

# KEEPING THE BUILD UP-TO-PAR

An empirical study on in-range breaking updates in the npm ecosystem



Presented By Benjamin Rombaut  
MSc Student  
Software Analysis & Intelligence Lab  
Queen's University  
Kingston, Ontario, Canada



Queen's  
UNIVERSITY

# BREAKING IN-RANGE UPDATES

- Clients can specify accepted versions of dependencies they would like to use.
- Greenkeeper automatically tests new dependency versions, and opens issue reports if they fail a project's CI pipeline.
- Breaking build issue reports for in-range updates means the project will fail to build for any new installs or upgrades.

## An in-range update of postcss is breaking the build

 Open

greenkeeper bot opened this issue on Jan 22 · 4 comments



greenkeeper bot commented on Jan 22

+  ...

The devDependency [postcss](#) was updated from `7.0.13` to `7.0.14`.

 [View failing branch.](#)

This version is **covered** by your **current version range** and after updating it in your project **the build failed**.

postcss is a devDependency of this project. It **might not break your production code or affect downstream projects**, but probably breaks your build or test tools, which may **prevent deploying or publishing**.

# CHARACTERISTICS OF IN-RANGE BREAKING UPDATES AND HOW CLIENT'S RESOLVE THEIR BUILD

01



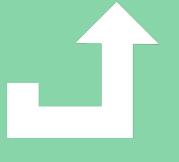
What are the characteristics of in-range updates that break a client's build?

02



How do clients respond to in-range breaking updates?

03



Do broken builds in clients prompt a response from the breakage-inducing provider?

