Navigating Dependency Abandonment

Bogdan Vasilescu

Courtney Miller

Christian Kästner

August 3, 2024
FOSSY 2024, Portland, OR

Carnegie Mellon University

STRUDEL
SOCIO-TECHNICAL RESEARCH USING DATA EXCAVATION LAB

S3D

About me

@b_vasilescu

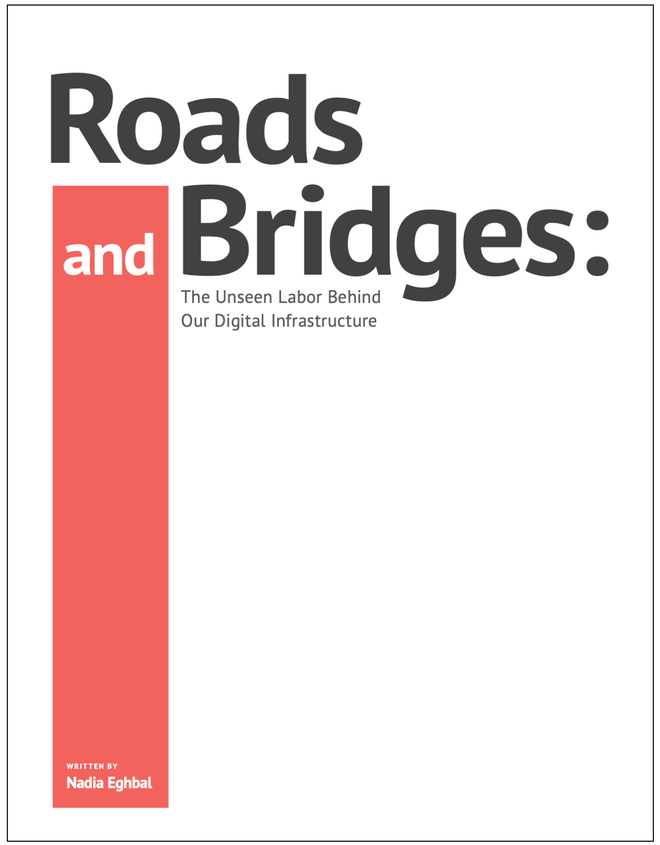
Associate Professor @CMU

Director of the Societal Computing PhD program

STRUDEL research group

Dark chocolate apple strudel, Poushe, Zurich, 2024

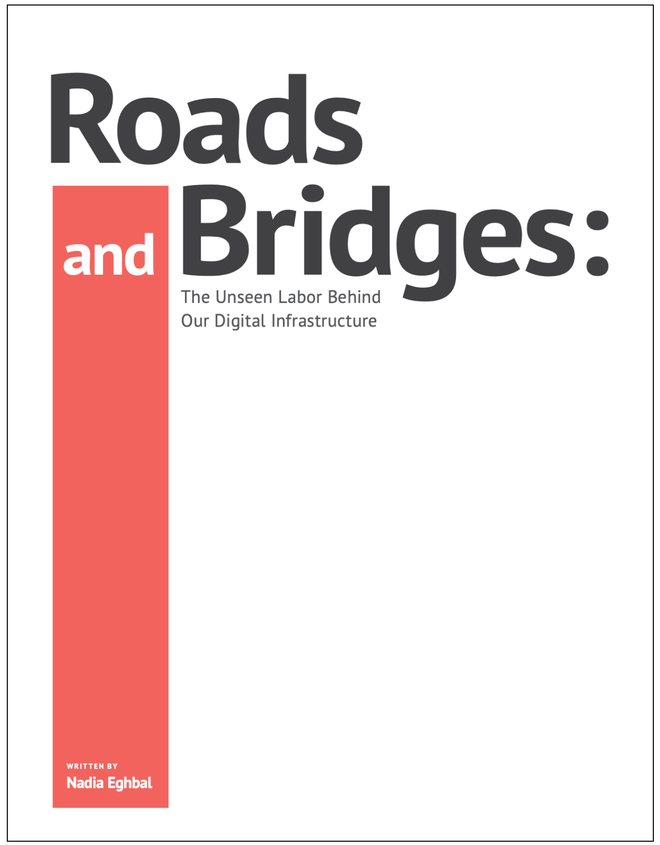
Open source software has become digital infrastructure



Everybody uses open source:

- Fortune 500 companies
- Major software companies
- Startups
- Government
- …

Like any infrastructure, it needs regular upkeep and maintenance

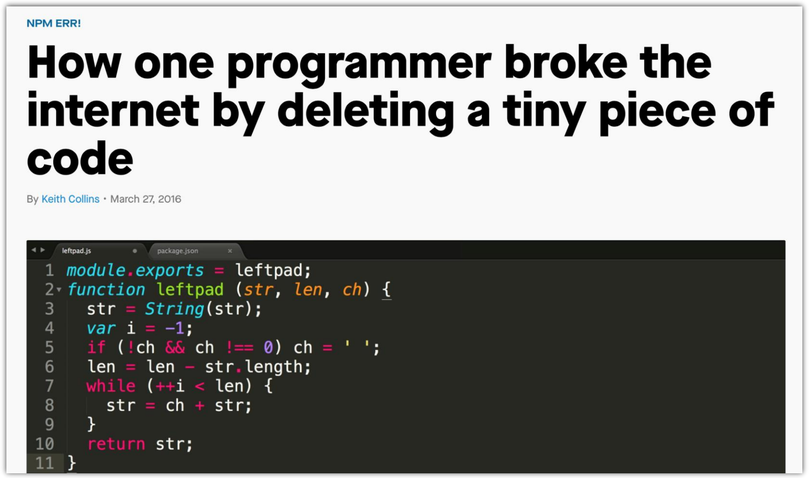


Everybody uses open source:

- Fortune 500 companies
- Major software companies
- Startups
- Government
- …

If undermaintained:

- Brittle supply chains
- Risks for downstream users
- Slows down innovation
- …



https://qz.com/646467/how-one-programmer-broke-the-internet-by-deleting-a-tiny-piece-of-code/

Open-source sustainability research has focused on keeping projects and ecosystems alive and maintained.

STRUDEL sustainability research on …

Project practices

- CHASE 2023 (social media)
- ICSE 2020 (forking)
- ESEC/FSE 2019 (forking)
- ESEC/FSE 2018 (abandonment factors)

Funding models

- ICSE 2020 (donations)

Sunsetting

- ESEC/FSE 2023
- **ICSE 2025** (dealing with abandonment)

Attracting contributors

- ICSE 2022 (Twitter)
- MSR 2020 (Twitter)
- CSCW 2019 (signals)
- ESEC/FSE 2015 (social connections)

Transparency and signaling

- ESEC/FSE 2020 (diffusion of practices)
- CSCW 2019 (signals)
- ICSE 2018 (badges)

Stress, burnout, disengagement

- ICSE 2022 (toxicity theory)
- ICSE SEIS 2022 (toxicity vs pushback)
- ICSE NIER 2020 (toxic language)
- ICSE 2019 (overwork)
- OSS 2019 (dropout, survival analysis)

Diversity and inclusion

- CHI 2023 (ClimateCoach)
- ICSE SEIS 2023 (census)
- ICSE 2019 (social capital)
- CHI 2015 (gender & tenure)
- CHASE 2015 (survey)

Novelty and innovation

- ICSE 2024 (atypical combinations)

Network effects

- ICSE 2024 (innovation)
- ESEC/FSE 2023 (labor pools)
- ICSE 2022 (Twitter)
- ESEC/FSE 2020 (diffusion of practices)
- ICSE 2019 (social capital)
- ESEC/FSE 2018 (abandonment factors)

Maintainers often leave projects for reasons we can't / shouldn’t prevent:

switching jobs (voluntarily), starting a family, losing interest, …

Often nobody steps up when maintainers disengage.

More research should focus on helping open-source maintainers with sunsetting, and helping open-source users with the effects of that.

Today

How big is the problem? What do people do to prepare / deal with it?

- Interviews with maintainers of Javascript, Python, and PHP projects with abandoned upstream dependencies.
- A large-scale quantitative study of abandoned npm packages.

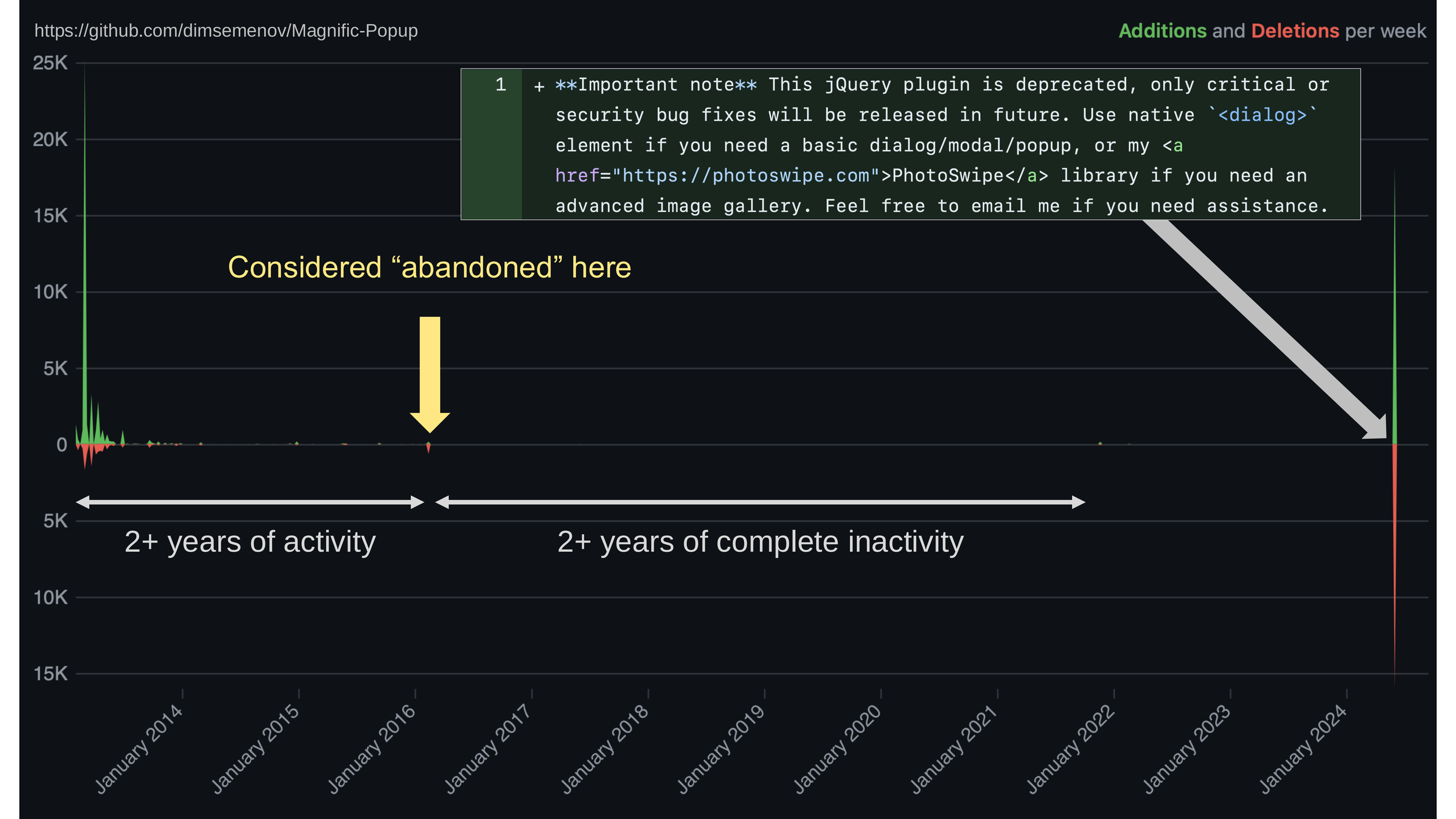
C. Miller, C. Kästner, and B. Vasilescu. **“We feel like we’re winging it:” A study on navigating open-source dependency abandonment**. In International Conference on the Foundations of Software Engineering (FSE), page 1281–1293. ACM, 2023.

