Renovate Bot

A bot for automated dependency updates

What is Renovate?

Renovate (often referred to as "Renovate Bot") is an Open Source tool designed to **automate the process** of:

- **Detecting dependencies** in a repository
  - Open Source
  - Private/closed source
- **Checking if there are newer versions** which can be updated to
- Creating commits and **Merge/Pull Requests** to apply such changes
  - include Release Notes if available

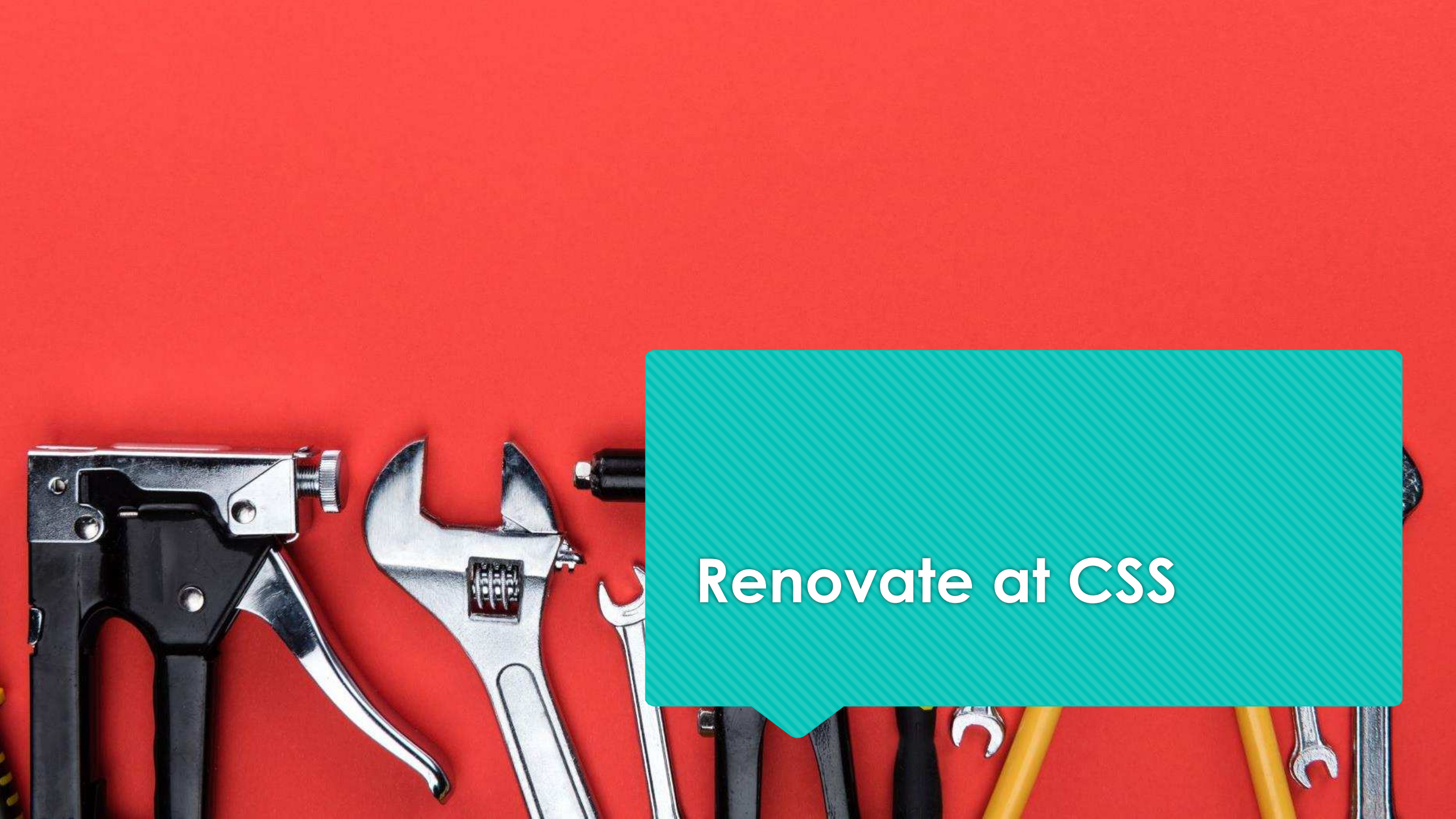
Purpose

- Address the **problem of stale/out-of-date dependencies** in software projects
- Out-of-date projects **missing** out on **bug fixes or new features**, but they also suffer from the following **indirect consequences** too
  - Getting further into "technical debt" by **increasing the amount of custom code** using deprecated APIs
  - Increasing the time-to-resolution of vulnerabilities due to the **risk of performing large jumps** of dependency versions under stress
- Save time to **focus on more important duties** by automating the process of updating dependencies

Language Support

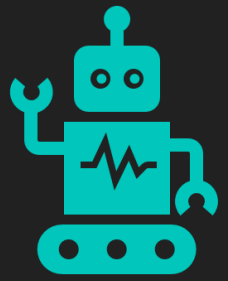
Renovate supports a bunch of languages

- Docker
  - Docker's Dockerfile files
- Java
  - Maven
  - Gradle
- Javascript
  - package.json files
  - npm, yarn and pnpm
- And many more ;)



Renovate at CSS

Why do we use it?