## DATA COLLECTION



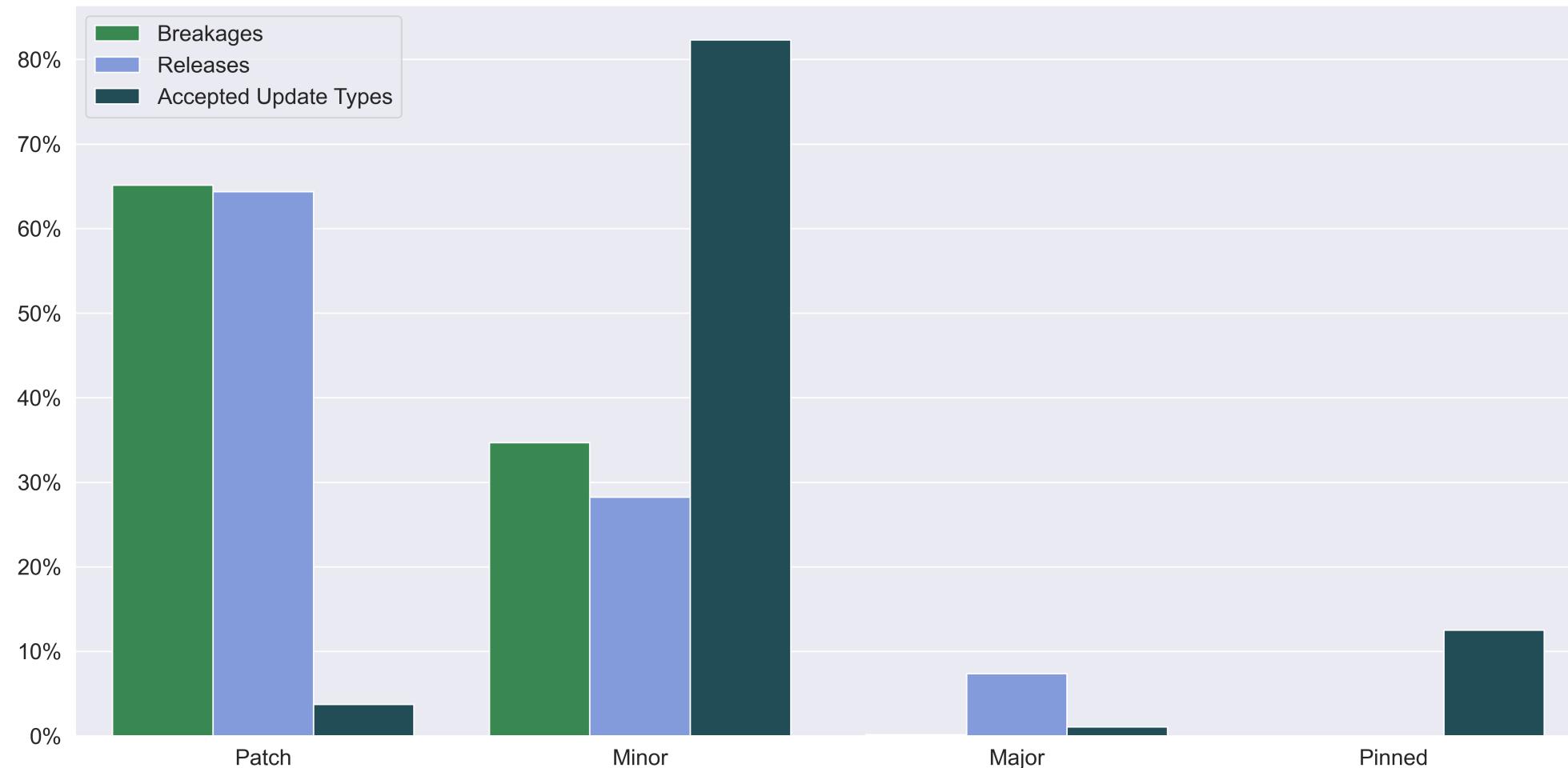
- 12,134 Projects

- 123,197 Issue Reports
- 365,625 Comments
- 209,750 Events
- 17,623 Commits

