



 Universe2020

# Catching vulnerabilities early with GitHub

**William Bartholomew**

Staff Product Manager, GitHub

**Maya Kaczorowski**

Sr Director Product Manager, GitHub

# Agenda

## Dependencies

Software supply chain security

Risks from dependencies

## Dependency management with GitHub

Dependency Graph

Dependabot

## New: Dependency review

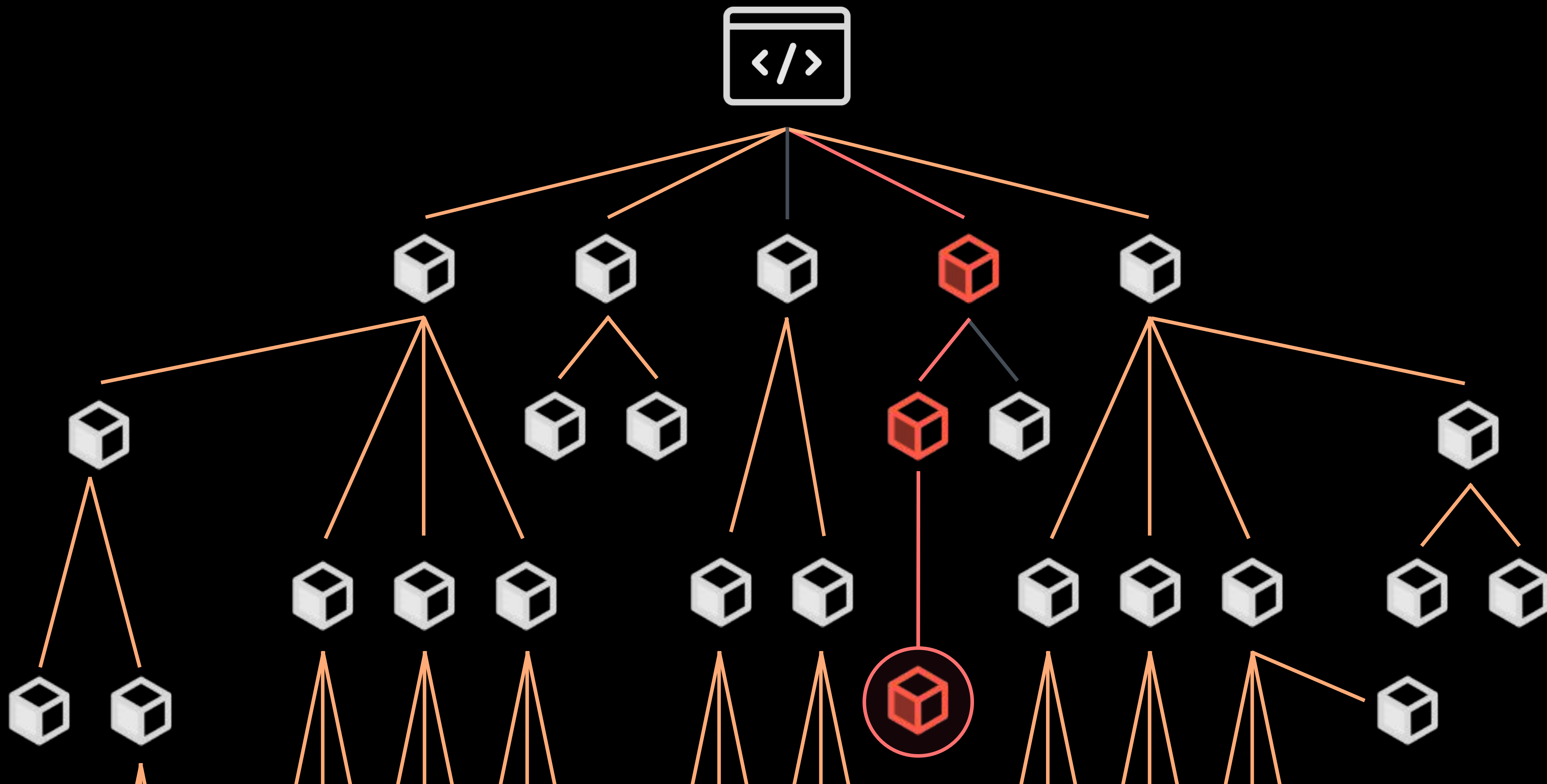
Introducing dependency review

How dependency review works

