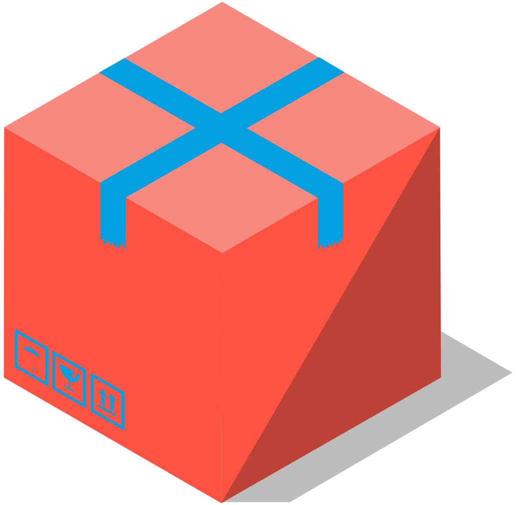
Package management

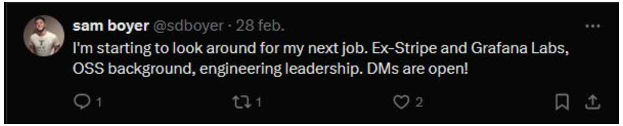
Based on:

SE Radio 489: Sam Boyer on Package Management



Alberto Guerra Rodas
Ángel Macías Rodríguez
Pedro Limeres Granado
Sergio Truébano Robles

Sam Boyer



sam boyer @sdboyer · 28 feb. ···

I'm starting to look around for my next job. Ex-Stripe and Grafana Labs, OSS background, engineering leadership. DMs are open!

stripe

Grafana

TABLE OF CONTENTS

01

PACKAGES

02

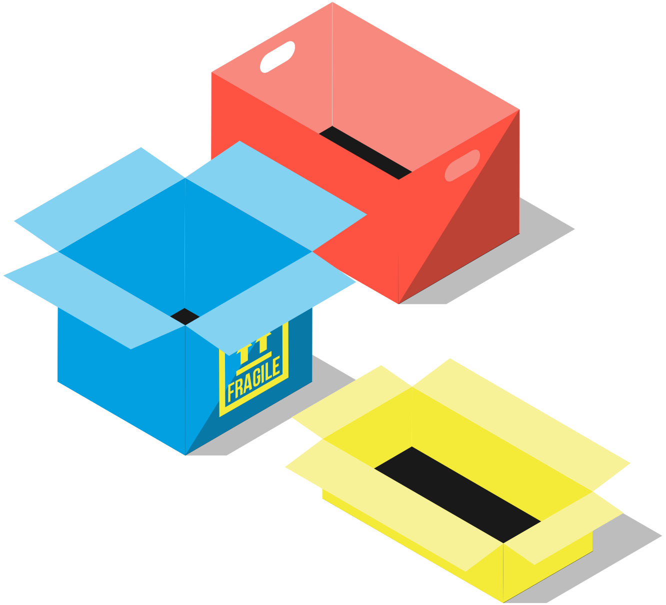
PACKAGE MANAGERS

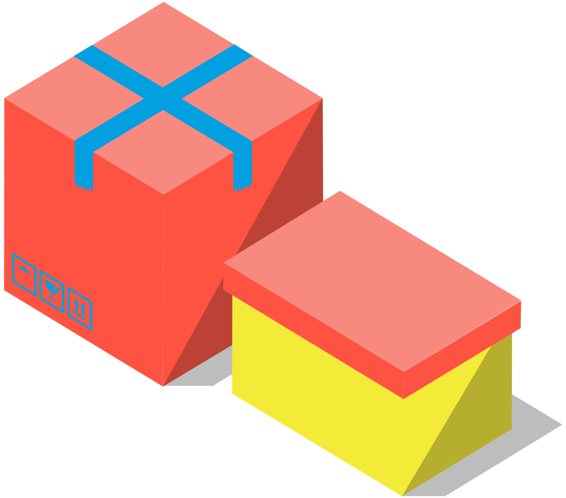
03

DEPENDENCIES

01

Packages

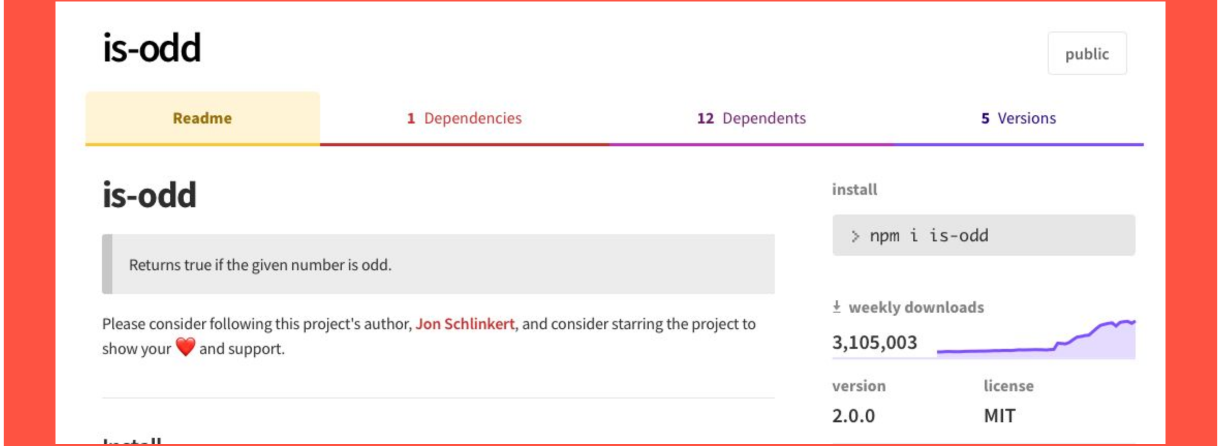




What is a package?