- 556,742 Version Release Records
- Release Frequency of 7,361 Projects

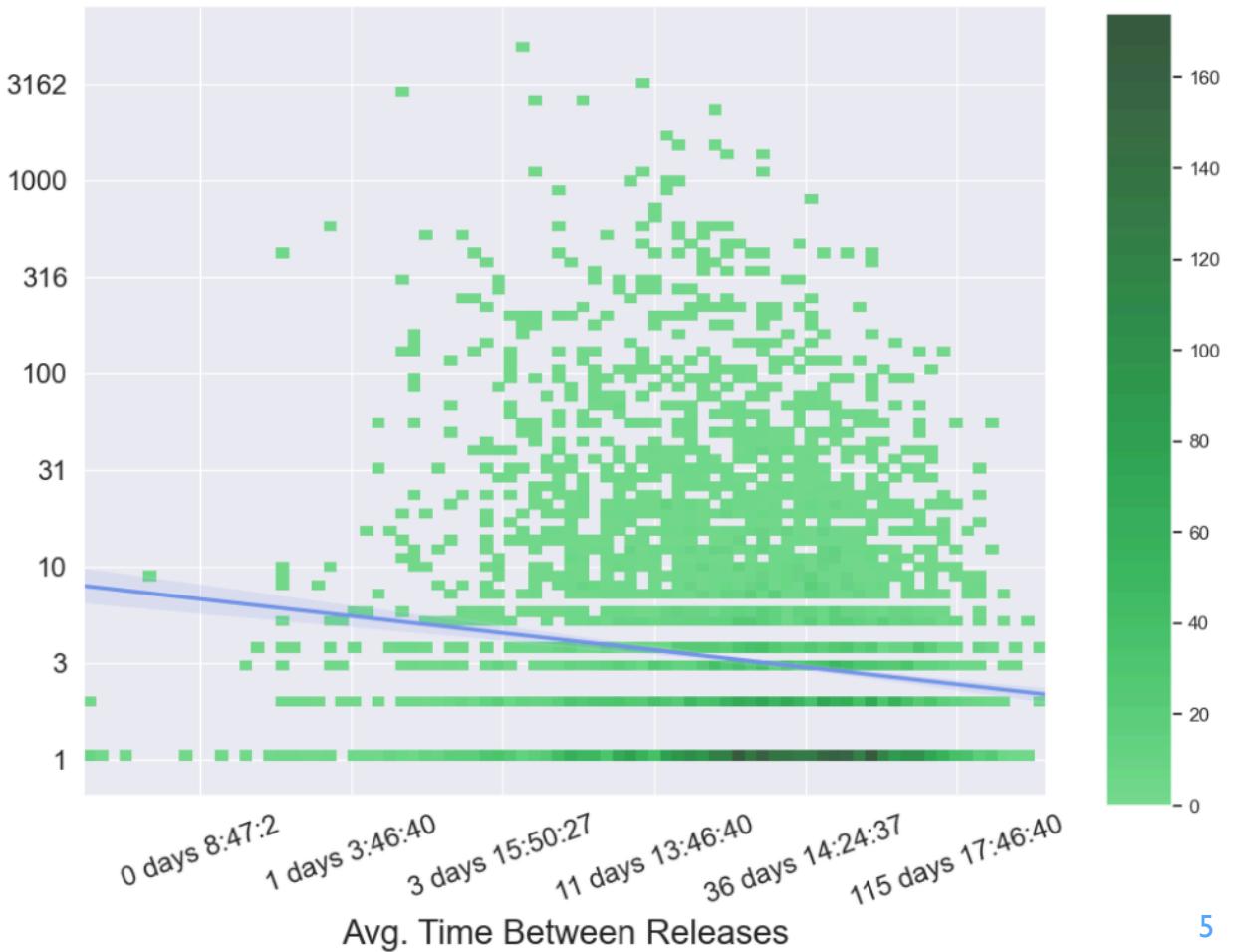
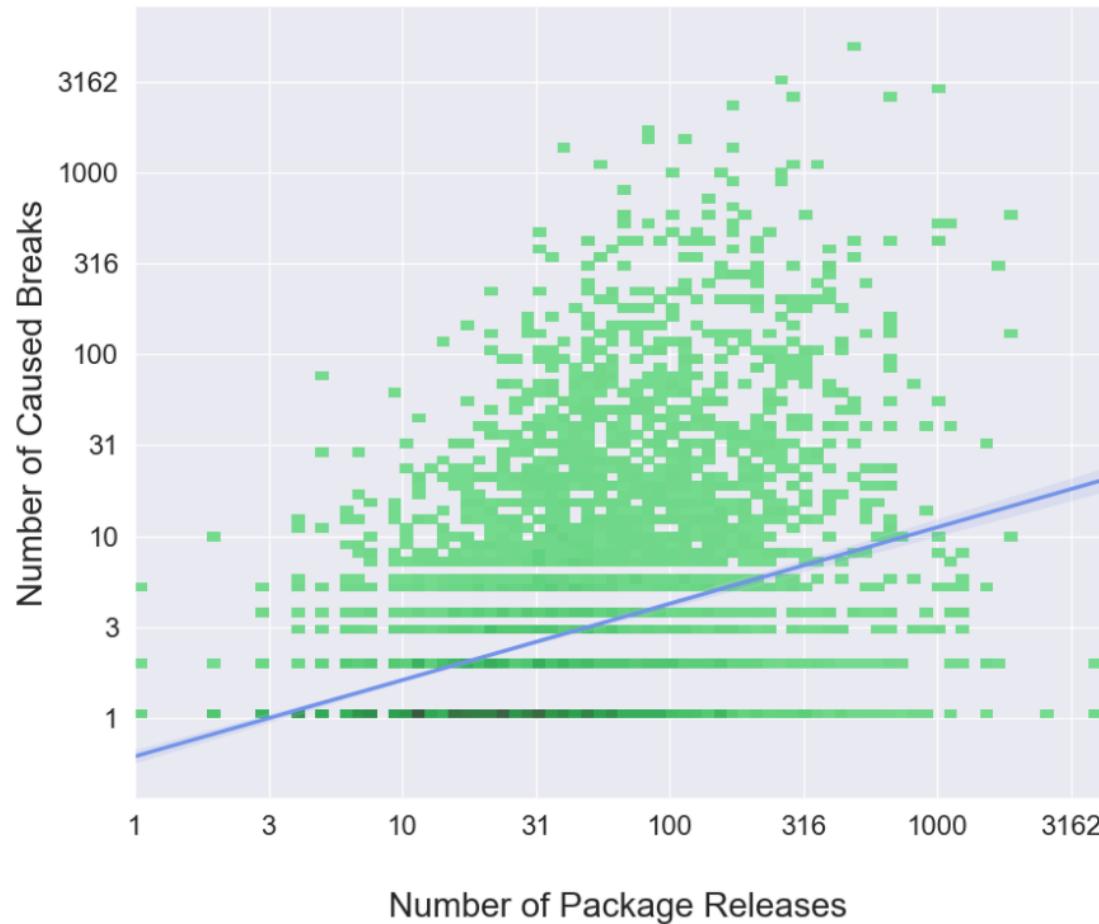