C. Miller, M. Jahanshahi, A. Mockus, B. Vasilescu, and C. Kästner. **Understanding the Response to Open-Source Dependency Abandonment in the npm Ecosystem**. In International Conference on Software Engineering (ICSE). IEEE, 2025.

Part 1: Interviews

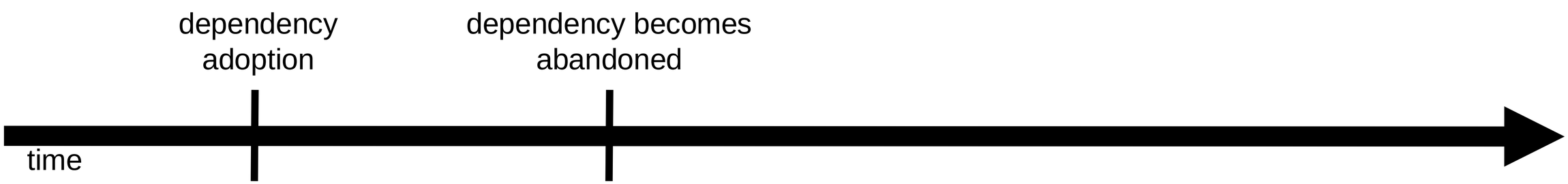

https://github.com/dimsemenov/Magnific-Popup
Additions and Deletions per week
25K
20K
15K
10K
5K
0
5K
10K
15K
January 2014
January 2015
January 2016
January 2017
January 2018
January 2019
January 2020
January 2021
January 2022
January 2023
January 2024


https://github.com/dimsemenov/Magnific-Popup
Additions and Deletions per week
25K
20K
15K
10K
5K
0
5K
10K
15K
Considered “abandoned” here
2+ years of activity
2+ years of complete inactivity
January 2014
January 2015
January 2016
January 2017
January 2018
January 2019
January 2020
January 2021
January 2022
January 2023
January 2024

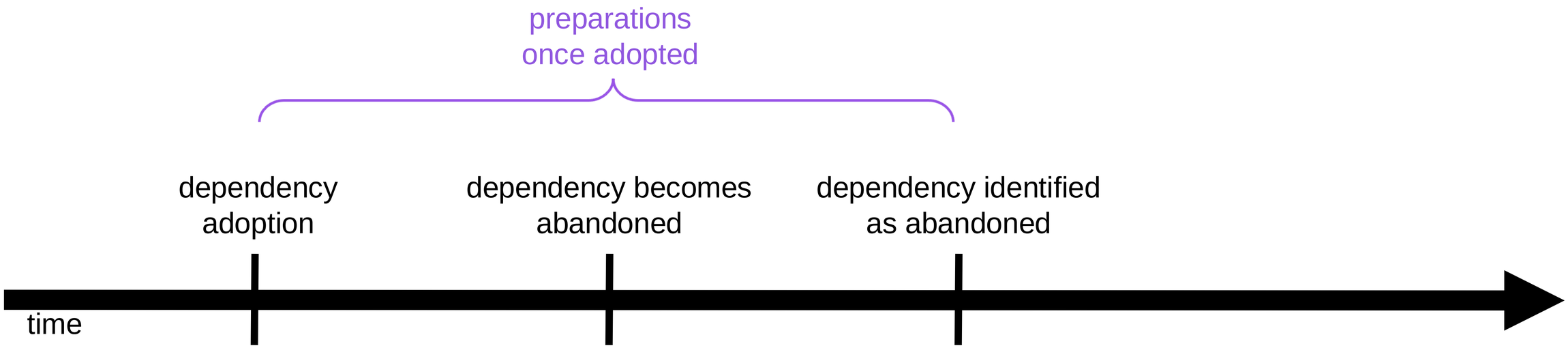

https://github.com/dimsemenov/Magnific-Popup
Additions and Deletions per week
1 + **Important note** This jQuery plugin is deprecated, only critical or security bug fixes will be released in future. Use native `<dialog>` element if you need a basic dialog/modal/popup, or my PhotoSwipe library if you need an advanced image gallery. Feel free to email me if you need assistance.
Considered “abandoned” here
25K
20K
15K
10K
5K
0
5K
10K
15K
2+ years of activity
2+ years of complete inactivity
January 2014
January 2015
January 2016
January 2017
January 2018
January 2019
January 2020
January 2021
January 2022
January 2023
January 2024

Timeline from the perspective of a consumer

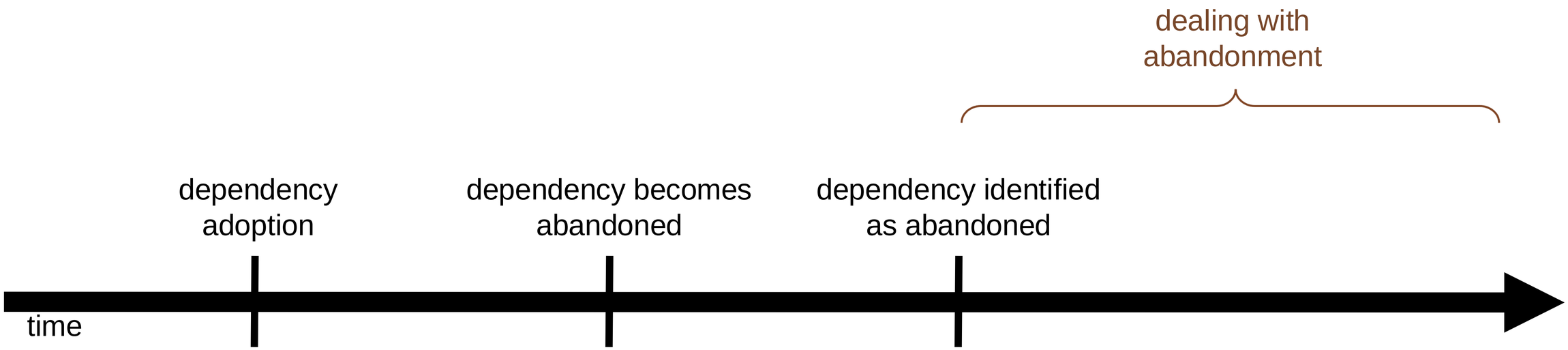
Timeline from the perspective of a consumer



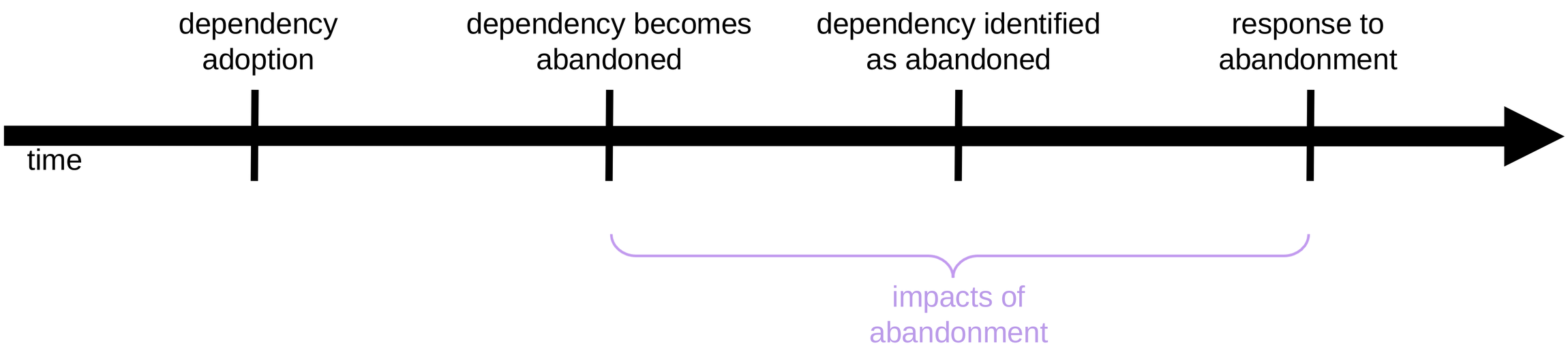
Timeline from the perspective of a consumer



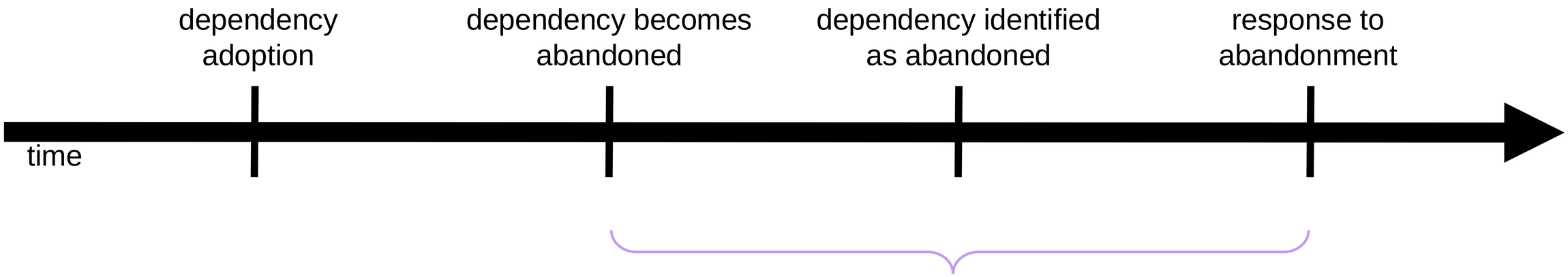
Timeline from the perspective of a consumer