- 🟨 Element collection with name and context
- 🟦 Challenging to define

Package Example



is-odd

public

Readme | 1 Dependencies | 12 Dependents | 5 Versions

is-odd

> Returns true if the given number is odd.

Please consider following this project's author, Jon Schlinkert, and consider starring the project to show your ❤️ and support.

install

```
> npm i is-odd
```

weekly downloads

3,105,003

version

2.0.0

license

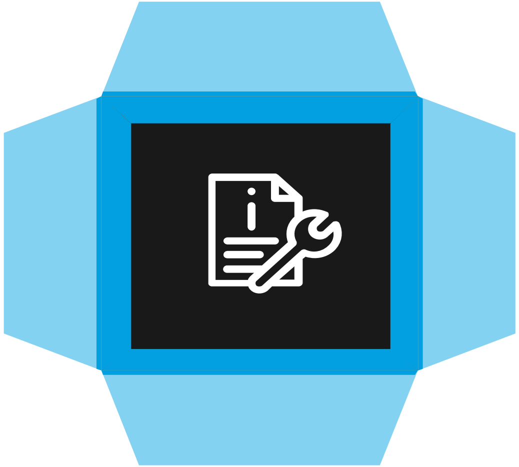
MIT

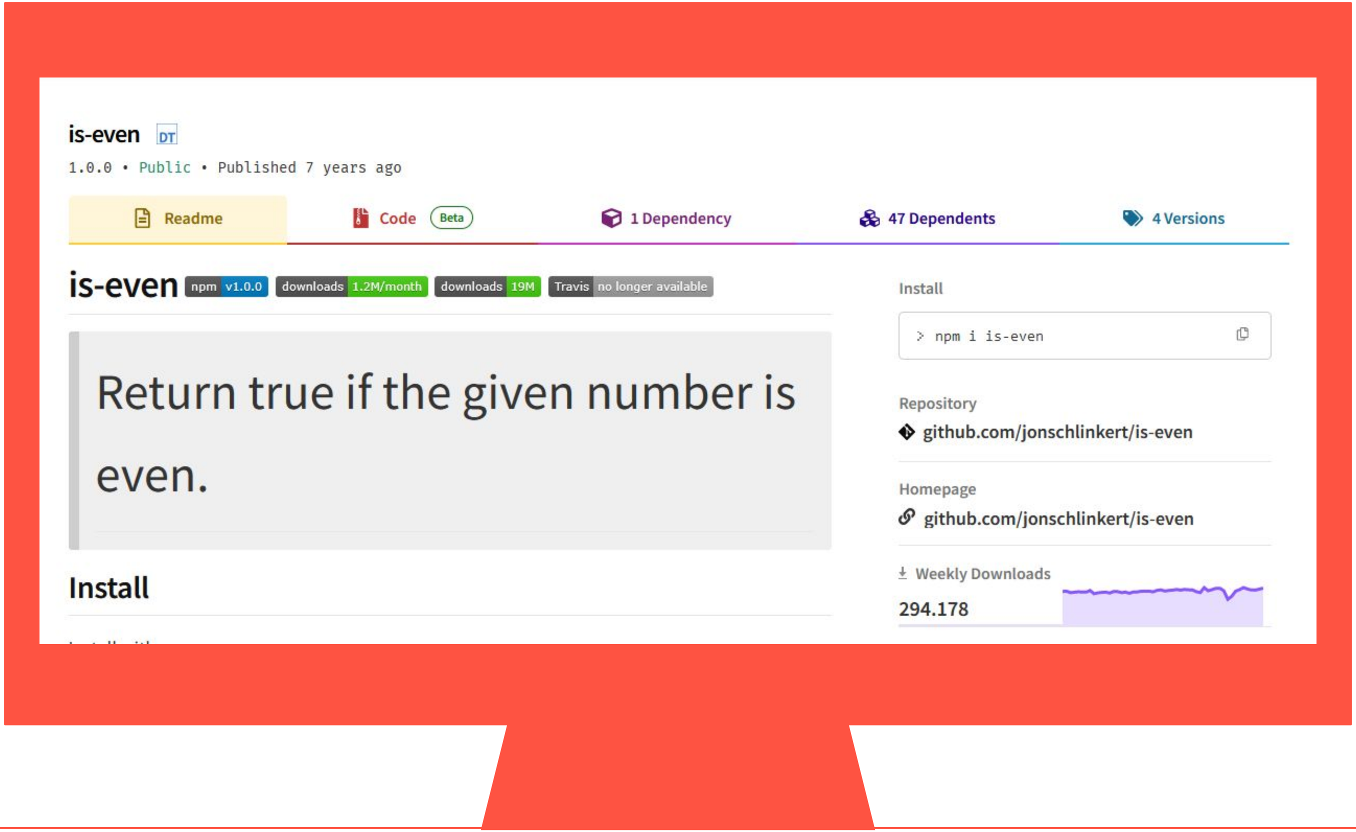
Packages & Metadata

Name: is-odd

Version: 2.0.0

Dependencies: ....





is-even

1.0.0 • Public • Published 7 years ago

is-even

> Return true if the given number is even.

