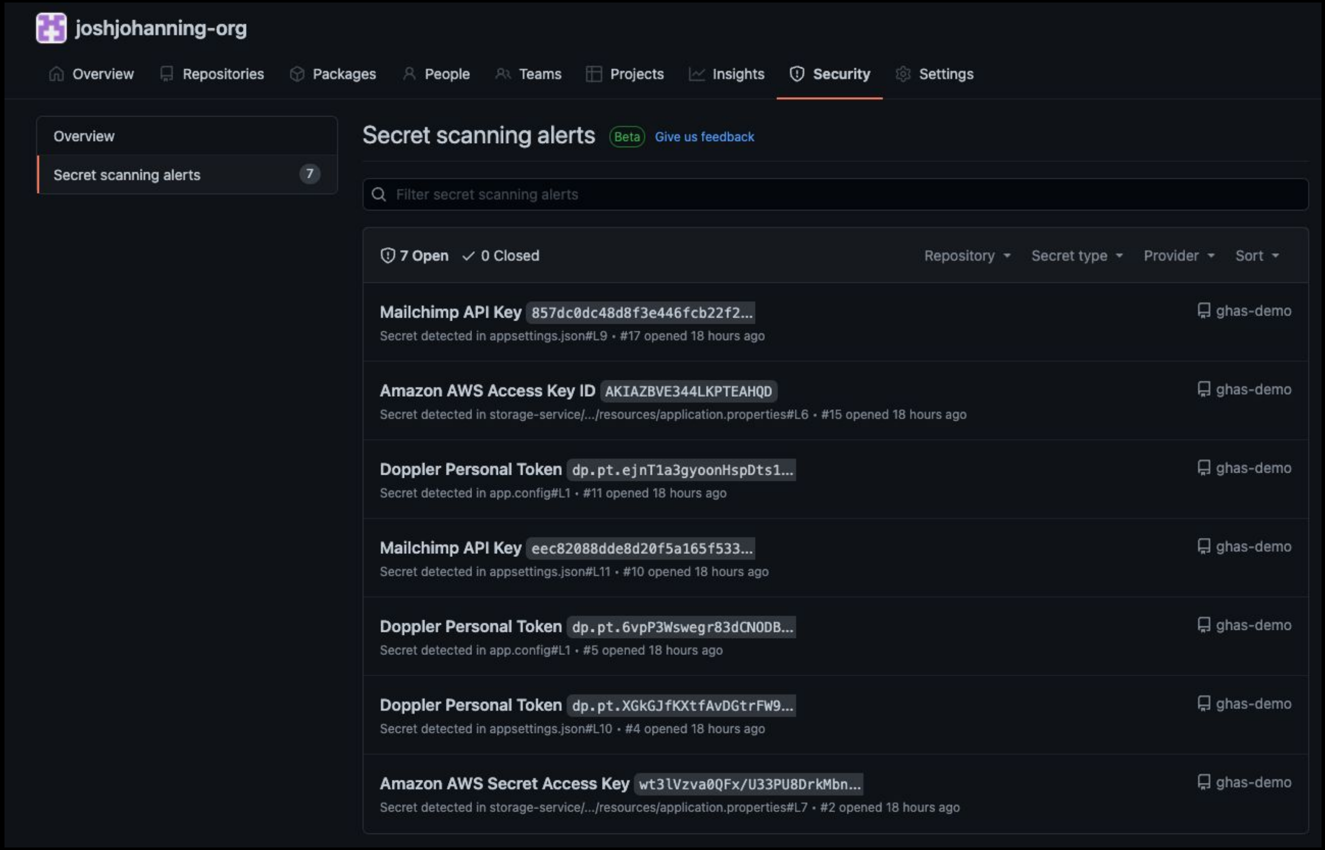
sort:last-updated

☒ Clear current search query, filters, and sorts

37 repositories Risk ▾ Type ▾ Team ▾ Sort ▾

sherlock-heroku-poc-mvn-package Public	Updated 1 minute ago	Medium		✓	1
azdo-terraform-tailspin Internal	Updated 1 minute ago	Low	5	0	0
ghas-demo Internal	Updated yesterday	High	16	8	56
secret-scan-two	Updated yesterday	Clear	×	0	0

GitHub Enterprise Cloud - Security Overview - Secrets



Secret scanning alerts Beta Give us feedback

Filter secret scanning alerts

7 Open ✓ 0 Closed Repository ▾ Secret type ▾ Provider ▾ Sort ▾

Mailchimp API Key `857dc0dc48d8f3e446fcb22f2...` ghas-demo
Secret detected in appsettings.json#L9 • #17 opened 18 hours ago

Amazon AWS Access Key ID `AKIAZBVE344LKPTEAHQD` ghas-demo
Secret detected in storage-service/.../resources/application.properties#L6 • #15 opened 18 hours ago