Timeline from the perspective of a consumer

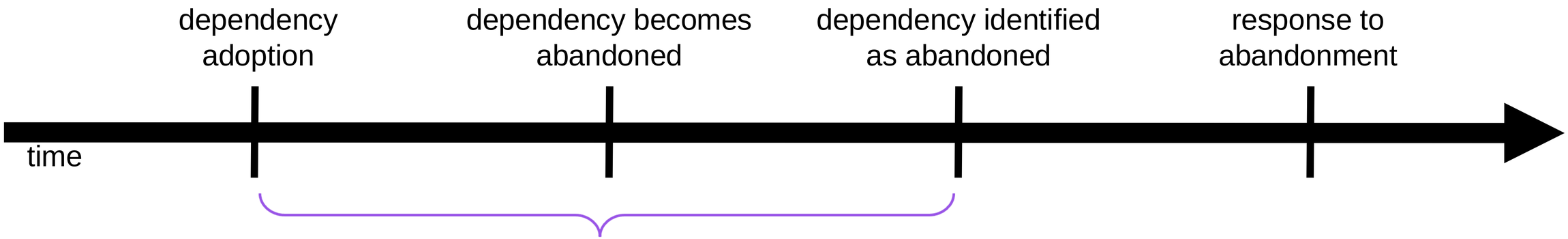


Impacts of abandonment are debated

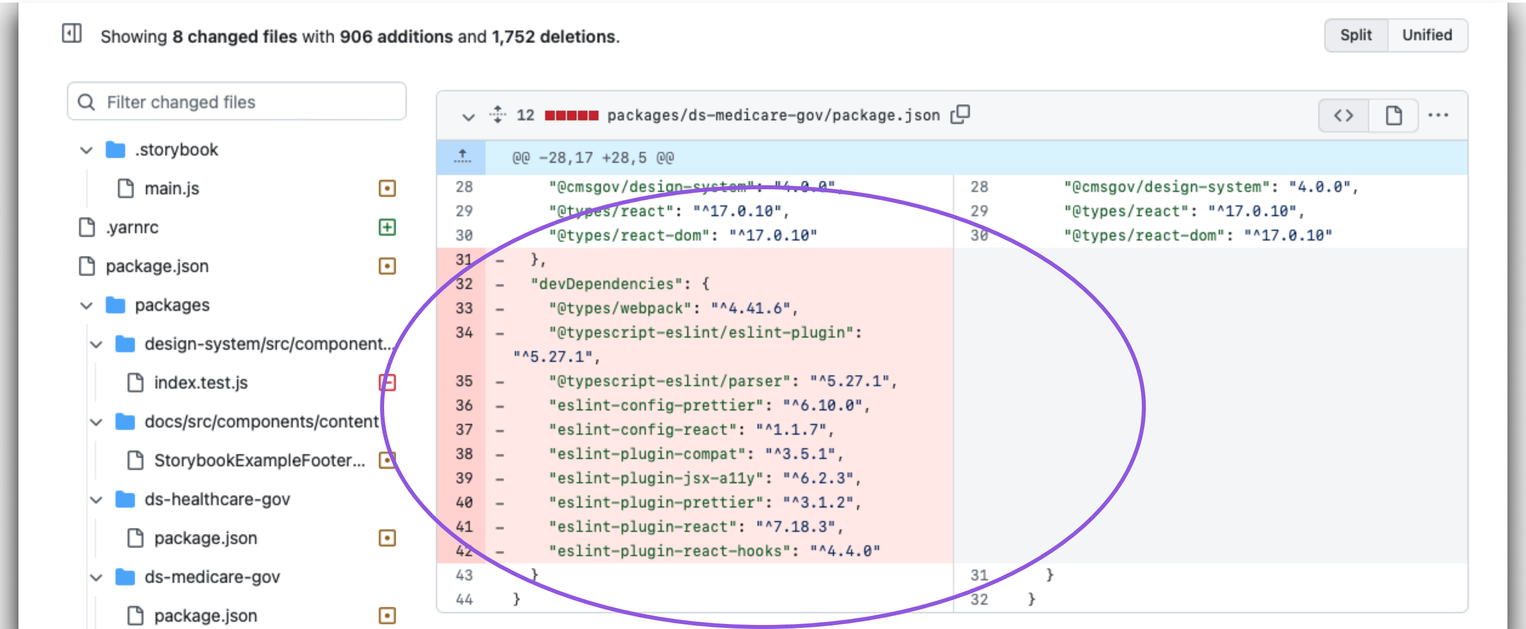


- Some concrete, e.g., language incompatibilities (Python 2 to 3), missing needed features
- Many more anticipated, e.g., future updates, security concerns
- Some expect no meaningful impact

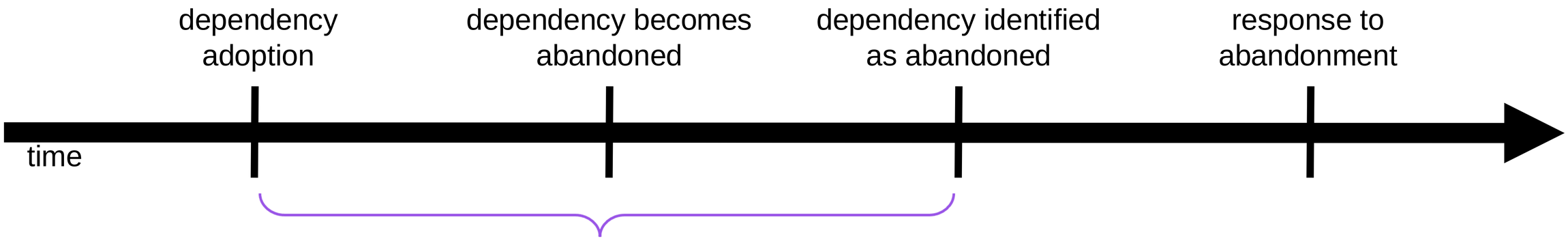
Preparations post-adoption seem rare



E.g., building abstraction layers, minimizing dependencies, monitoring



Preparations post-adoption seem rare



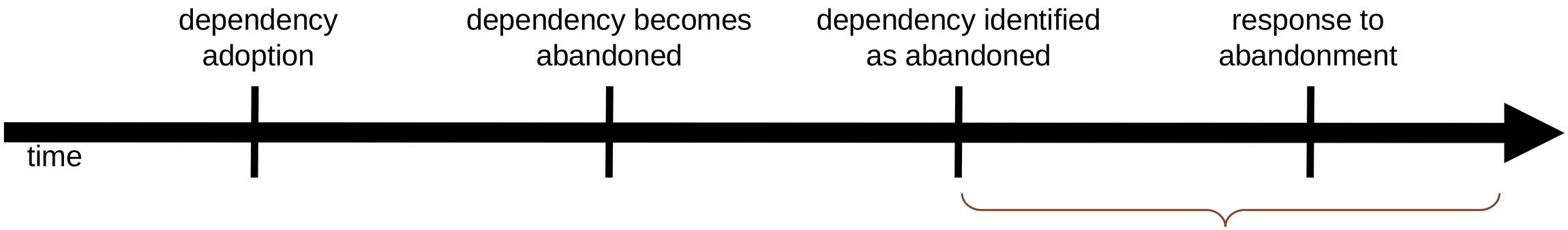
Not all interviewees considered prep worth the effort

We are basically employing the strategy of

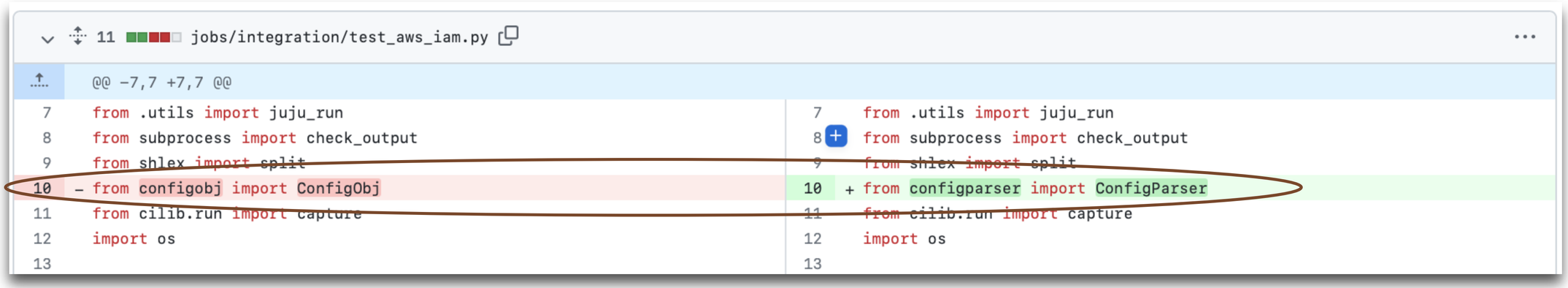
‘if it works it works, if it breaks then I’ll fix the issues.’

- PID10

The most common way to deal with abandonment is to switch to an alternative dependency



Another common solution was to fork or vendor code



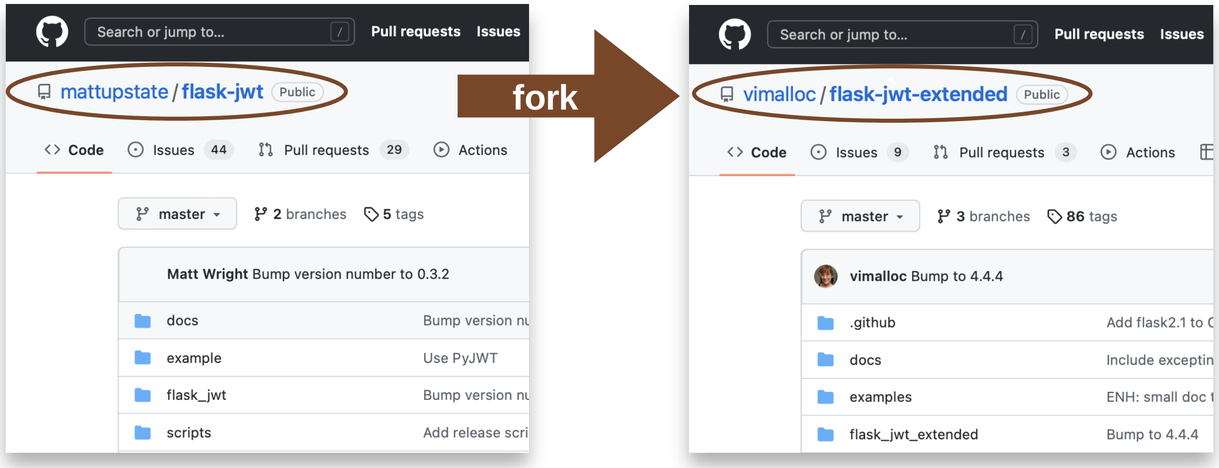
11 jobs/integration/test_aws_iam.py

@@ -7,7 +7,7 @@

```
 7  from .utils import juju_run
 8  from subprocess import check_output
 9  from shlex import split
10 - from configobj import ConfigObj
11  from cilib.run import capture
12  import os
13
```

