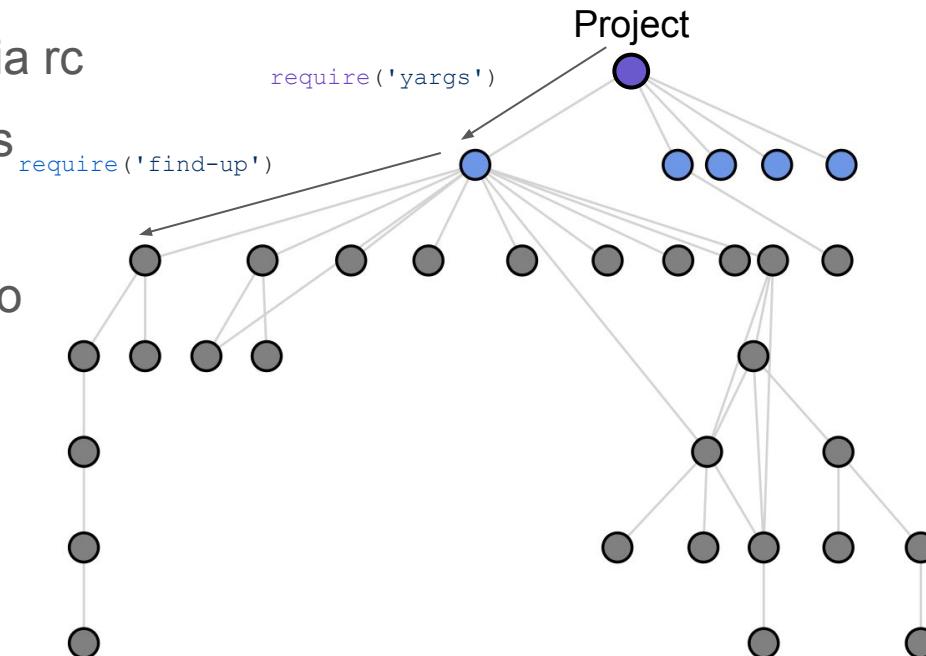


REM: Visualizing the Ripple Effect on Dependencies Using Metrics of Health

Zhe Chen, Daniel German
University of Victoria, Canada
September 2020

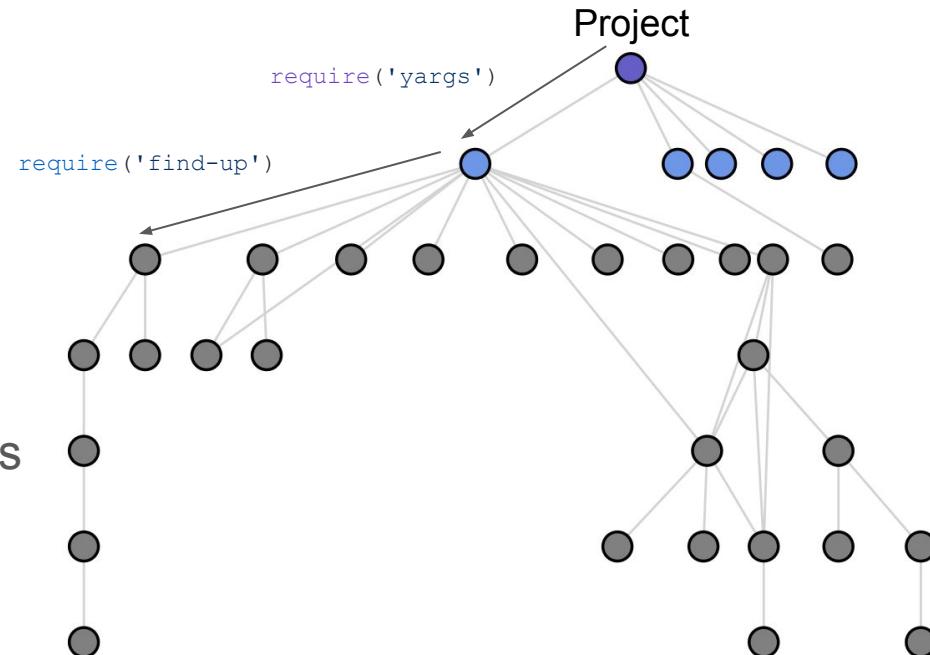
Scenario

- Build a project - configurable via rc
 - Using external dependencies is requi common
 - These dependencies could also rely on other dependencies