Doppler Personal Token `dp.pt.ejnT1a3gyoonHspDts1...` ghas-demo
Secret detected in app.config#L1 • #11 opened 18 hours ago

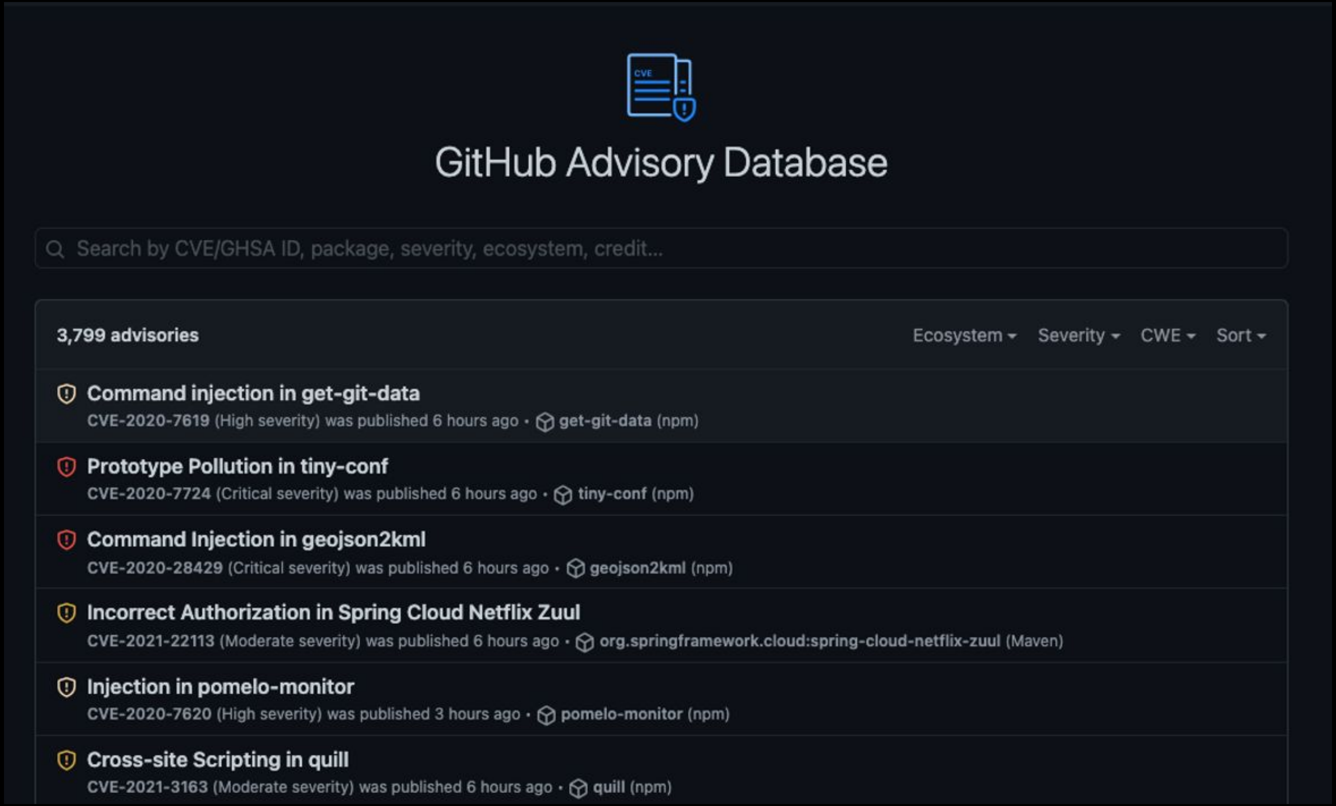
Mailchimp API Key `eec82088dde8d20f5a165f533...` ghas-demo
Secret detected in appsettings.json#L11 • #10 opened 18 hours ago

Doppler Personal Token `dp.pt.6vpP3Wswegr83dCNODB...` ghas-demo
Secret detected in app.config#L1 • #5 opened 18 hours ago

Doppler Personal Token `dp.pt.XGkGJfKXtfAvDGtrFW9...` ghas-demo
Secret detected in appsettings.json#L10 • #4 opened 18 hours ago

Amazon AWS Secret Access Key `wt3lVzva0QFx/U33PU8DrkMbn...` ghas-demo
Secret detected in storage-service/.../resources/application.properties#L7 • #2 opened 18 hours ago

GitHub - Advisory Database



GitHub Advisory Database

Search by CVE/GHSA ID, package, severity, ecosystem, credit...