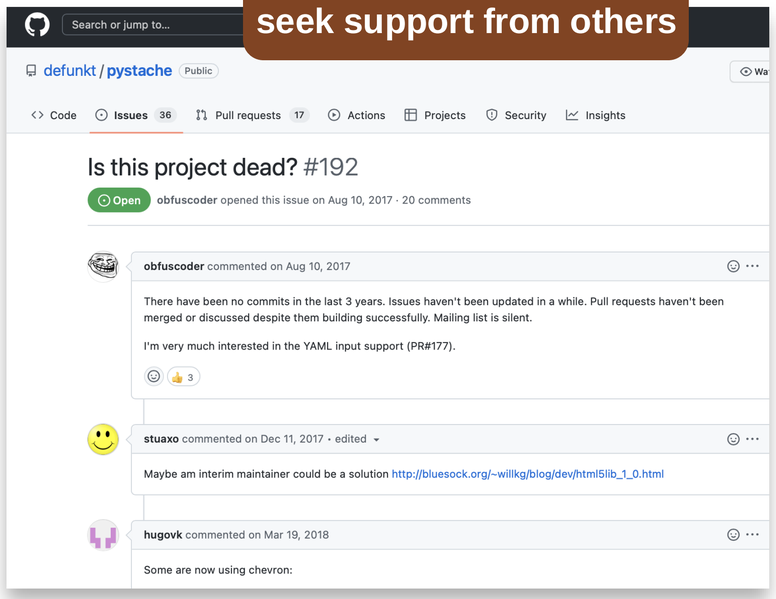
```
 7  from .utils import juju_run
 8  from subprocess import check_output
 9  from shlex import split
10 + from configparser import ConfigParser
11  from cilib.run import capture
12  import os
13
```

Dealing with abandonment typically required trial-and-error

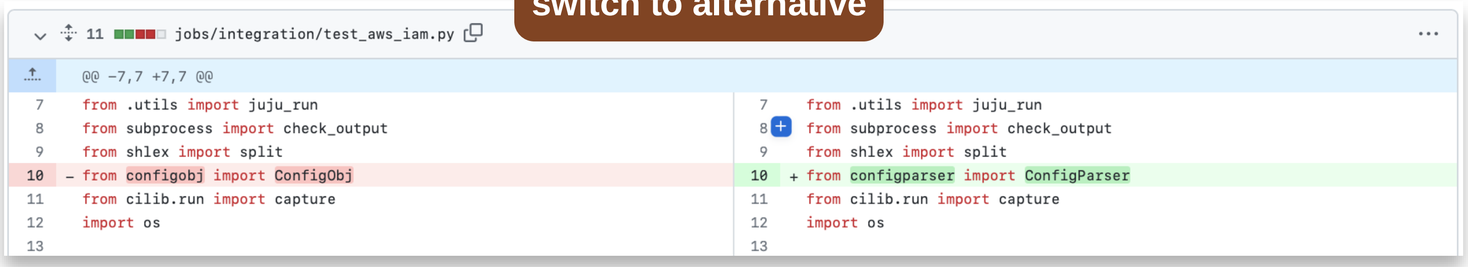


fork

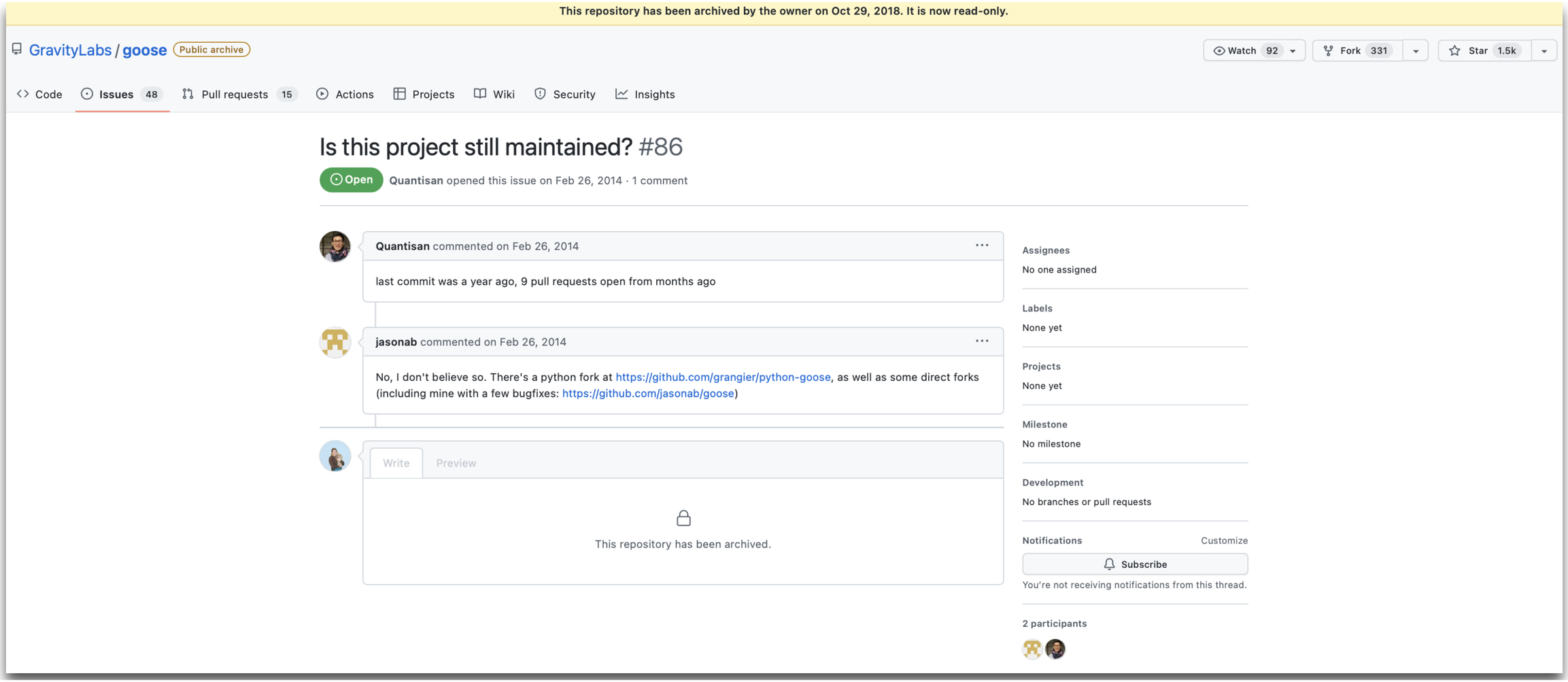
seek support from others



switch to alternative



Common theme: Interviewees benefitted from the actions of others



This repository has been archived by the owner on Oct 30, 2018. It is now read-only.

GravityLabs / goose Public archive

Notifications Fork 360 Star 1.5k

Code Issues 48 Pull requests 15 Actions Projects Wiki Security Insights

master 4 branches 32 tags Go to file Code

Migration Discussion

Quantisan commented on Feb 26, 2014

last commit was a year ago, 9 pull requests open from months ago

jasonab commented on Feb 26, 2014

No, I don't believe so. There's a python fork at https://github.com/grangier/python-goose, as well as some direct forks (including mine with a few bugfixes: https://github.com/jasonab/goose)

Add a comment

Write Preview

Add your comment here...

Comment

Tom Commit Release 2.1.29_2.10: ... 462f04a on Dec 1, 2015 197 commits

misc/PSD	adding new unit tests	13 years ago
src	Commit Release 2.1.29_2.10:	8 years ago
.gitignore	Check in Release 2.1.22_2.10, which was a port of 2.1.22 to Scala ...	8 years ago
LICENSE	adding apache2.0 licensing to files and added a LICENSE file	12 years ago
NOTICE	adding apache2.0 licensing to files and added a LICENSE file	12 years ago
README.md	Fix markdown formatting for bullet points in Readme.	12 years ago
pom.xml	Commit Release 2.1.29_2.10:	8 years ago

README.md

About

Html Content / Article Extractor in Scala - open sourced from Gravity Labs

gravity.com

Readme

Apache-2.0 license

Activity

1.5k stars

93 watching

360 forks

Report repository

Releases

32 tags

Packages

No packages published

Contributors 6

Languages

Scala 100.0%

Possible (simple) solution to support creation of community-oriented solutions

Part 1 Summary:

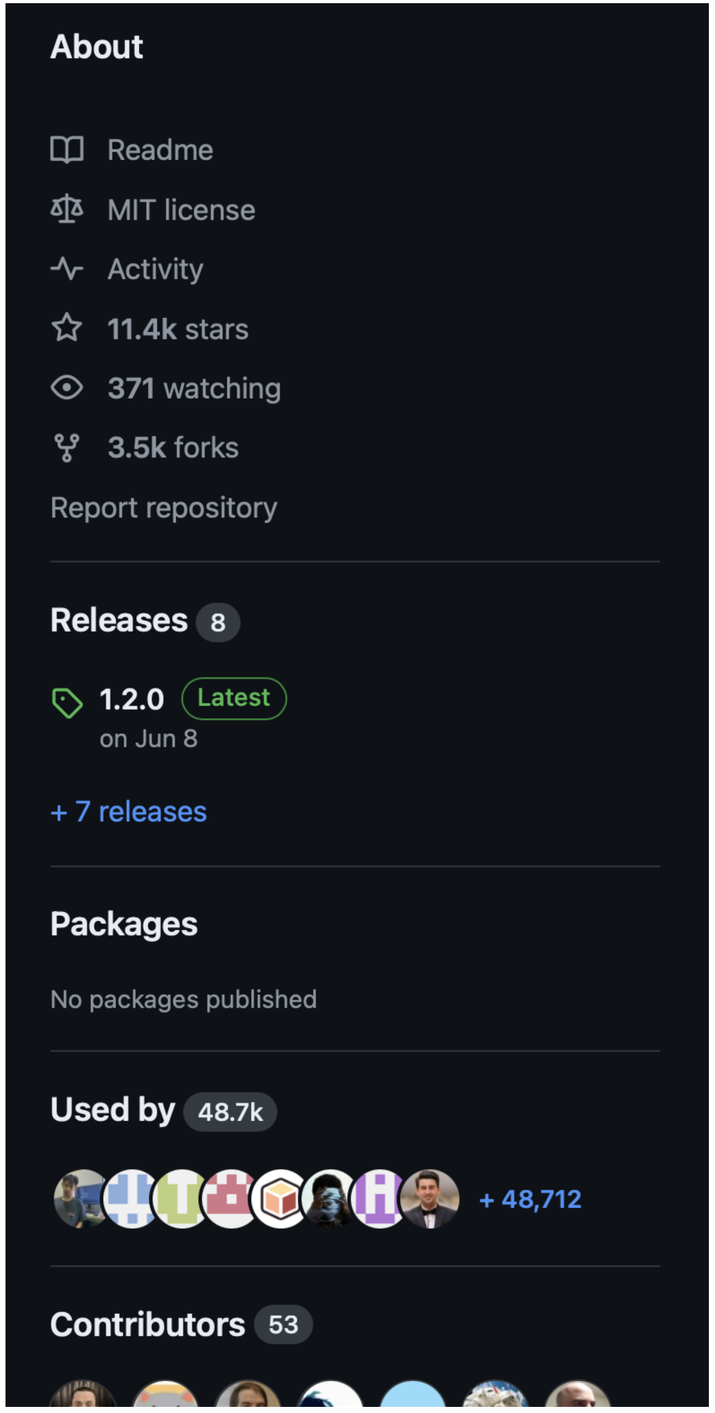
Every time a project becomes abandoned, or we think it might be abandoned, we feel like we're winging it.