Install

Install

```
> npm i is-even
```

Repository

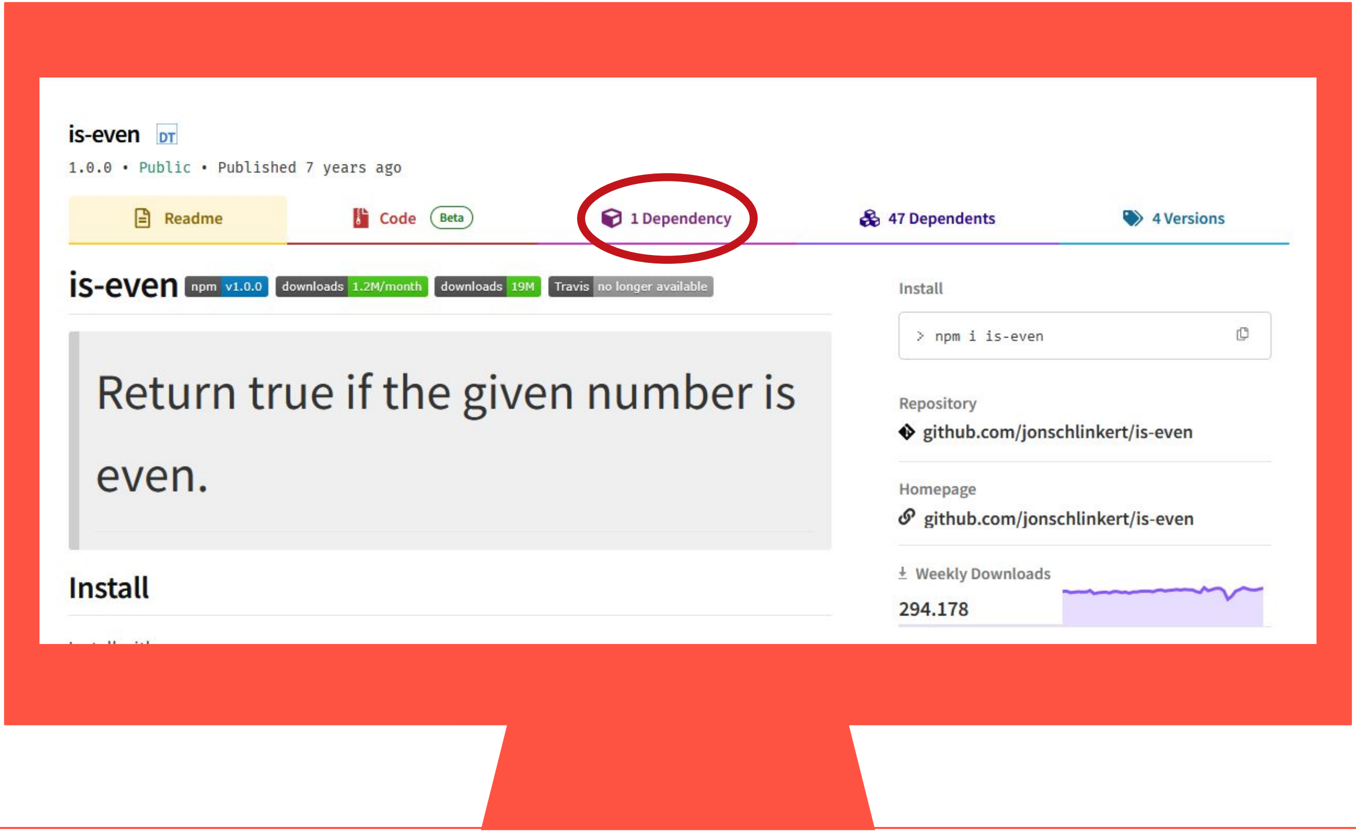
github.com/jonschlinkert/is-even

Homepage

github.com/jonschlinkert/is-even

Weekly Downloads

294.178



is-even DT

1.0.0 • Public • Published 7 years ago

Readme | Code Beta | 1 Dependency | 47 Dependents | 4 Versions

is-even npm v1.0.0 downloads 1.2M/month downloads 19M Travis no longer available

> Return true if the given number is even.