How GitHub helps you shift left

# Dependencies and your software supply chain





**A **dependency** is another binary that your software needs in order to run**

**A **dependency** is another binary that your software needs in order to run**

Author

Date of  
contribution

Date of  
publication

Security reviews

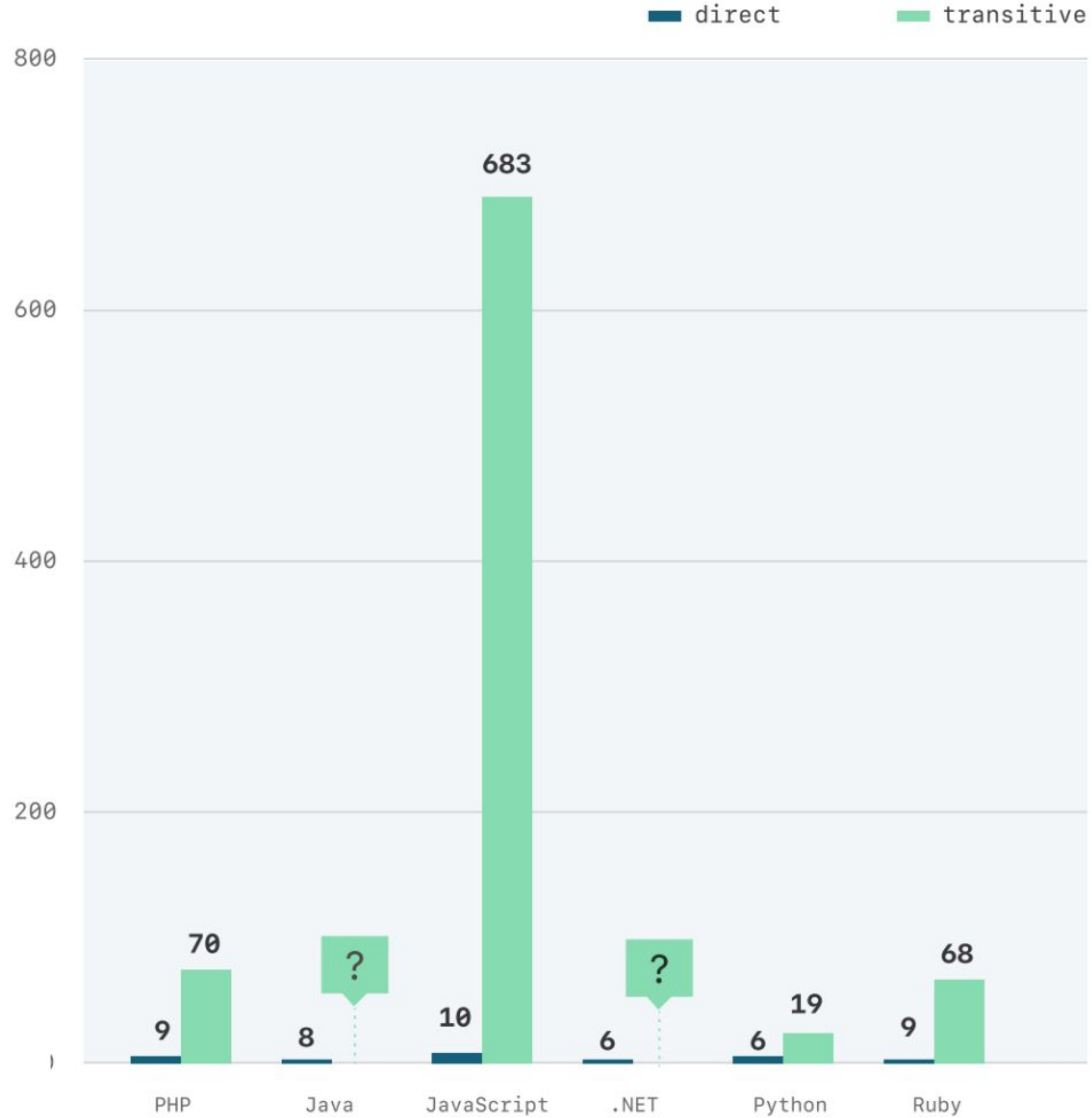
Known  
vulnerabilities

Supported  
versions

License  
information

etc.