We feel like we're dealing with it for the first time

- PID4

Part 2: Repository Mining

28,100 npm packages out of 1M+ in 2020
had at least one month with 10,000+ downloads

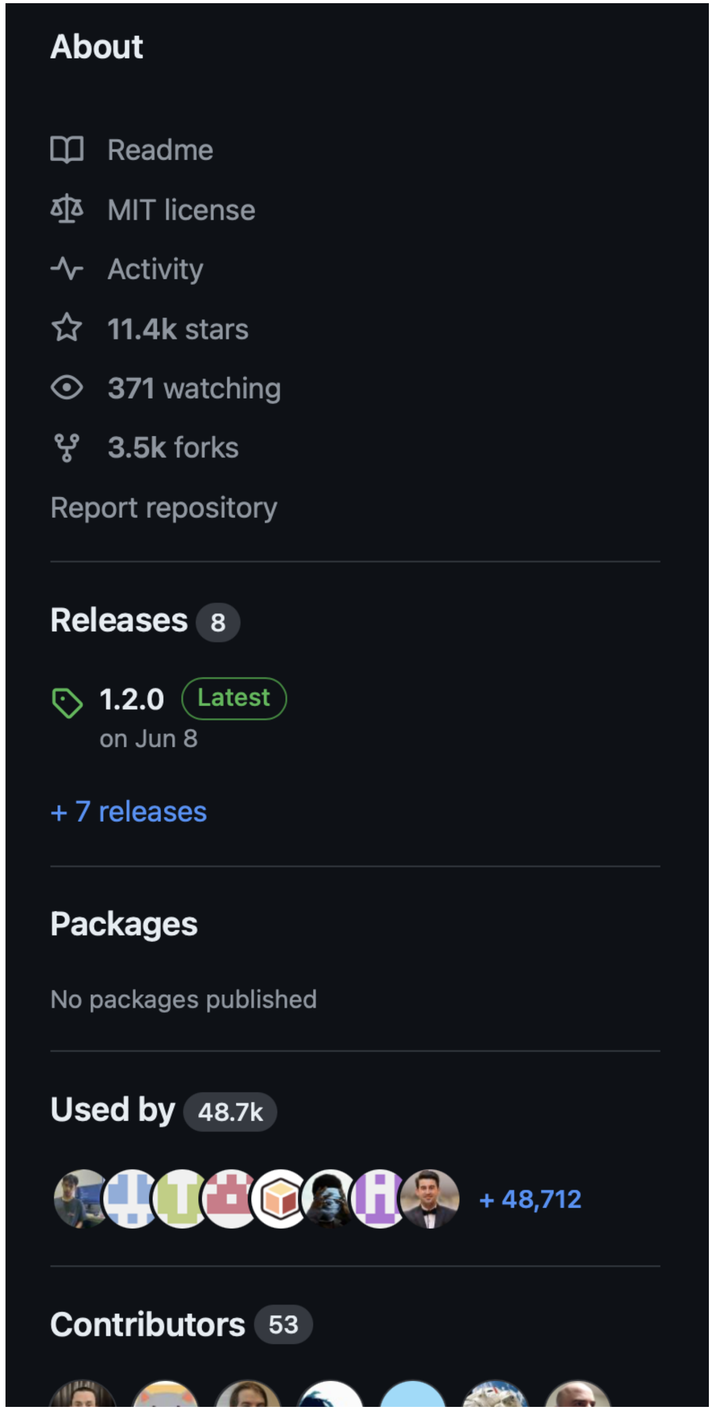


28,100 npm packages out of 1M+ in 2020
had at least one month with 10,000+ downloads

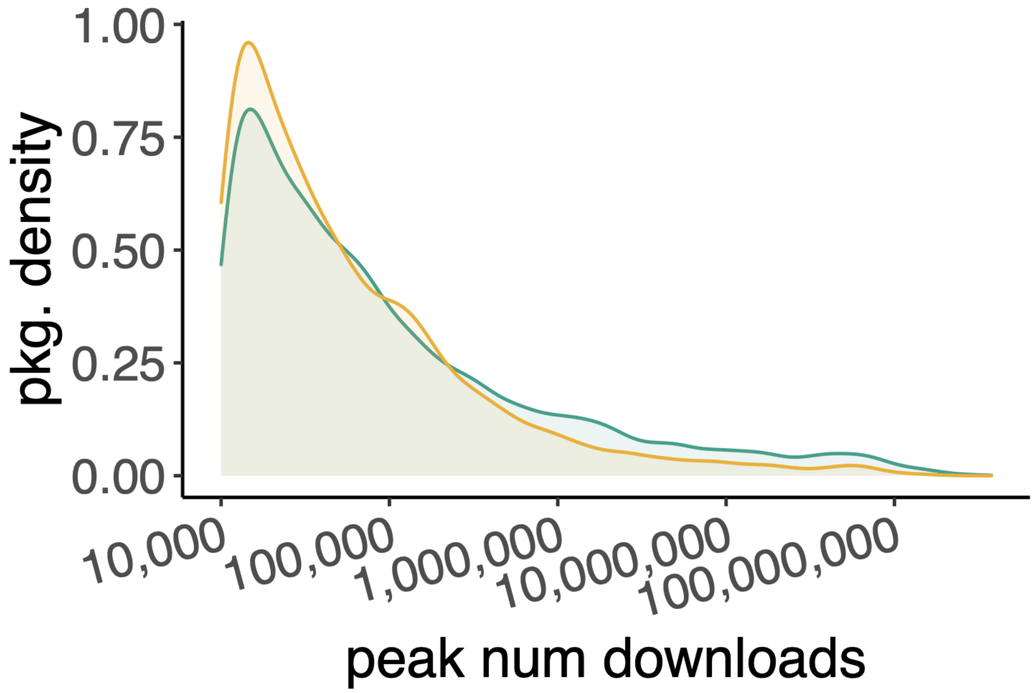
15% (4,108)

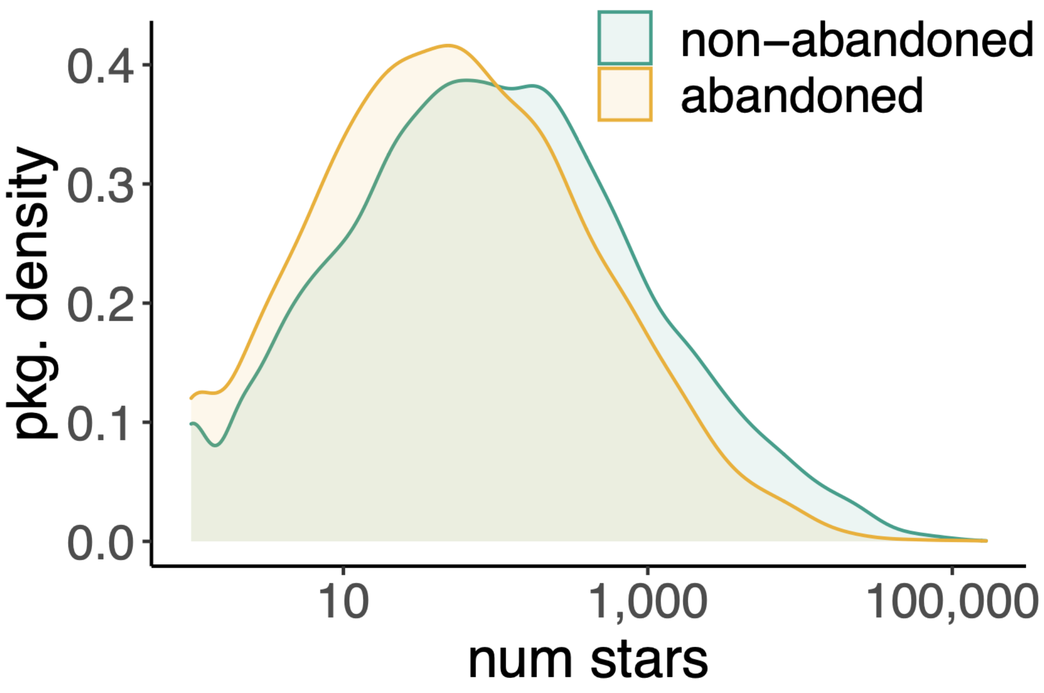
became abandoned

Observation window: Jan 2015 to Dec 2020



The distributions of peak download and current star counts for both abandoned and non-abandoned packages are similar.