Install

Install

```
> npm i is-even
```

Repository

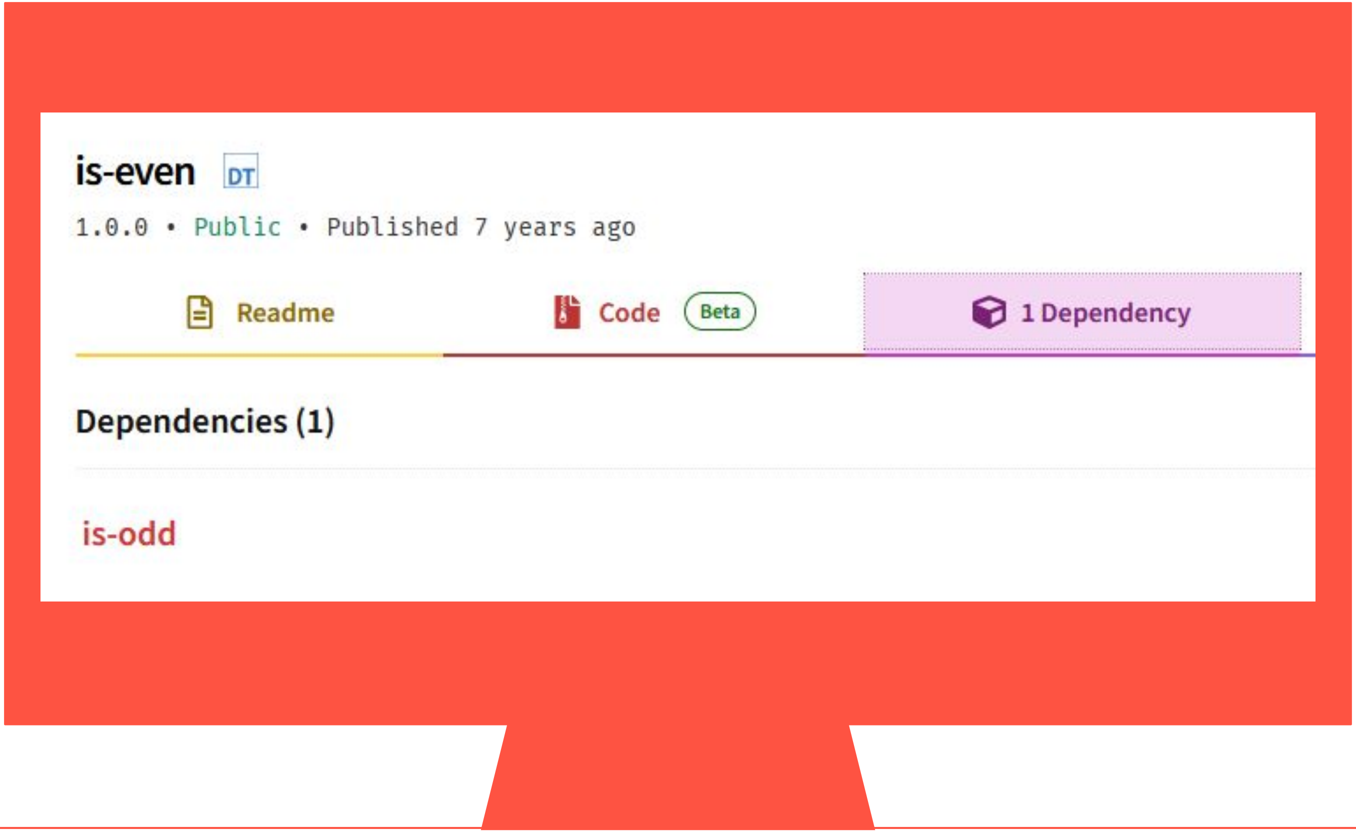
github.com/jonschlinkert/is-even

Homepage

github.com/jonschlinkert/is-even

Weekly Downloads

294.178



is-even

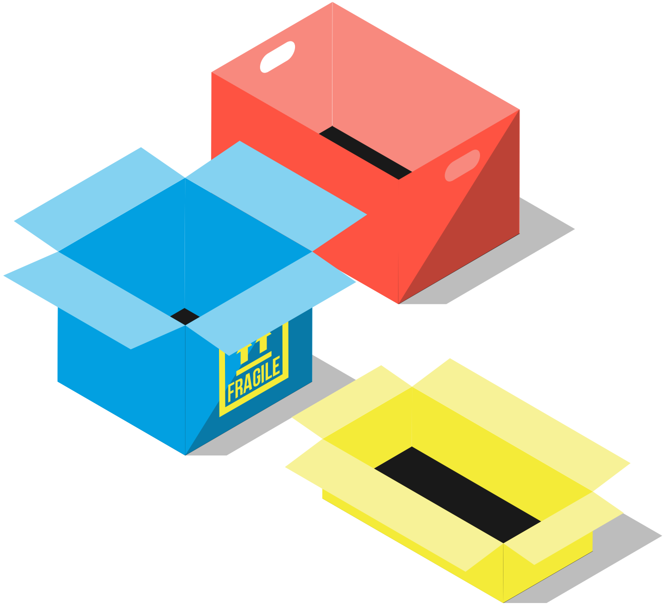
1.0.0 • Public • Published 7 years ago

Dependencies (1)