Median direct and transitive dependencies  
per repository by package ecosystem



**Software  
dependencies are  
pervasive**



# Dependency management with GitHub

# Dependency management with GitHub



## Know your environment

### Dependency graph

Understand your project's dependencies

## Manage your dependencies

### Dependabot alerts

Be notified of a vulnerability in a dependency

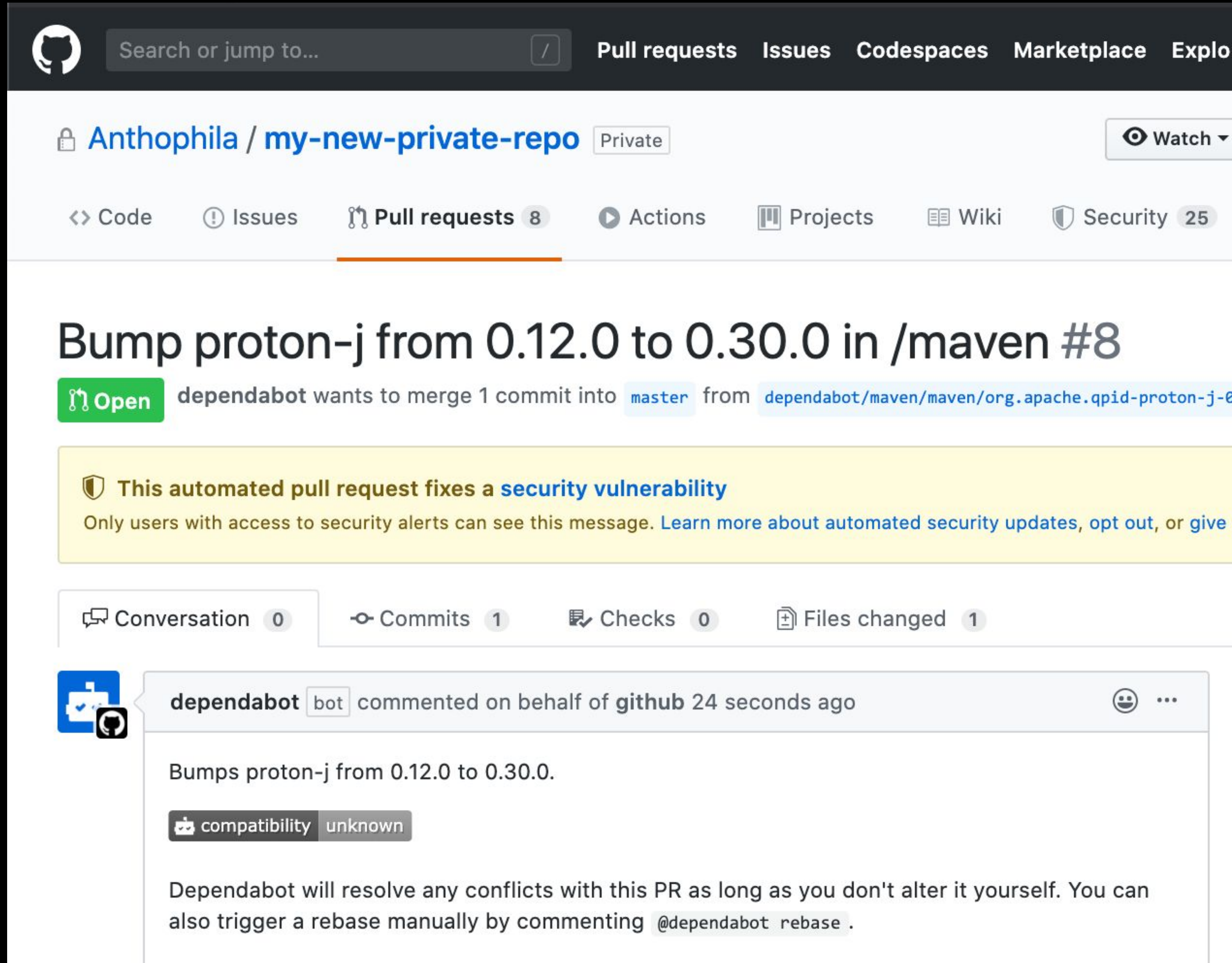
### Dependabot security updates

Review a PR to update to the minimum fixed version

### Dependabot version updates

Review a PR to update to the latest stable dependency version

# Fixing vulnerabilities is as simple as merging a PR



The screenshot shows a GitHub interface for a pull request in a repository named 'my-new-private-repo' by user 'Anthophila'. The pull request is titled 'Bump proton-j from 0.12.0 to 0.30.0 in /maven #8' and is from the 'dependabot/maven/maven/org.apache.qpid-proton-j-0' branch. A green 'Open' button is visible. A yellow banner states: 'This automated pull request fixes a security vulnerability. Only users with access to security alerts can see this message. Learn