## WHILE THE MAJORITY OF CLIENTS WILL ACCEPT MINOR UPDATES, MOST BREAKAGES ARE CAUSED BY PATCH UPDATES





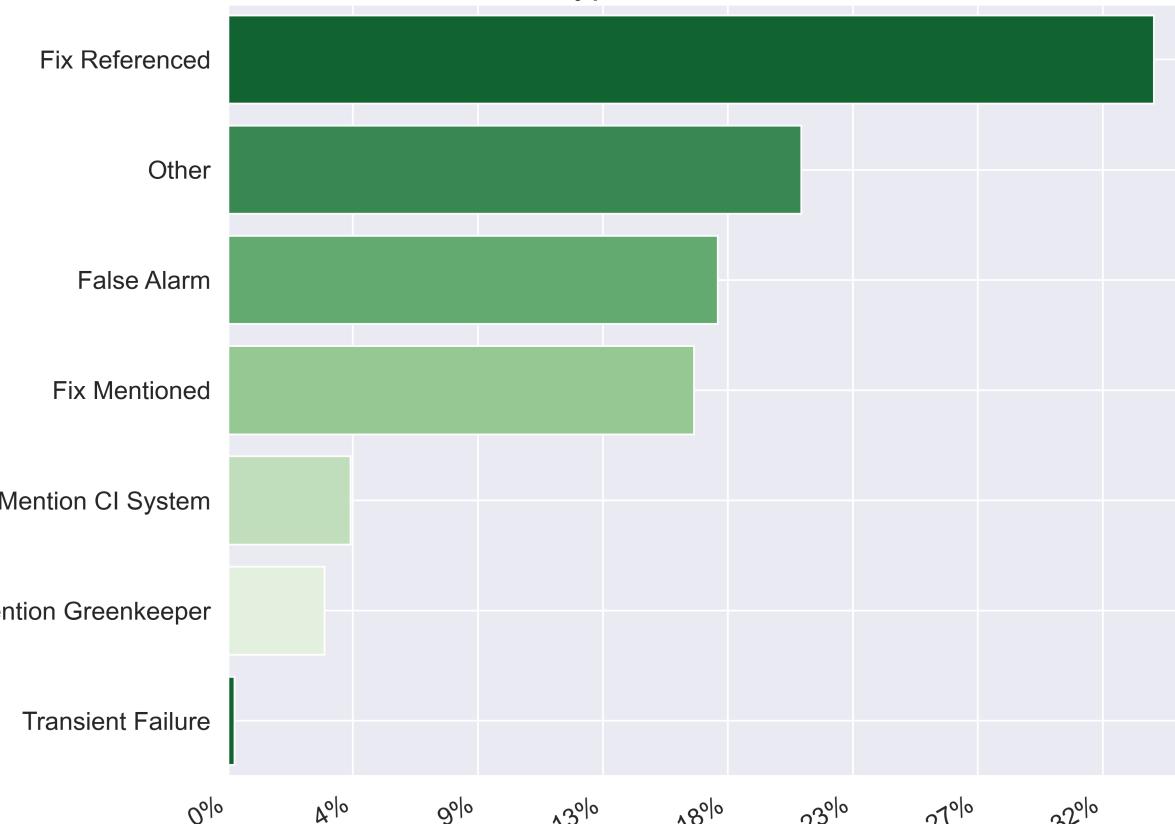
# PACKAGES WITH HIGHER TOTAL AND MORE FREQUENT RELEASES TEND TO CAUSE MORE BREAKAGES