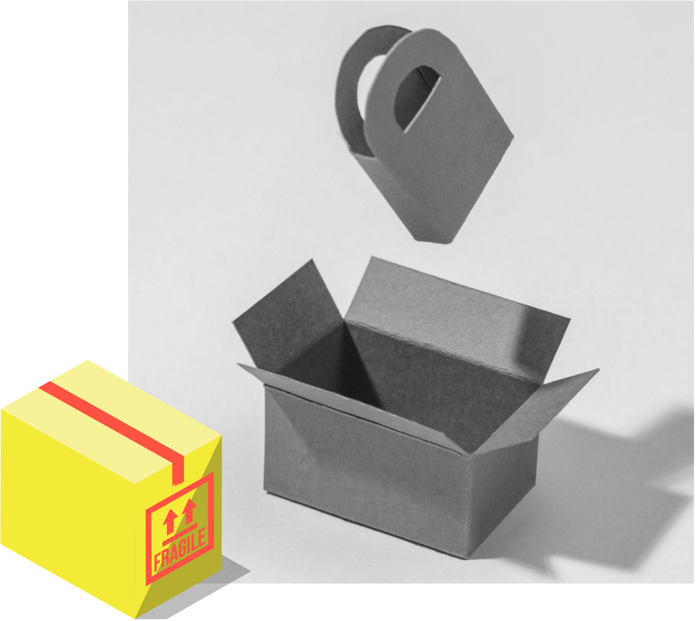
is-odd

02

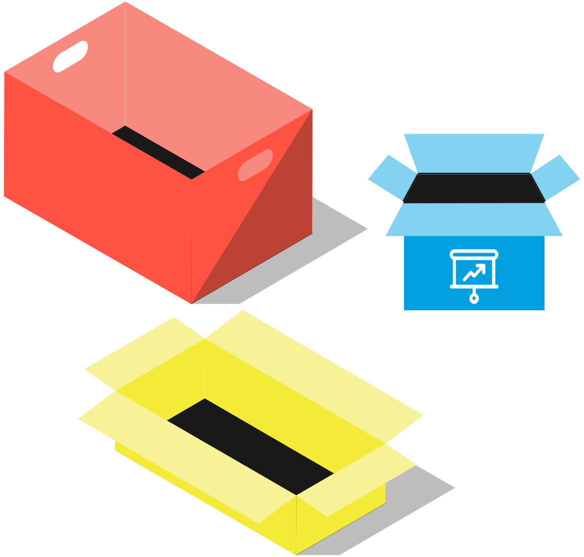
Package managers



What is a Package Manager



- Automation Tools
- Uniformed Systems



Package Manager trends

🟨 Manager 🤝 Toolchain

🟦 Same language

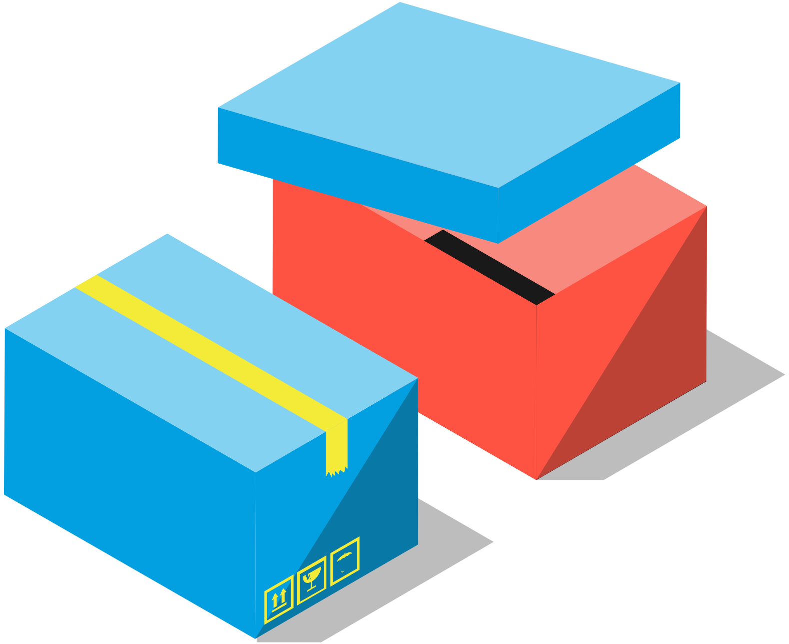
Package manager operations

⇊

Package retrieval

⇈

Package publishing

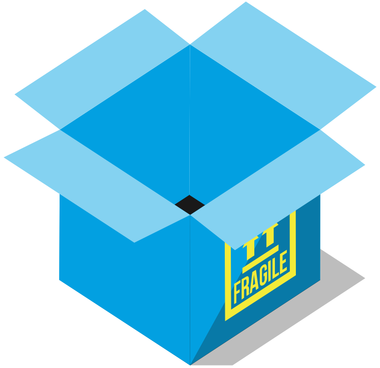


Validity process

01 Repositories

02 Name resolution

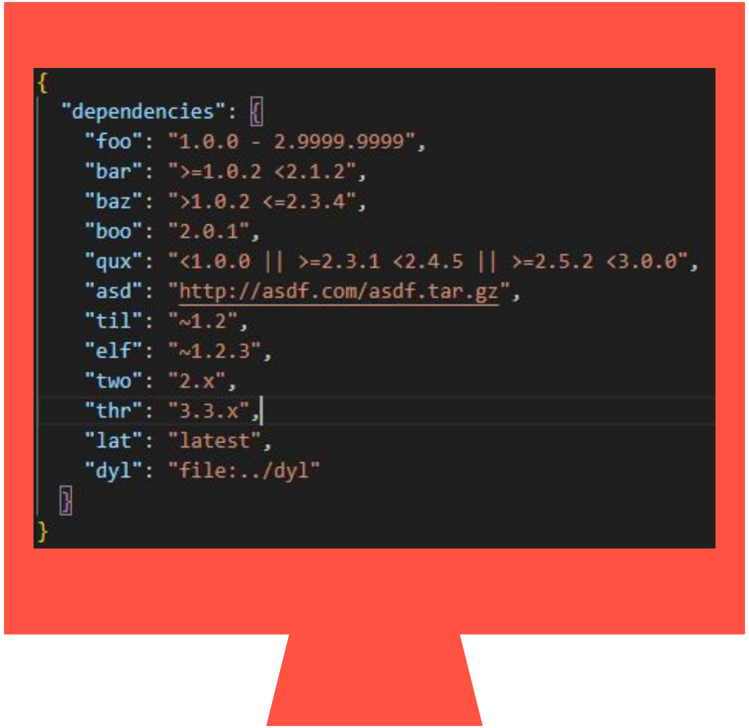
03 Identity verification



Configuration

Metadata file

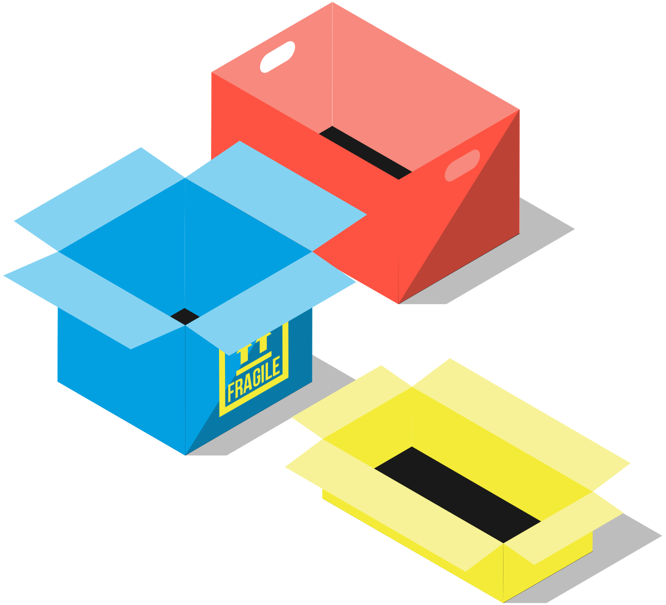
Command-line



```
{
  "dependencies": {
    "foo": "1.0.0 - 2.9999.9999",
    "bar": ">=1.0.2 <2.1.2",
    "baz": ">1.0.2 <=2.3.4",
    "boo": "2.0.1",
    "qux": "<1.0.0 || >=2.3.1 <2.4.5 || >=2.5.2 <3.0.0",
    "asd": "http://asdf.com/asdf.tar.gz",
    "til": "~1.2",
    "elf": "~1.2.3",
    "two": "2.x",
    "thr": "3.3.x",
    "lat": "latest",
    "dyl": "file:../dyl"
  }
}
```