more about automated security updates, opt out, or give feedback.' Below this, a summary bar shows 'Conversation 0', 'Commits 1', 'Checks 0', and 'Files changed 1'. A comment from 'dependabot bot' (commented 24 seconds ago) reads: 'Bumps proton-j from 0.12.0 to 0.30.0. 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.'

Search or jump to... / Pull requests Issues Codespaces Marketplace Explo

Anthophila / my-new-private-repo Private Watch

Code Issues Pull requests 8 Actions Projects Wiki Security 25

## Bump proton-j from 0.12.0 to 0.30.0 in /maven #8

Open dependabot wants to merge 1 commit into master from dependabot/maven/maven/org.apache.qpid-proton-j-0

**This automated pull request fixes a security vulnerability**  
Only users with access to security alerts can see this message. [Learn more about automated security updates, opt out, or give feedback](#)

Conversation 0 Commits 1 Checks 0 Files changed 1

dependabot bot commented on behalf of github 24 seconds ago

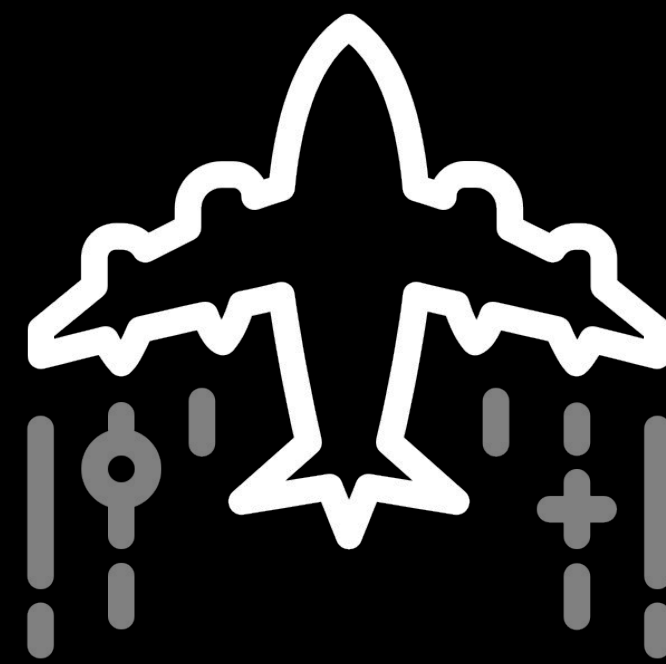
Bumps proton-j from 0.12.0 to 0.30.0.

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 .