Edgar not suitable for DevOps applications (AWL 2.0)

css-versions-maven-plugin: Specialized application/plugin that defines and updates the dependency versions **based on the CSS software release schedule**

Releases transient snapshot dependencies

DevOps team is responsible to use the correct versions

In DevOps mode there is **no fixed schedule**

No snapshot versions, only released versions

Running Renovate

- CSS is using the self-hosting approach on our **K8s cluster**
- Renovate is run as **CRON job** at **every full hour** (0 * * * *)
  - This can be changed on demand for a whole Bitbucket project (not repository level)

- Renovate is **enabled by default** for every **new DevOps project**
  - Older projects need to be enabled by support ticket
  - Teamcity builds need to be adjusted (no display, apply and update dependencies builds anymore)

Onboarding

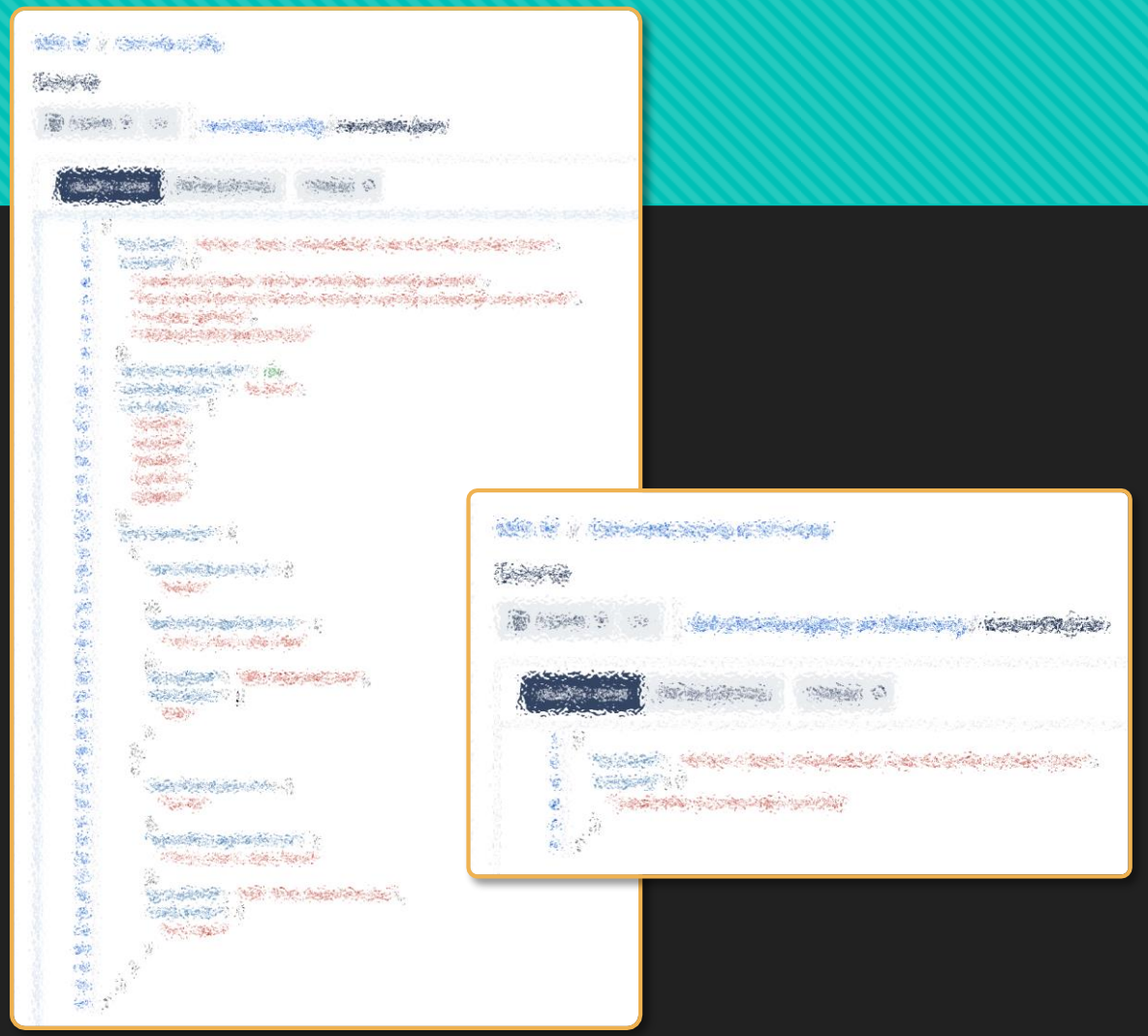
- Once Renovate is enabled there will be a **"Configure Renovate" Pull Request** (aka Onboarding PR) created
  - Explains the configuration and what will be updated if merged
- **Risk-free onboarding**
  - No further PRs until Onboarding PR is merged
  - Edit configuration within the `renovate/configure` branch
    - Renovate updates the description according to the changes
- Onboarding PR creates **renovate.json file** in root directory
  - Contains the default settings
  - Can be updated with custom settings