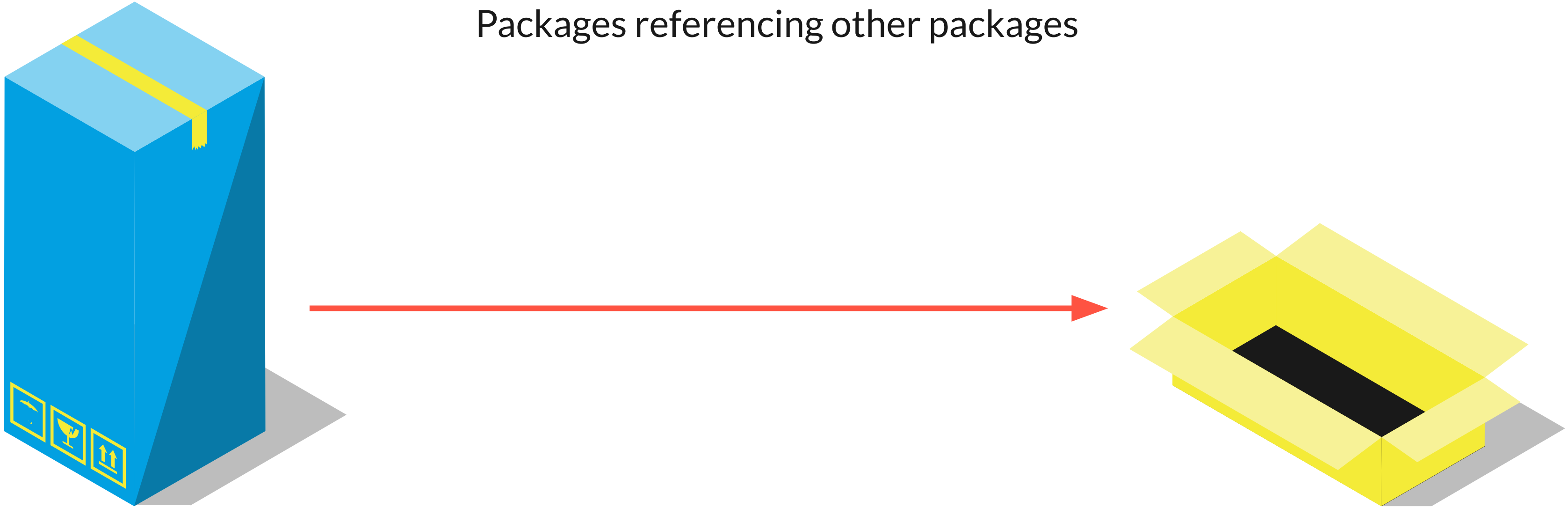
03

Dependencies

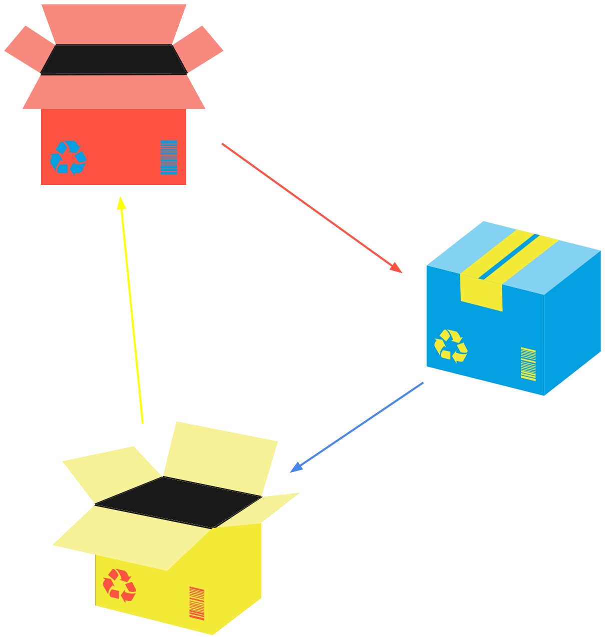


Dependencies

Packages referencing other packages



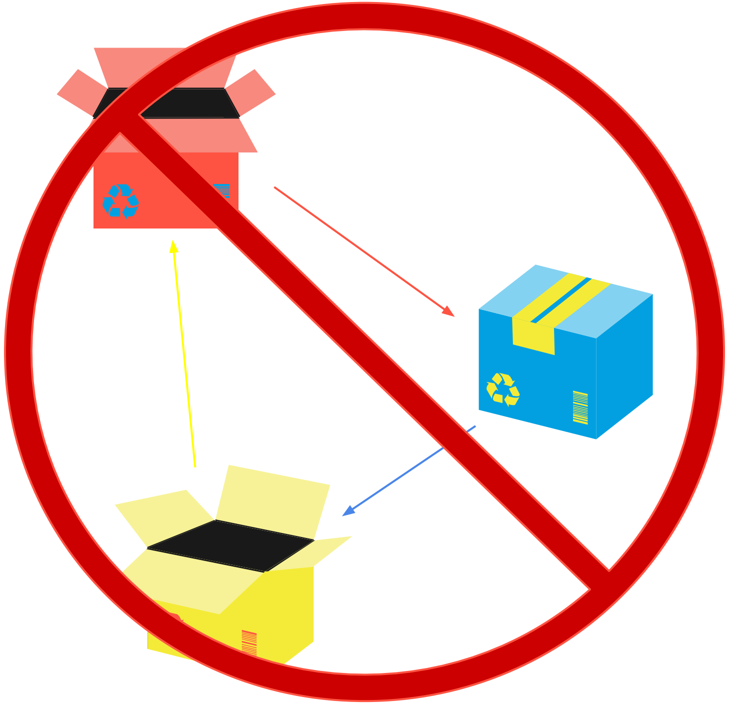
What is a cycle?