3,799 advisories

Ecosystem
Severity
CWE
Sort

Command injection in get-git-data
CVE-2020-7619 (High severity) was published 6 hours ago · get-git-data (npm)

Prototype Pollution in tiny-conf
CVE-2020-7724 (Critical severity) was published 6 hours ago · tiny-conf (npm)

Command Injection in geojson2kml
CVE-2020-28429 (Critical severity) was published 6 hours ago · geojson2kml (npm)

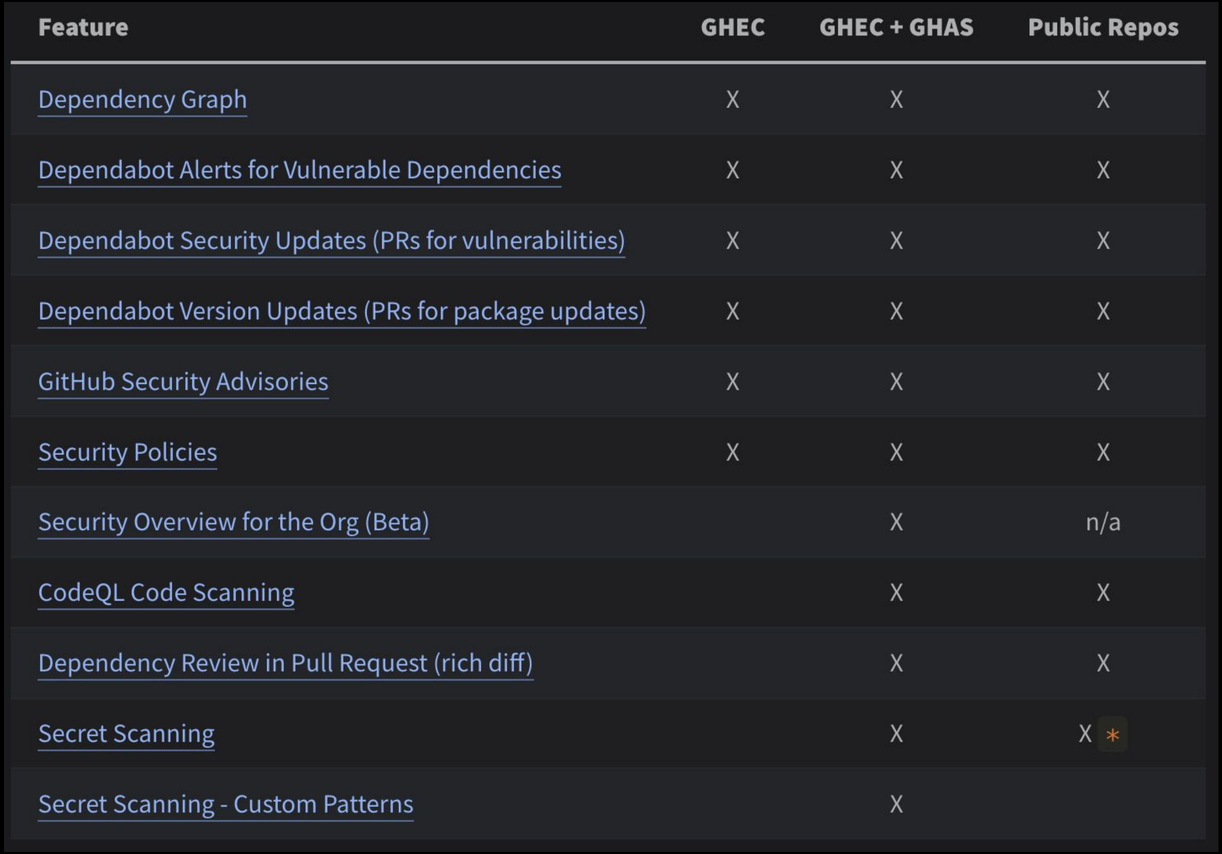
Incorrect Authorization in Spring Cloud Netflix Zuul
CVE-2021-22113 (Moderate severity) was published 6 hours ago · org.springframework.cloud:spring-cloud-netflix-zuul (Maven)

Injection in pomelo-monitor
CVE-2020-7620 (High severity) was published 3 hours ago · pomelo-monitor (npm)

Cross-site Scripting in quill
CVE-2021-3163 (Moderate severity) was published 6 hours ago · quill (npm)

https://github.com/advisories

GHAS - License/Feature Comparison



Feature	GHEC	GHEC + GHAS	Public Repos
Dependency Graph	X	X	X
Dependabot Alerts for Vulnerable Dependencies	X	X	X
Dependabot Security Updates (PRs for vulnerabilities)	X	X	X
Dependabot Version Updates (PRs for package updates)	X	X	X
GitHub Security Advisories	X	X	X
Security Policies	X	X	X
Security Overview for the Org (Beta)		X	n/a
CodeQL Code Scanning		X	X
Dependency Review in Pull Request (rich diff)		X	X
Secret Scanning		X	X *
Secret Scanning - Custom Patterns		X	

https://josh-ops.com/posts/github-advanced-security-feature-chart/

Questions?