# 1.4x

**faster to apply a patch  
when an automatic pull request is generated**



# Shift left

to catch security issues earlier





# New Dependency review

# Dependency review

- Understand and review dependency changes in pull requests
- Catch additions and changes of vulnerable or out of date dependencies
- Avoid “after the fact” alerts and remediation

The screenshot shows a GitHub pull request titled "Catalyzer fix #01" by user kaylee.frye. The pull request is open and shows 1 commit being merged into the "serenity-main" branch from the "repair-parts" branch. The interface includes navigation tabs for Code, Issues (1), Pull requests (1), Actions, Projects, Wiki, and Settings. Below the title, there are tabs for Conversation (0), Commits (2), Checks (1), and Files changed (1). The "Files changed" tab is selected, showing a list of changes in "client/package-lock.json". The list includes several dependencies with their versions and release dates. A security alert is visible for "jsonwebtoken" 4.1.1, indicating a "Verification Bypass in jsonwebtoken (CVE-2015-9235)" with "critical severity" and noting it was "Patched in version 4.2.2". Other dependencies listed include "acorn" 6.4.0, "express" 4.13.4, "express-jwt" 3.3.0, and "express-session" 1.13.0.

firefly / serenity Private

<> Code Issues 1 Pull requests 1 Actions Projects Wiki Settings

## Catalyzer fix #01

Open kaylee.frye wants to merge 1 commit into serenity-main from repair-parts

Conversation 0 Commits 2 Checks 1 Files changed 1

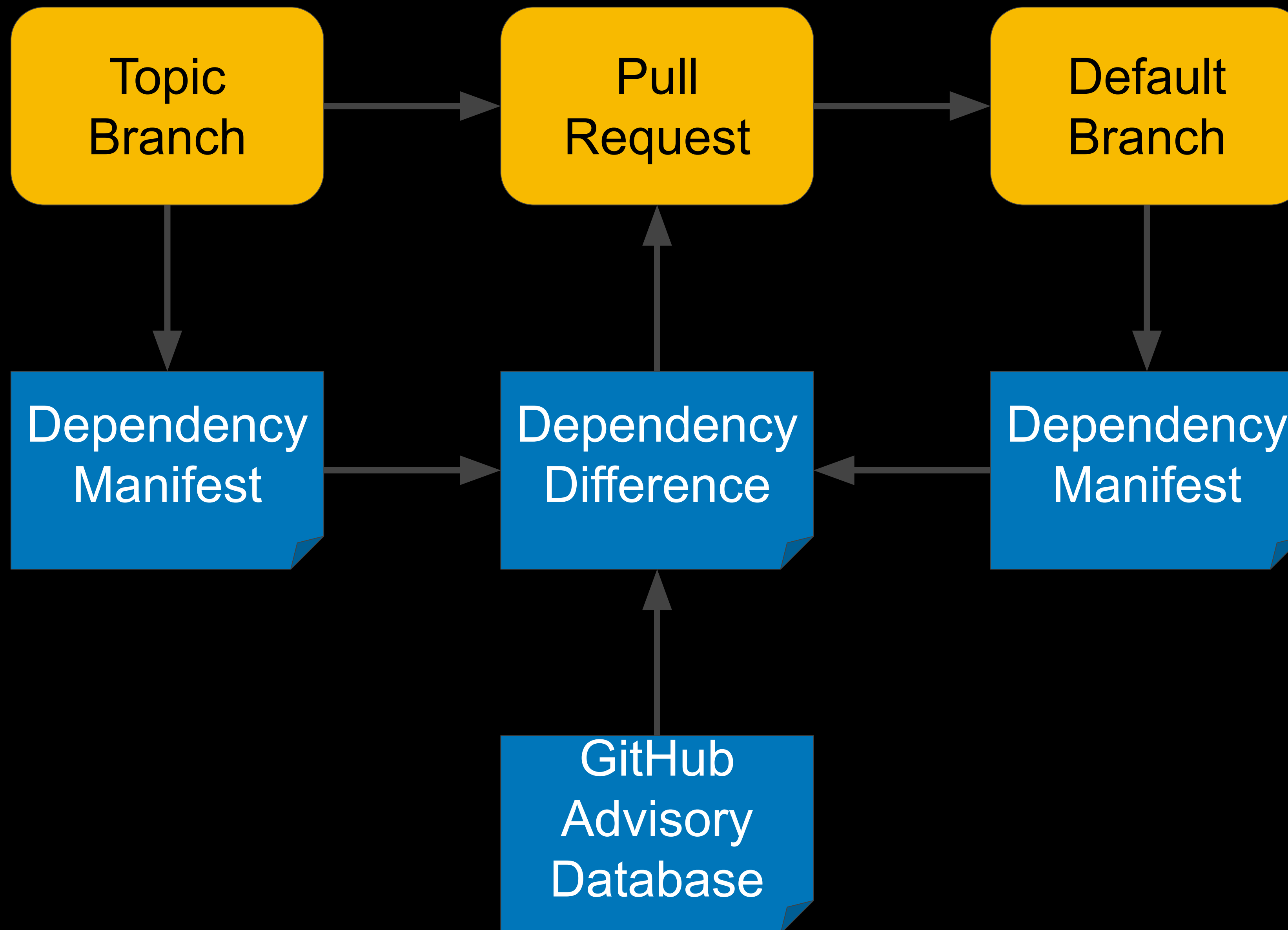
Changes from all commits File filter... Clear filters Jump to... Settings