🟨 Simple closed path, with no clear beginning or end

🟦 In a graph, when we can see a path through the nodes

How can we avoid them?



🟨 Generally, we cannot avoid these cycles when working with packages

🟥 Most package managers allow these types of cycles with packages

Versions problem

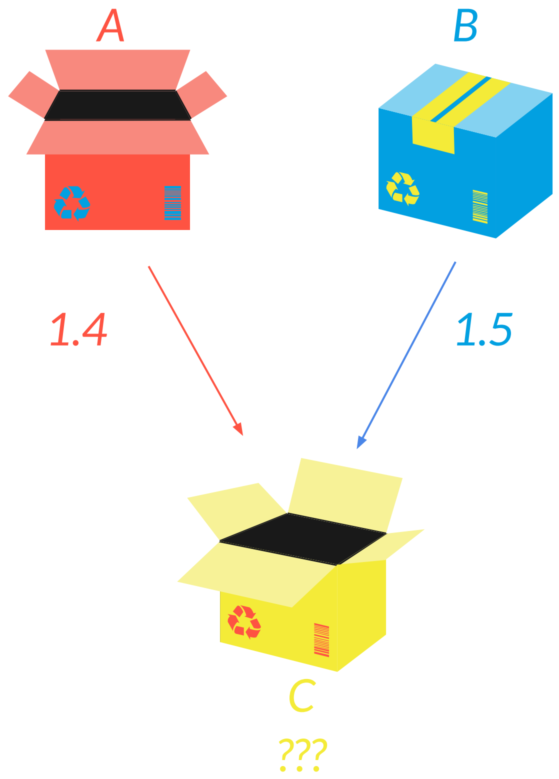
🟥 Package A depends on C

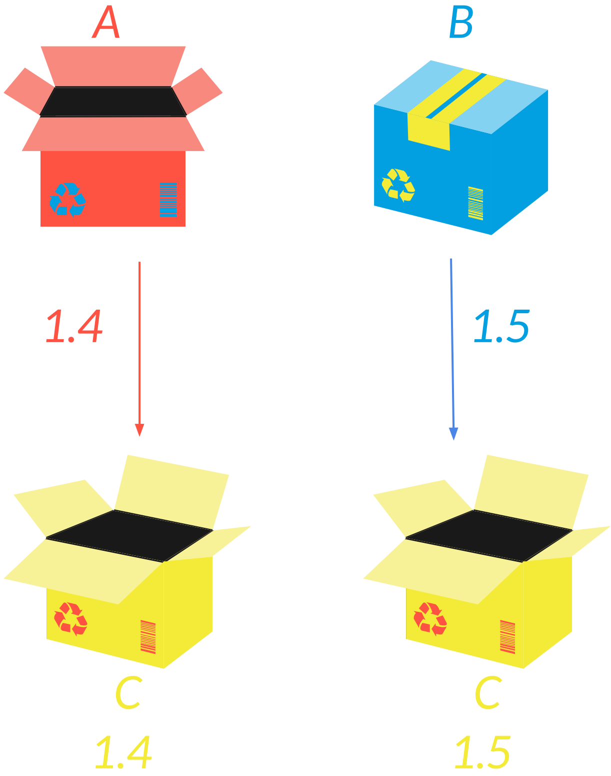
🟨 Package also B depends on C

🟦 A accepts version 1.4

🟨 B accepts version 1.5

🟥 Which version will C need?

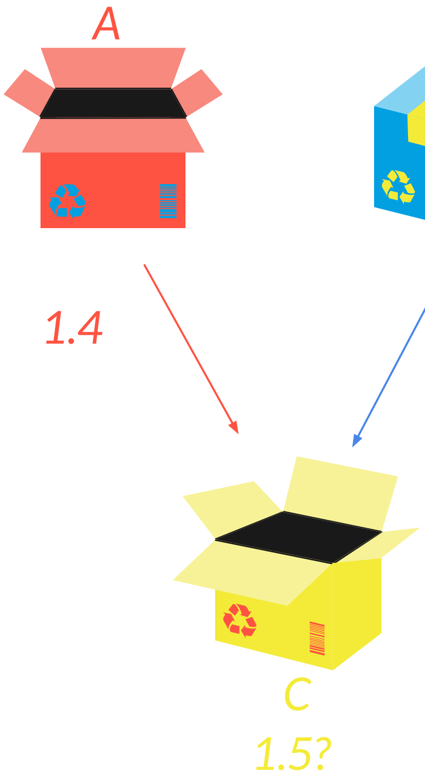




Possible solutions

🟦 In dynamic languages, the manager can decide with more freedom

🟨 A usual approach is to duplicate the C package, each one with different versions