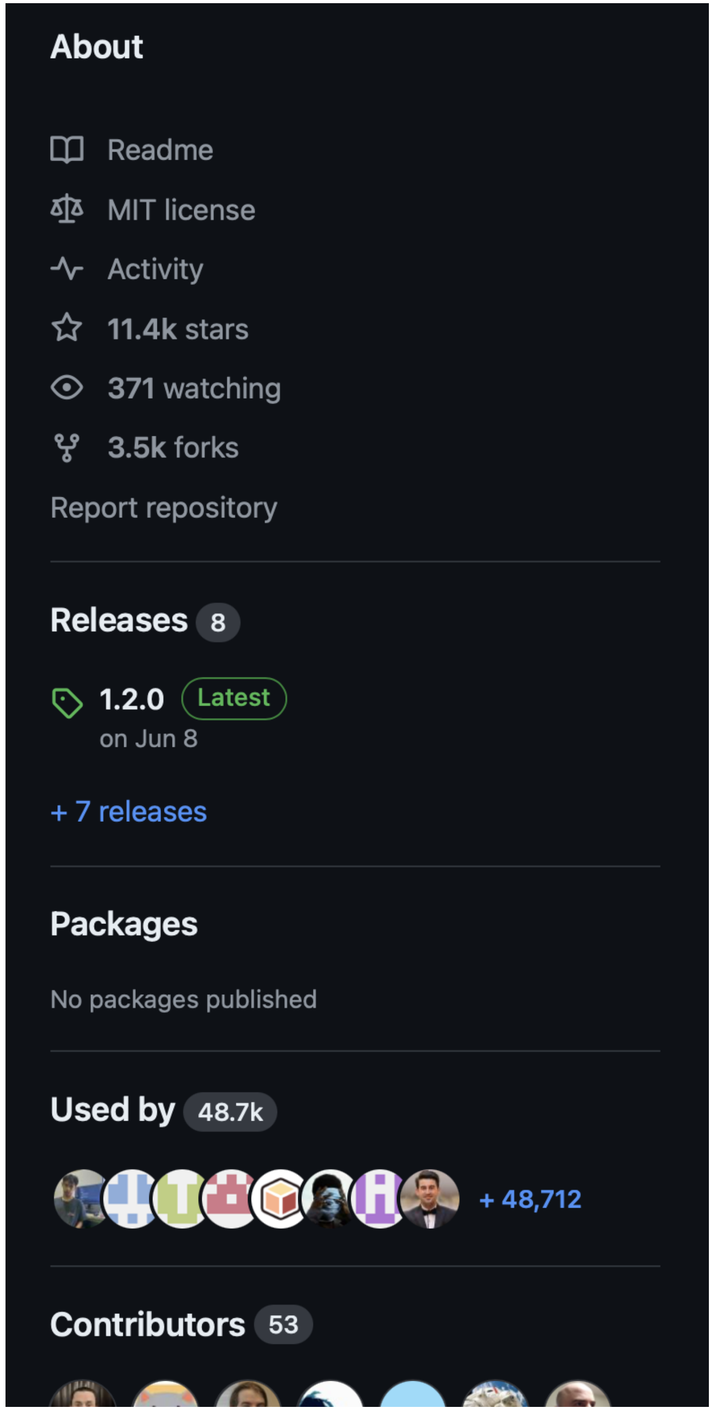


The abandoned projects impacted

~280k+ downstreams on GitHub

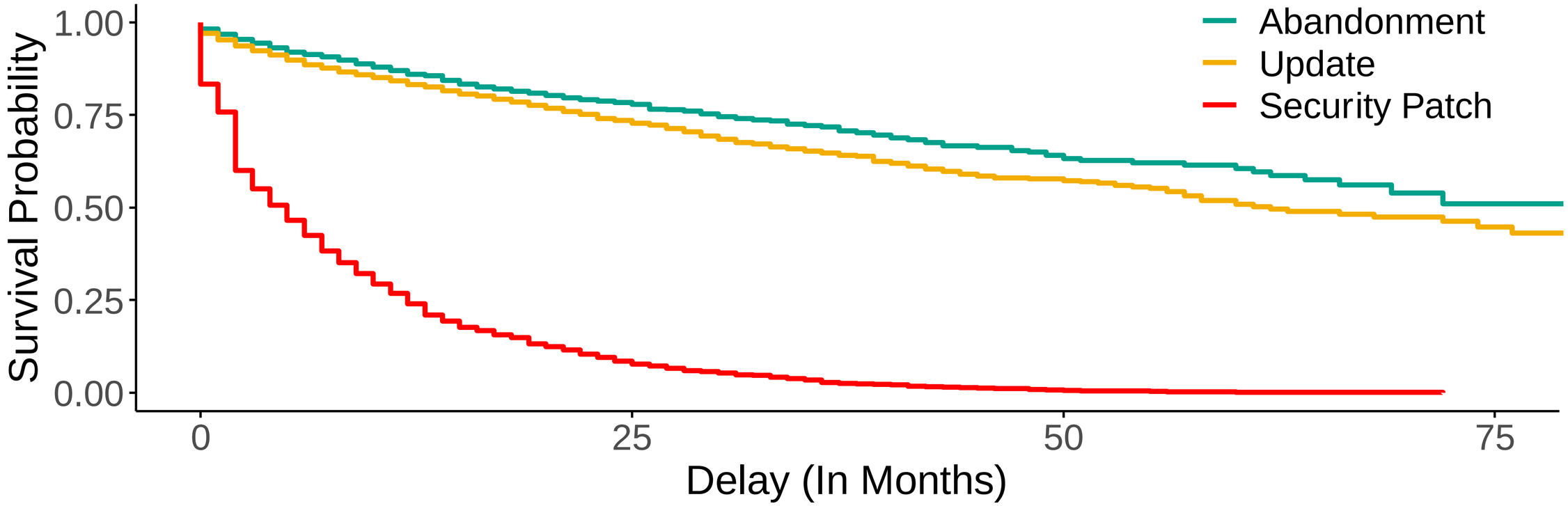
of which

~78k+ were still active at the time

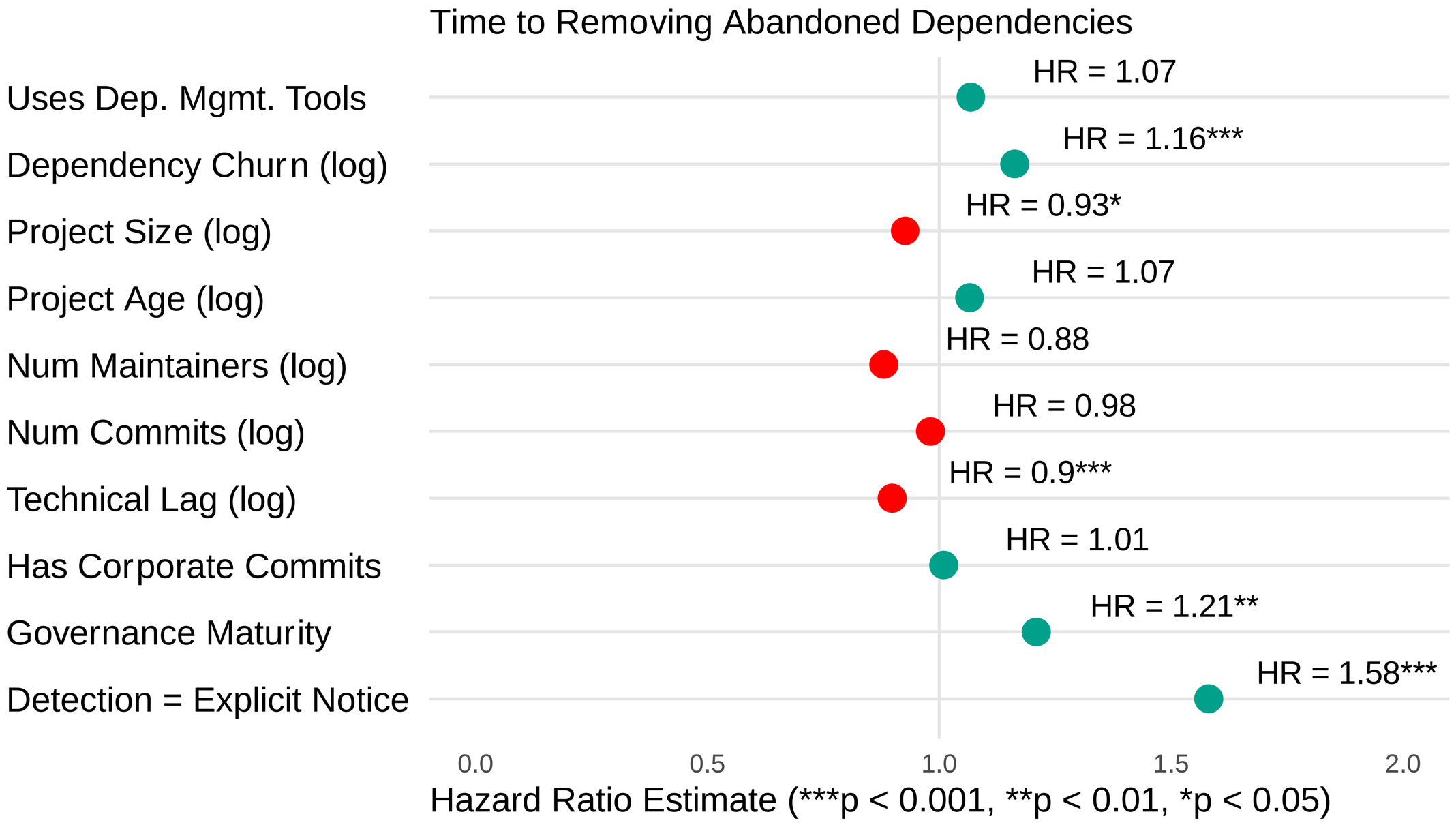


How much do people downstream react?

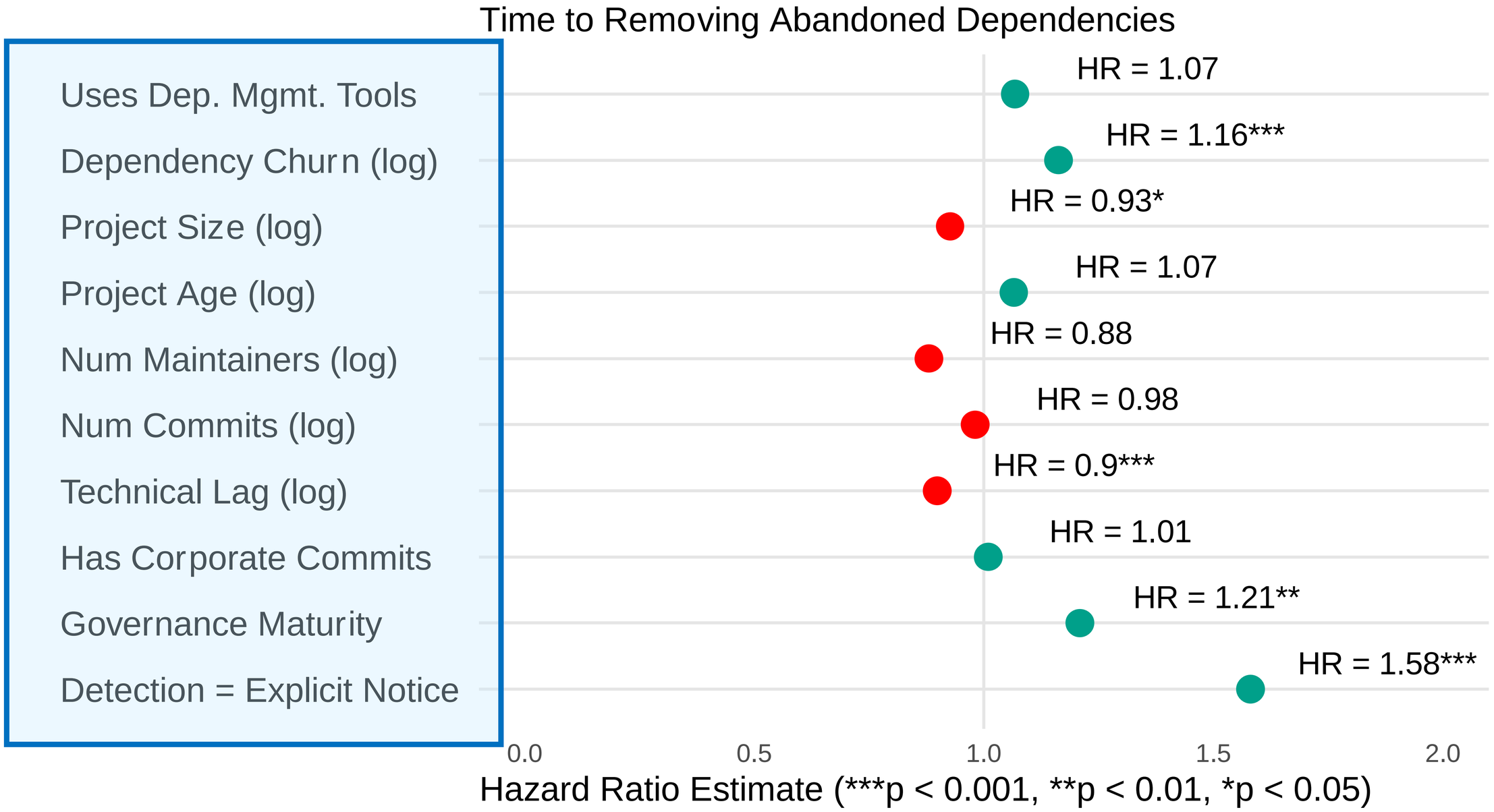
The rate of removing abandoned dependencies is similar to random dependency updates, and slower than security patch updates.