5 client/package-lock.json

- jsonwebtoken 4.1.1 released 2 years ago
  - Verification Bypass in jsonwebtoken (CVE-2015-9235)
    - critical severity Patched in version 4.2.2
- acorn 6.4.0 released 5 months ago
- express 4.13.4 released 8 months ago
- express-jwt 3.3.0 released 8 months ago
- express-session 1.13.0 released 7 months ago, child of express 4.13.4



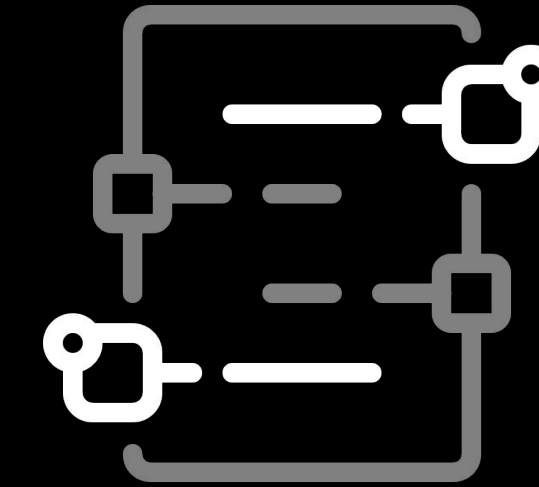
Demo





## Dependabot alerts

- Notifies you **after** you have made a change to a manifest file
- Also notifies you of **new vulnerabilities** in existing dependencies



## Dependency review

- Lets you “shift left” and catch vulnerable dependencies **before** they are introduced
- Provides **information** on license, dependents, and age of dependencies

**... you still need both!**



# Other ways to shift security left with GitHub



## **Code scanning**

Find vulnerabilities in custom code using static analysis

## **Dependabot version updates**

Update dependencies to the latest stable versions


## **Actions**

Automate all your software development workflows

## **Protected branches**




Enforce restrictions on how code branches are merged

# Now available...



Search or jump to...

[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)

firefly / serenity Private

[Watch](#) 4 [Star](#) 4 [Fork](#) 4

[Code](#) [Issues](#) 1 [Pull requests](#) 1 [Actions](#) [Projects](#) [Wiki](#) [Security](#) [Insights](#) [Settings](#)

Catalyzer fix #01

[Edit](#) [Open with](#)

[Open](#) kaylee.frye wants to merge 1 commit into serenity-main from repair-parts

[Conversation](#) 0 [Commits](#) 2 [Checks](#) 1 [Files changed](#) 1

Changes from all commits

File filter...

Clear filters

Jump to...

0 / 1 files viewed

Review changes

5 client/package-lock.json

jsonwebtoken 4.1.1 released 2 years ago

Verification Bypass in jsonwebtoken (CVE-2015-9235)  
critical severity Patched in version 4.2.2

acorn 6.4.0 released 5 months ago

5.9m Apache

express 4.13.4 released 8 months ago



8m MIT



express-jwt 3.3.0 released 8 months ago

69k MIT

express-session 1.13.0 released 7 months ago, child of express 4.13.4

568k MIT

# Learn more

Dependency review:

<https://github.co/dependency-review>

Enable supply chain security features:

<https://github.co/dependency-graph>

<https://github.co/security-alerts>

<https://github.co/security-updates>