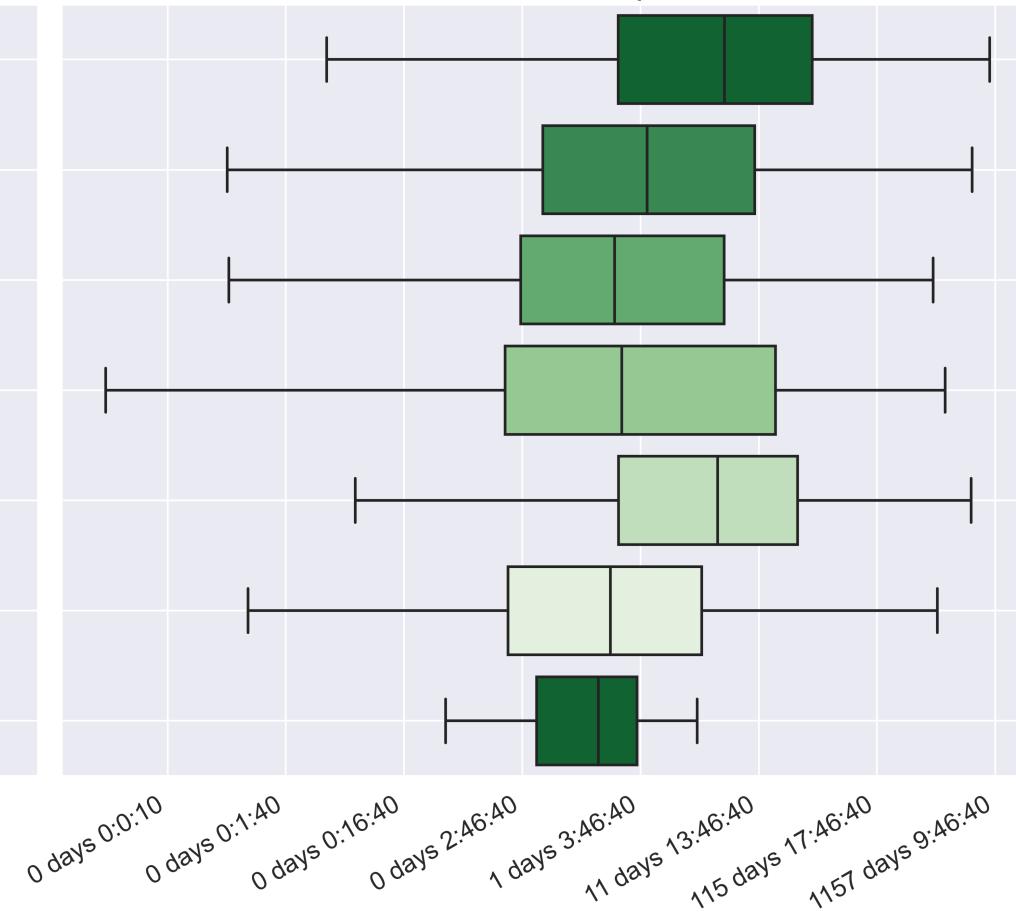


# THE MAJORITY OF CLIENT RESPONSES MENTION A FIX OR CONFIRM THE ISSUE IS INVALID

Types of Comments

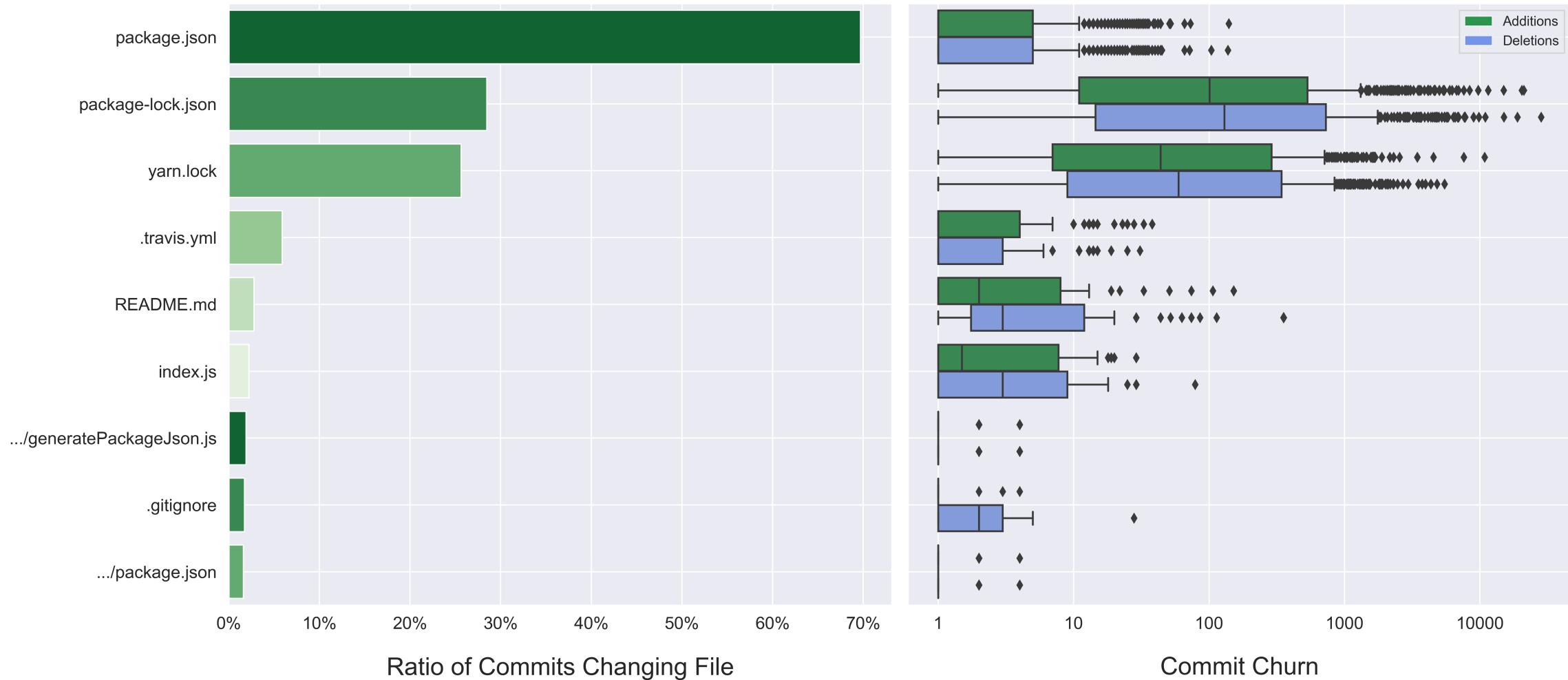


Time to First Response





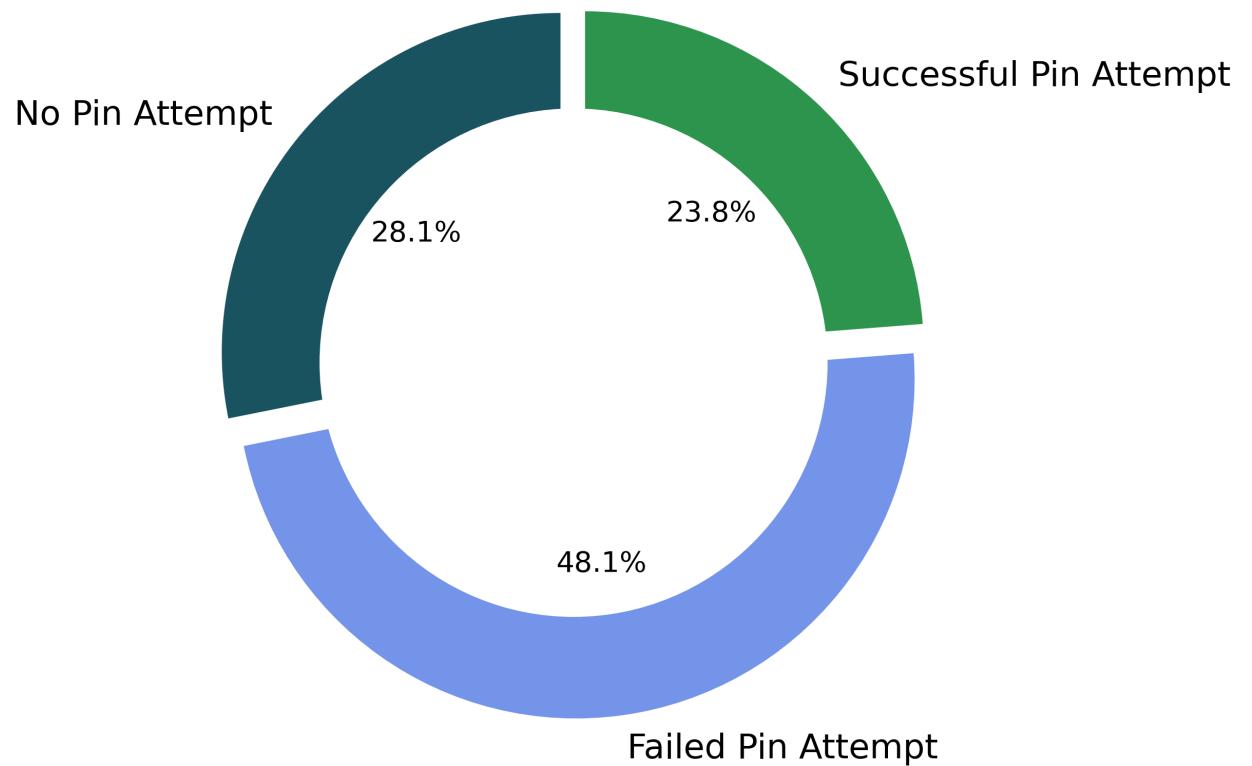
# MOST FIXES INVOLVE SMALL CHANGES TO DEPENDENCY SPECIFICATION FILES





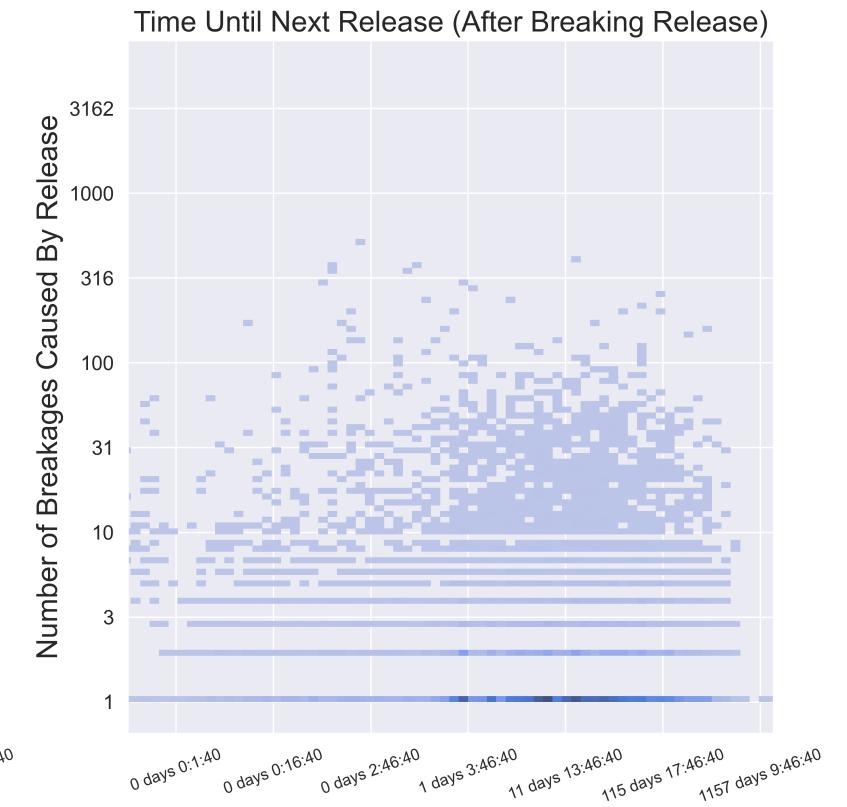
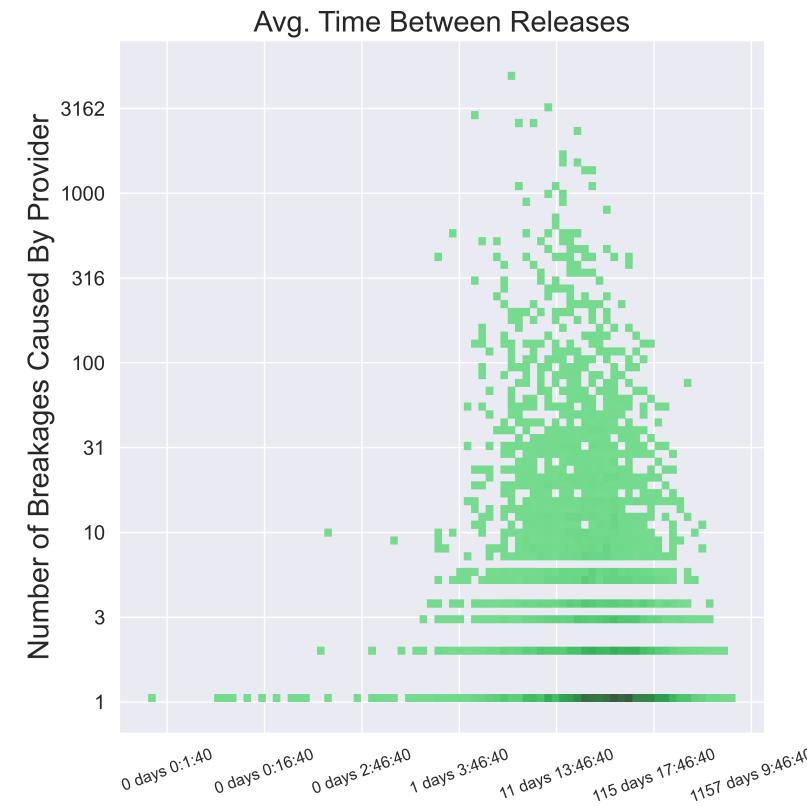
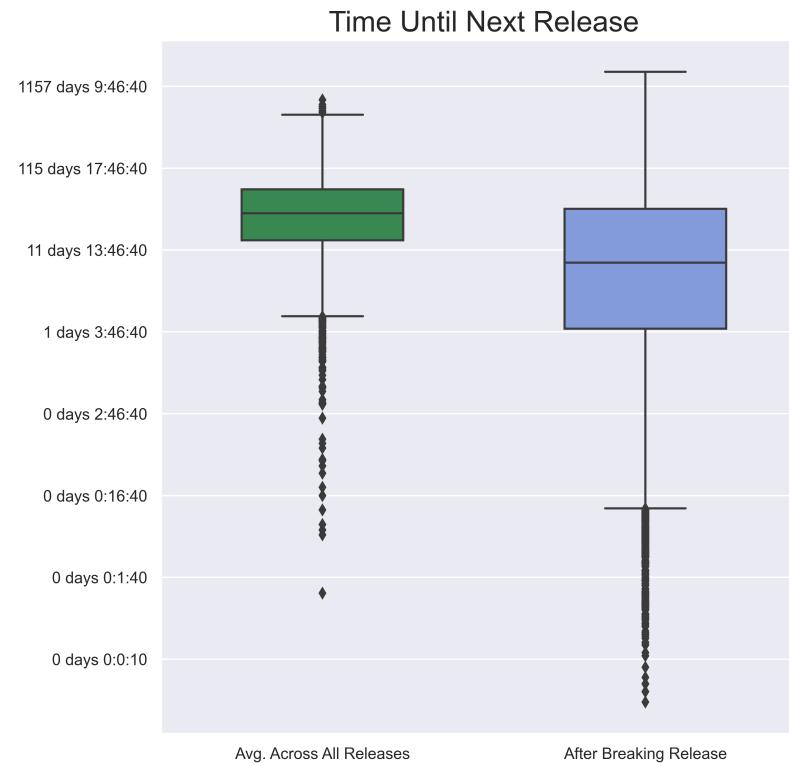
## WHILE PINNING THE DEPENDENCY IS A LEGITIMATE OPTION, IT IS NOT AS SUCCESSFUL AS EXPECTED

- Greenkeeper will automatically attempt to pin the failing dependency for most issue reports.
- Only about 250 referenced commits were found that matched pinning criteria





# PROVIDERS RELEASE A NEW VERSION QUICKER THAN USUAL AFTER RELEASING A VERSION THAT BREAKS CLIENT'S BUILDS



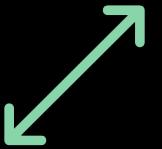
# MOVING FORWARD



Manual analysis of pinning failures.



More concrete analysis on how release frequency changes after a breaking update.



Expand study to include issues from Dependabot.

## CHARACTERISTICS OF IN-RANGE BREAKING UPDATES AND HOW CLIENT'S RESOLVE THEIR BUILD

01



What are the characteristics of in-range updates that break a client's build?

02



How do clients respond to in-range breaking updates?