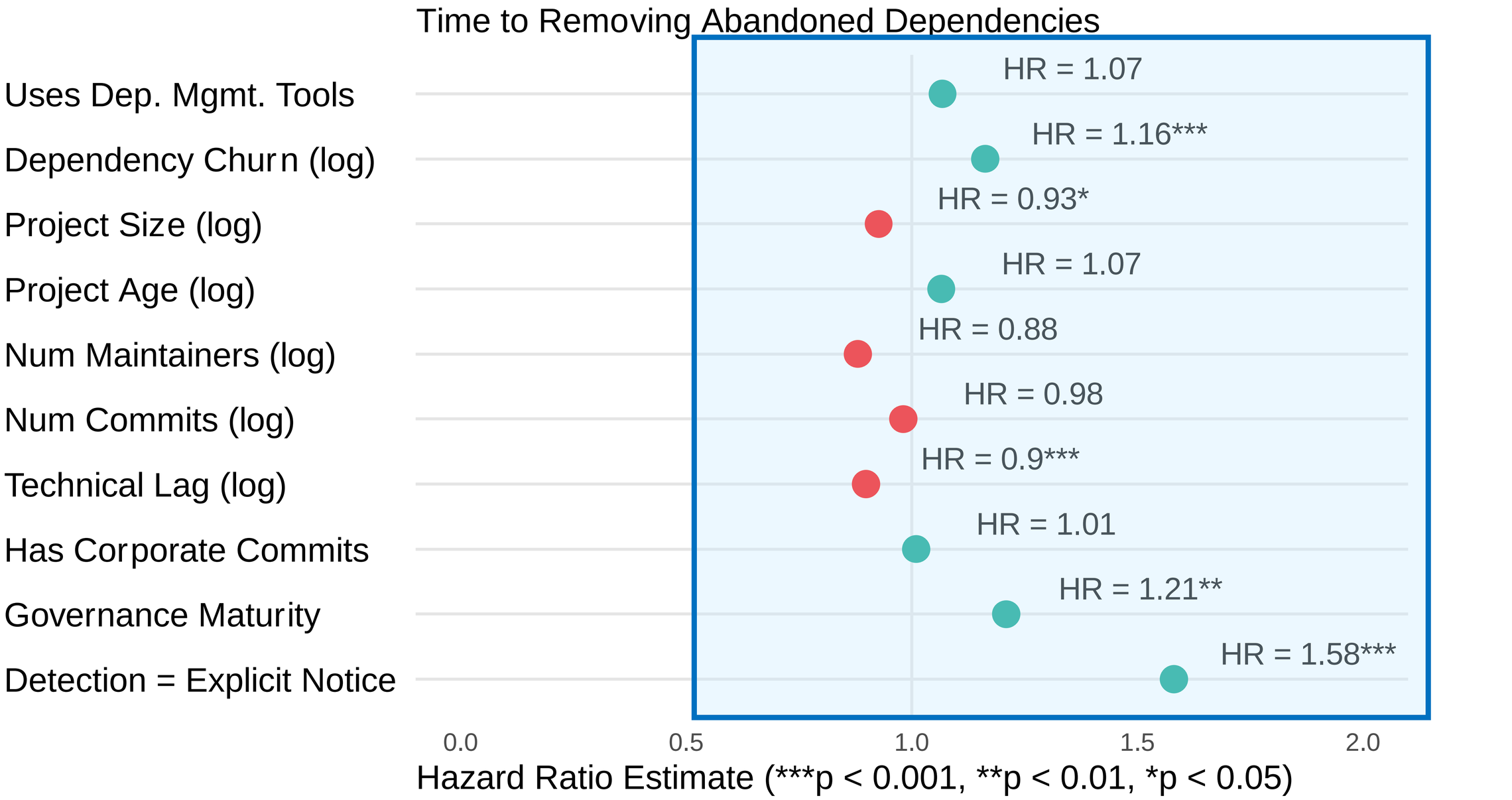
Which factors correlate with downstream projects reacting faster?


Time to Removing Abandoned Dependencies
Uses Dep. Mgmt. Tools
Dependency Churn (log)
Project Size (log)
Project Age (log)
Num Maintainers (log)
Num Commits (log)
Technical Lag (log)
Has Corporate Commits
Governance Maturity
Detection = Explicit Notice
HR = 1.07
HR = 1.16***
HR = 0.93*
HR = 1.07
HR = 0.88
HR = 0.98
HR = 0.9***
HR = 1.01
HR = 1.21**
HR = 1.58***
0.0
0.5
1.0
1.5
2.0
Hazard Ratio Estimate (***p < 0.001, **p < 0.01, *p < 0.05)

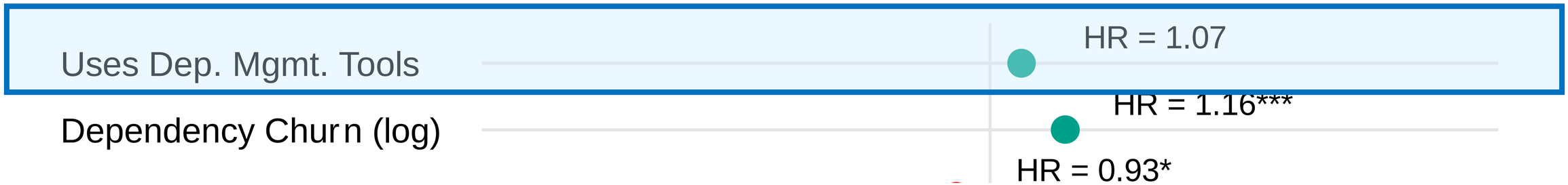
Factors


Time to Removing Abandoned Dependencies
Uses Dep. Mgmt. Tools
Dependency Churn (log)
Project Size (log)
Project Age (log)
Num Maintainers (log)
Num Commits (log)
Technical Lag (log)
Has Corporate Commits
Governance Maturity
Detection = Explicit Notice
HR = 1.07
HR = 1.16***
HR = 0.93*
HR = 1.07
HR = 0.88
HR = 0.98
HR = 0.9***
HR = 1.01
HR = 1.21**
HR = 1.58***
0.0
0.5
1.0
1.5
2.0
Hazard Ratio Estimate (***p < 0.001, **p < 0.01, *p < 0.05)