Possible solutions

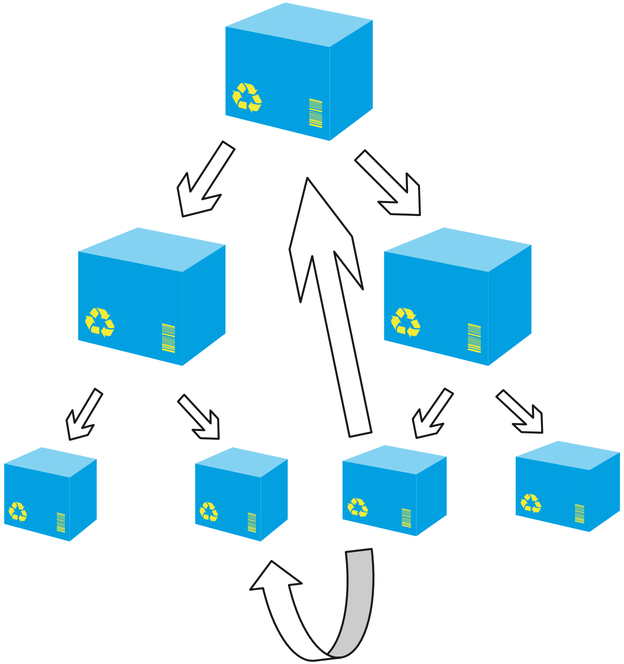
🟨 In statically typed languages, the usual approach is to compromise versions

🟥 For type checkers not to explode, only one version of package is required

Dependency Limbo

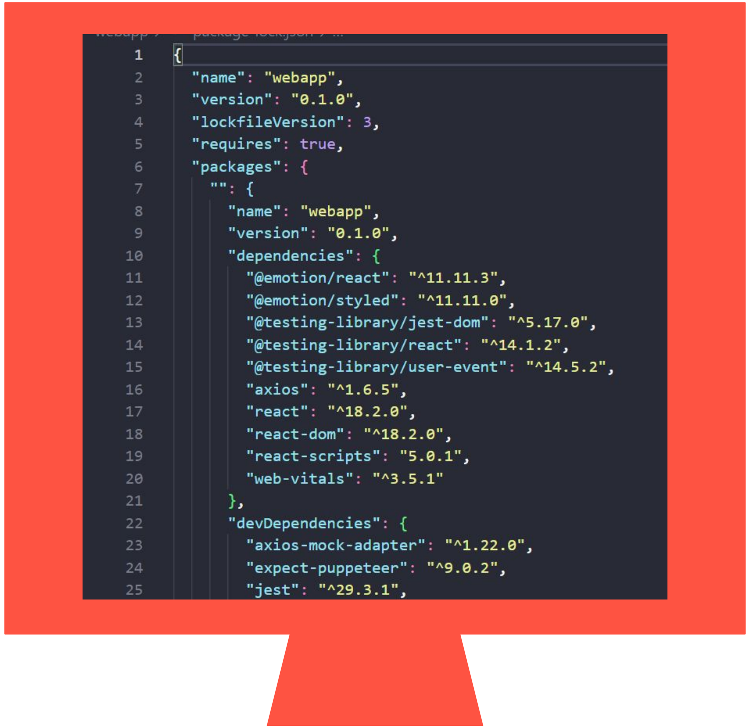
- There is a problem with versions in packages
- We are NOT SURE if our code is going to compile or if it is correct

Dependency Hell



🟦 Packages depend on other packages. What if a package is updated?

🟨 Override approach.

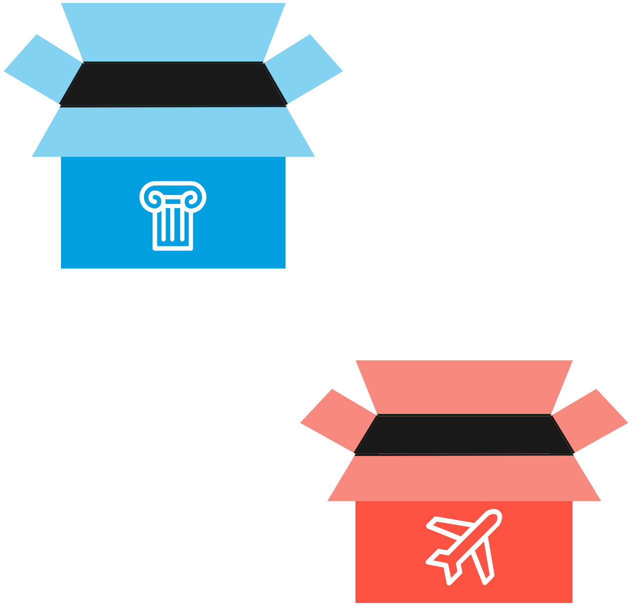


```
webapp > package-lock.json > ...
{
  "name": "webapp",
  "version": "0.1.0",
  "lockfileVersion": 3,
  "requires": true,
  "packages": {
    "": {
      "name": "webapp",
      "version": "0.1.0",
      "dependencies": {
        "@emotion/react": "^11.11.3",
        "@emotion/styled": "^11.11.0",
        "@testing-library/jest-dom": "^5.17.0",
        "@testing-library/react": "^14.1.2",
        "@testing-library/user-event": "^14.5.2",
        "axios": "^1.6.5",
        "react": "^18.2.0",
        "react-dom": "^18.2.0",
        "react-scripts": "5.0.1",
        "web-vitals": "^3.5.1"
      },
      "devDependencies": {
        "axios-mock-adapter": "^1.22.0",
        "expect-puppeteer": "^9.0.2",
        "jest": "^29.3.1",
```

Lock File

- We can store the version and dependencies.
- Selection algorithms.

Package Loading



🟦 Statically incorporated libraries (C languages).

🟥 Dynamically loaded libraries (Python/Ruby ...).