Configuration

Renovate is **highly configurable** through `renovate.json`. Some very **useful features** include the following

- Scheduling
- Automerge
- Reviewers
- Grouping
- Limit open branches/PRs
- Exclude dependencies

There is the ability to define so called **"config presets"** which can be reused across different repositories

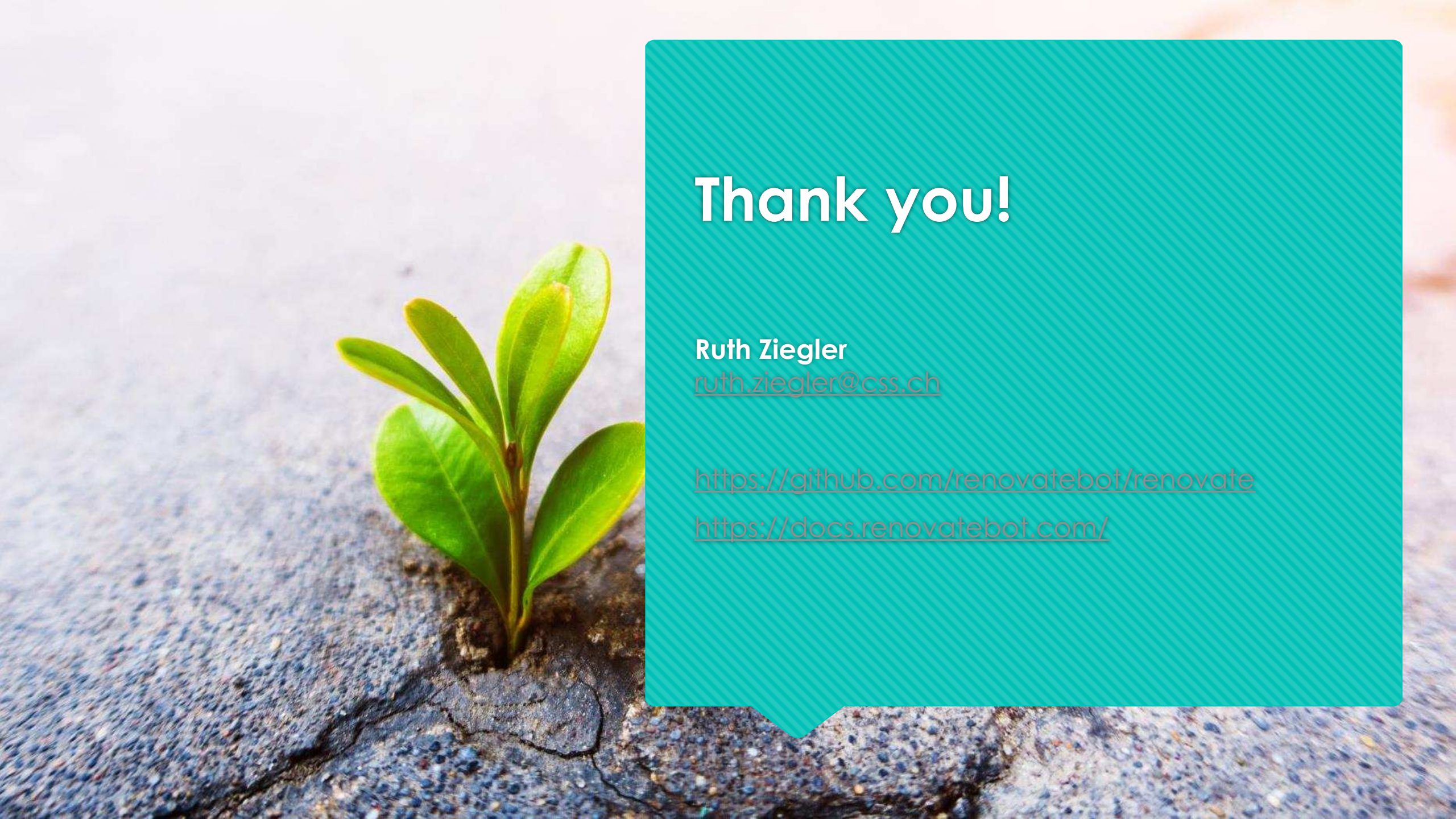


Lessons learned at DMS

- PR handling
  - To let Renovate rebase a stale PR type `rebase!` in front of PR title
  - Decline a PR will make Renovate not create it again (ie to skip a version of a dependency)
  - Delete a PR (and its branch) will cause Renovate to create it again in the next run (ie to solve a merge conflict)
- Use **automerge for bugfixes** to reduce noise
  - `"automergeType": "branch"`: Don't create PR, merge branch directly
- **Reduce** the use of **grouping** not to 'block' other dependencies from updating when one in group fails
- Define a **responsible person in the team** for the generated PRs

Renovate

Questions?



Thank you!

Ruth Ziegler
ruth.ziegler@css.ch

https://github.com/renovatebot/renovate

https://docs.renovatebot.com/