Magnitude of correlation

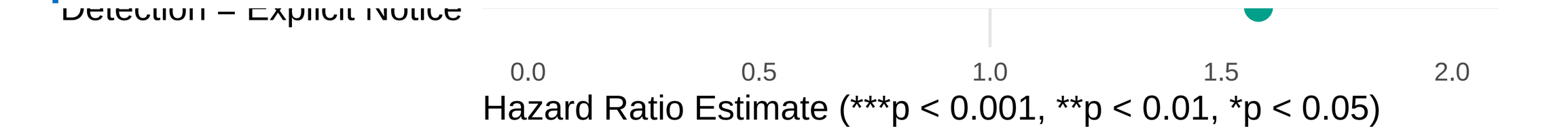


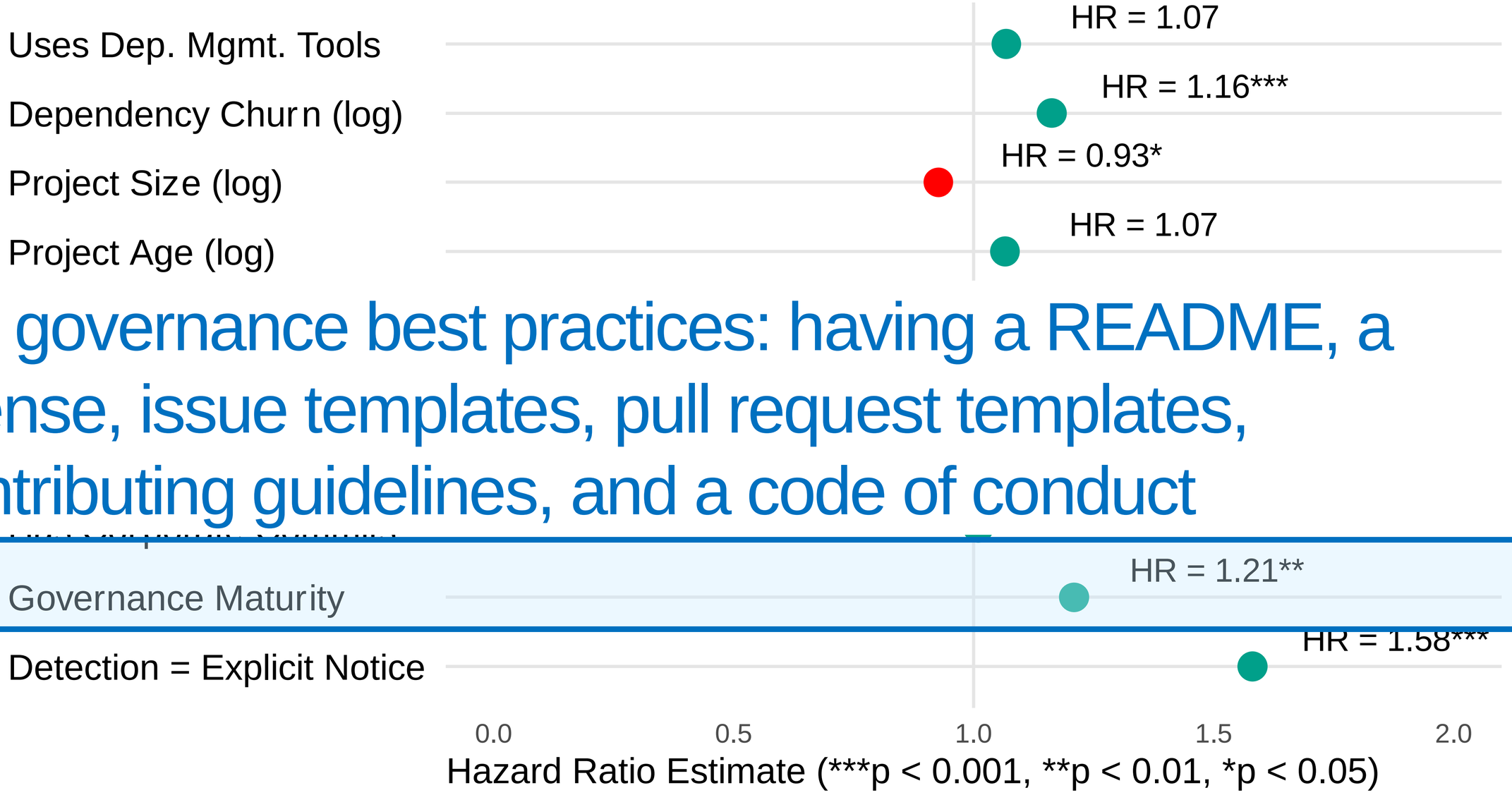
Automation: no effect



Project size: no effect

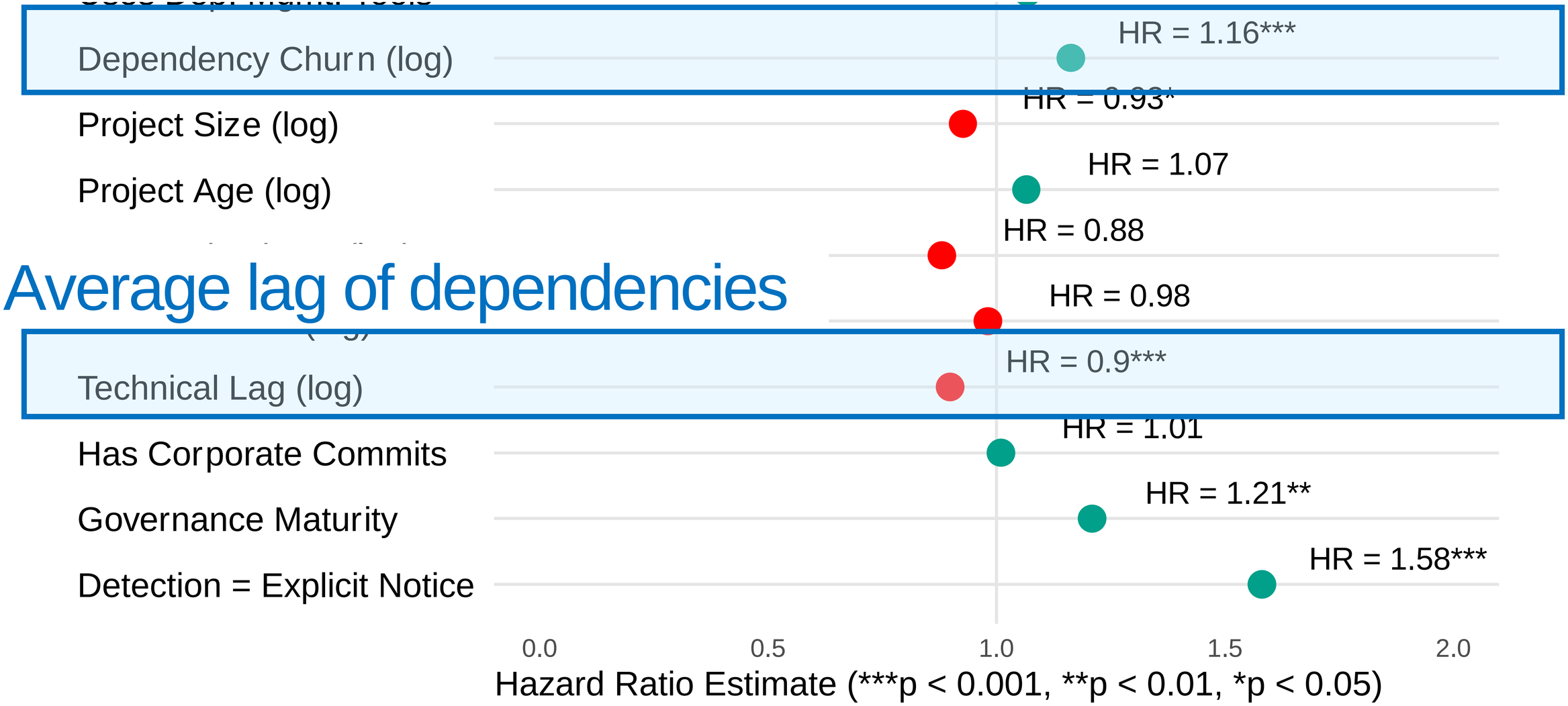
Corporate involvement: no effect



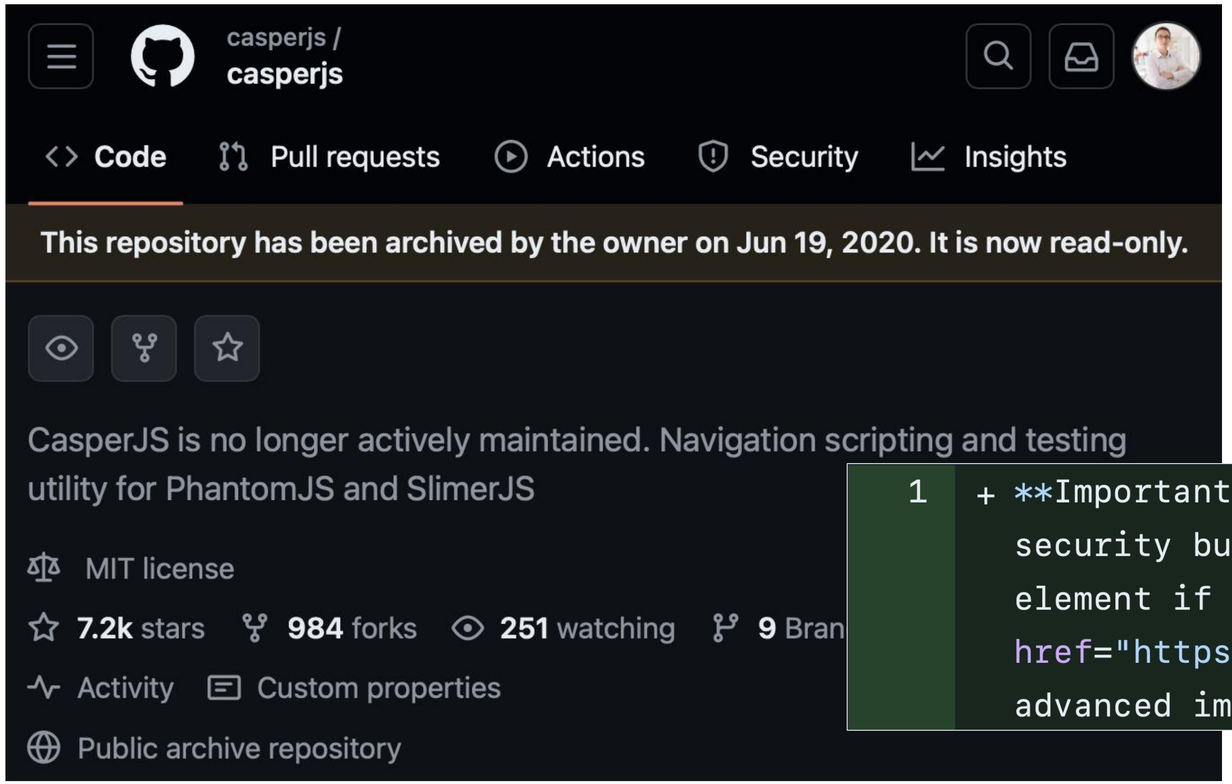


Six governance best practices: having a README, a license, issue templates, pull request templates, contributing guidelines, and a code of conduct

Updates to dependencies in the year before exposure



Average lag of dependencies

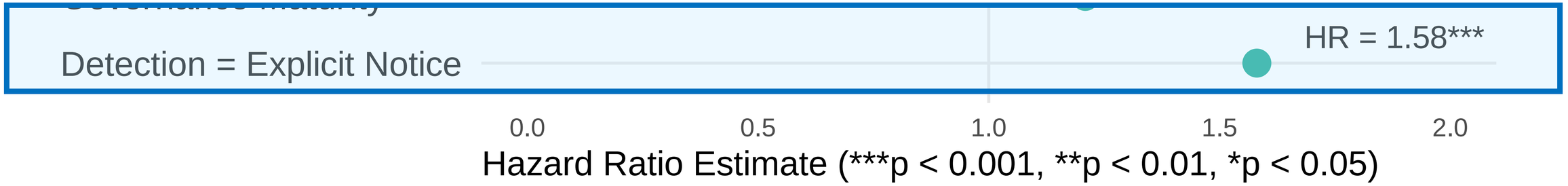


http://unmaintained.tech


```
1  + **Important note** This jQuery plugin is deprecated, only critical or
     security bug fixes will be released in future. Use native `<dialog>`
     element if you need a basic dialog/modal/popup, or my <a
     href="https://photoswipe.com">PhotoSwipe</a> library if you need an
     advanced image gallery. Feel free to email me if you need assistance.
```

Strongest effect: Explicit notice of abandonment

(Github archive flag, no-maintenance-intended badge, other mention in README)



Parting Thoughts

- Abandonment, even among widely-used npm packages, is fairly common.
- It can have rippling effects, especially when considering transitive impact.
- People seem to care about abandoned dependencies (many remove them), but may not notice them. It's also unclear what to do after.
- At the very least, we recommend that:
  - Maintainers place an **explicit notice** of abandonment somewhere visible.
  - Platforms implement features to **help with migration**.
- It's time to establish best practices for **responsible sunsetting** of packages, rather than insisting on indefinite maintenance!

Bogdan Vasilescu
@b_vasilescu
https://bvasiles.github.io

STRUDEL
SOCIO-TECHNICAL RESEARCH USING DATA EXCAVATION LAB

Our papers:
https://cmustrudel.github.io/publications/

Our sponsors:

NSF

DIGITAL INFRASTRUCTURE INSIGHTS FUND

Google Open Source

Courtney Miller
@courtneyelta
https://courtney-e-miller.github.io