03

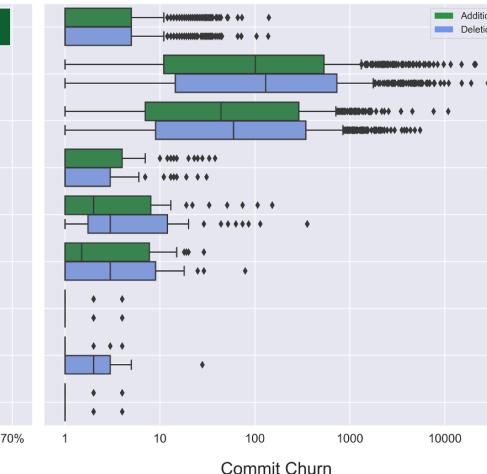
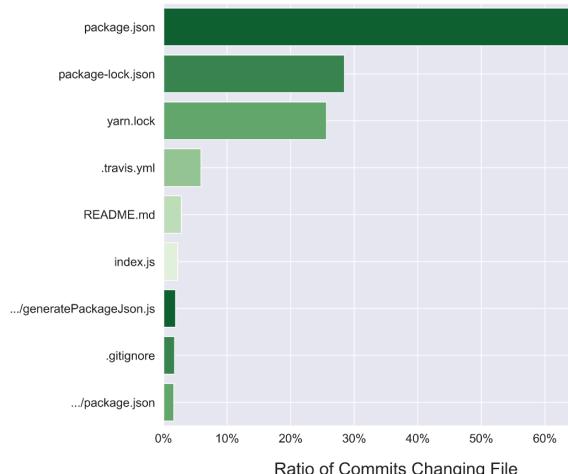


Do broken builds in clients prompt a response from the breakage-inducing provider?

2



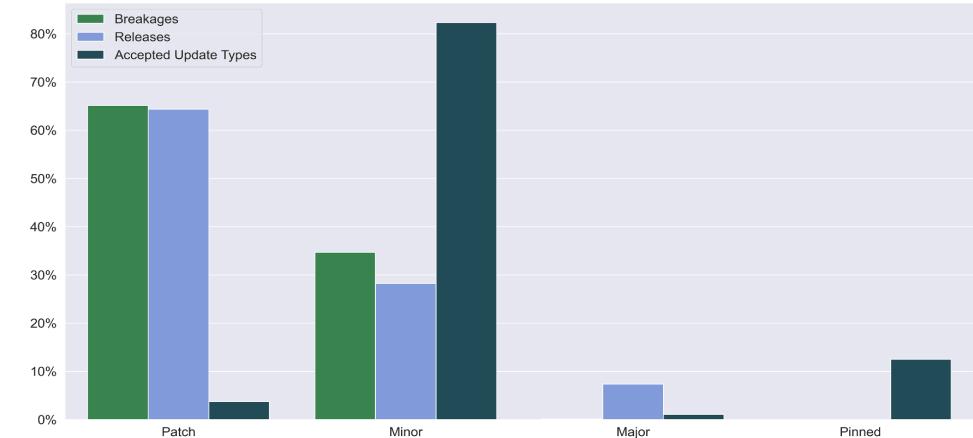
### MOST FIXES INVOLVE SMALL CHANGES TO DEPENDENCY SPECIFICATION FILES



7



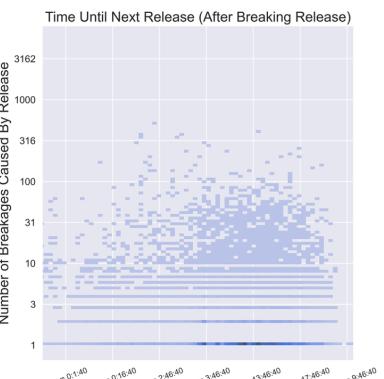
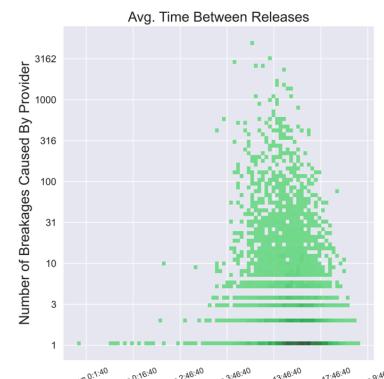
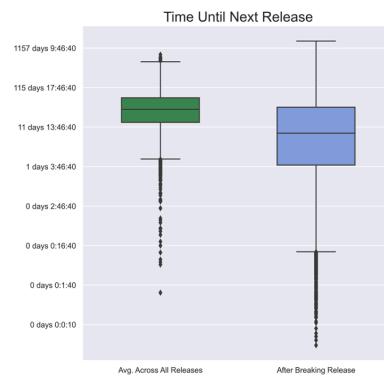
## WHILE THE MAJORITY OF CLIENTS WILL ACCEPT MINOR UPDATES, MOST BREAKAGES ARE CAUSED BY PATCH UPDATES



4



### PROVIDERS RELEASE A NEW VERSION QUICKER THAN USUAL AFTER RELEASING A VERSION THAT BREAK CLIENT'S BUILDS



8