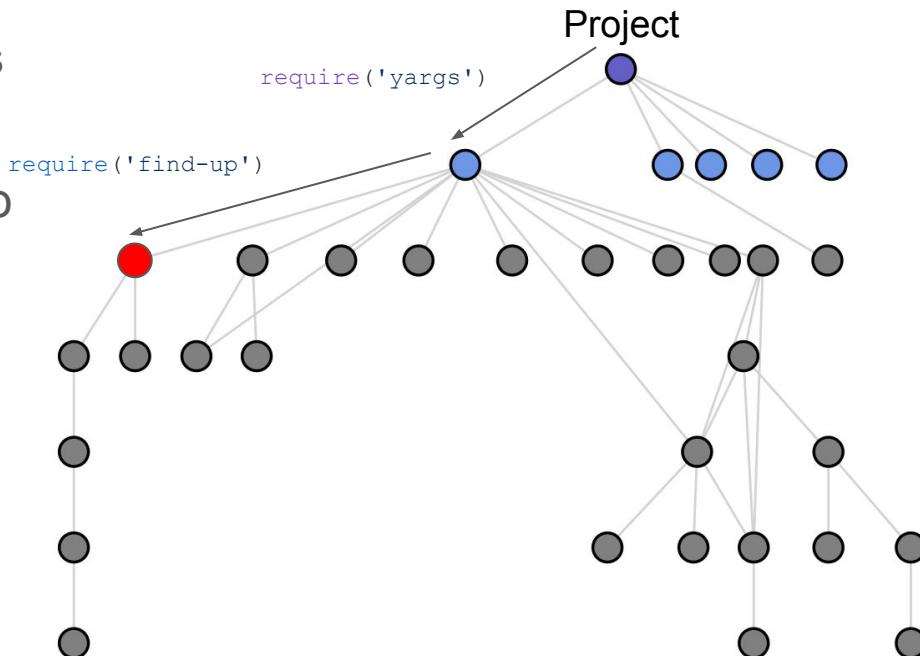
Scenario - Dependency Graph

- To describe software reuse
 - Hierarchical layout - top requires bottom
 - Direct dependency: software used by project
 - Transitive dependency: software used by dependencies of project



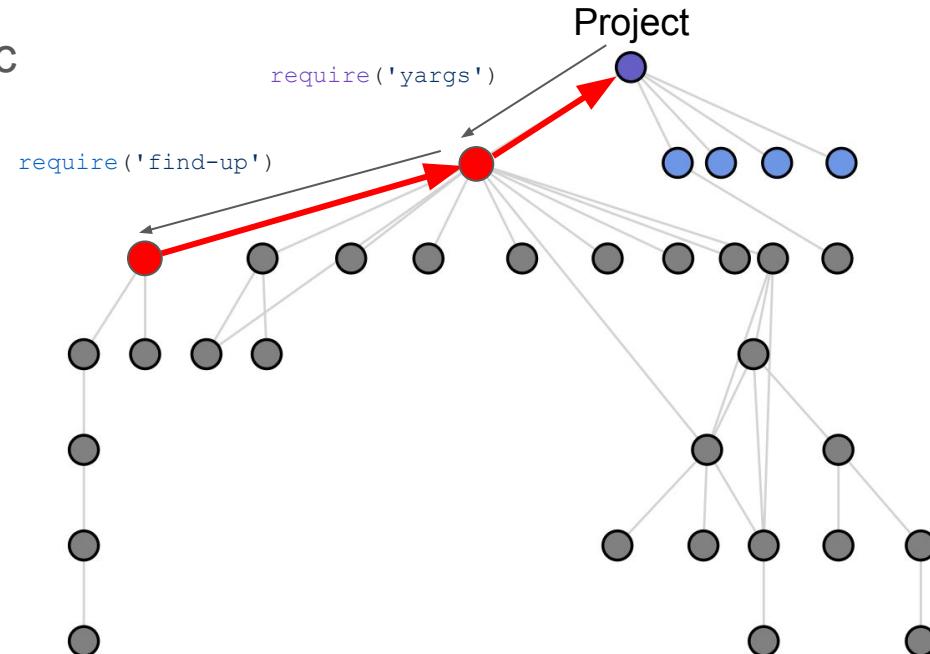
Scenario

- Using external dependencies is common
- These dependencies could also rely on other dependencies
- What if one of them is broken?



Scenario - Ripple Effect

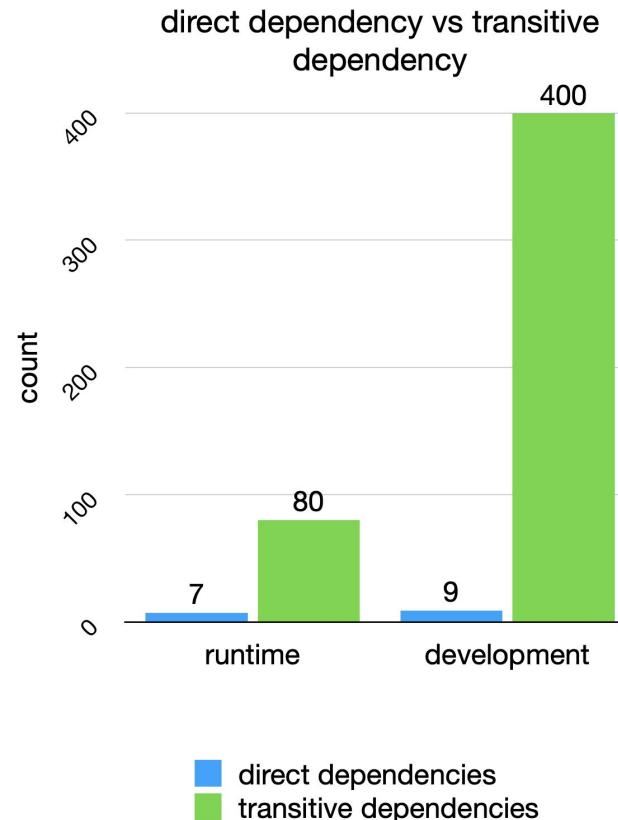
- Propagation from a problematic dependency to the software application
- Any dependency (direct or transitive) can break the software application



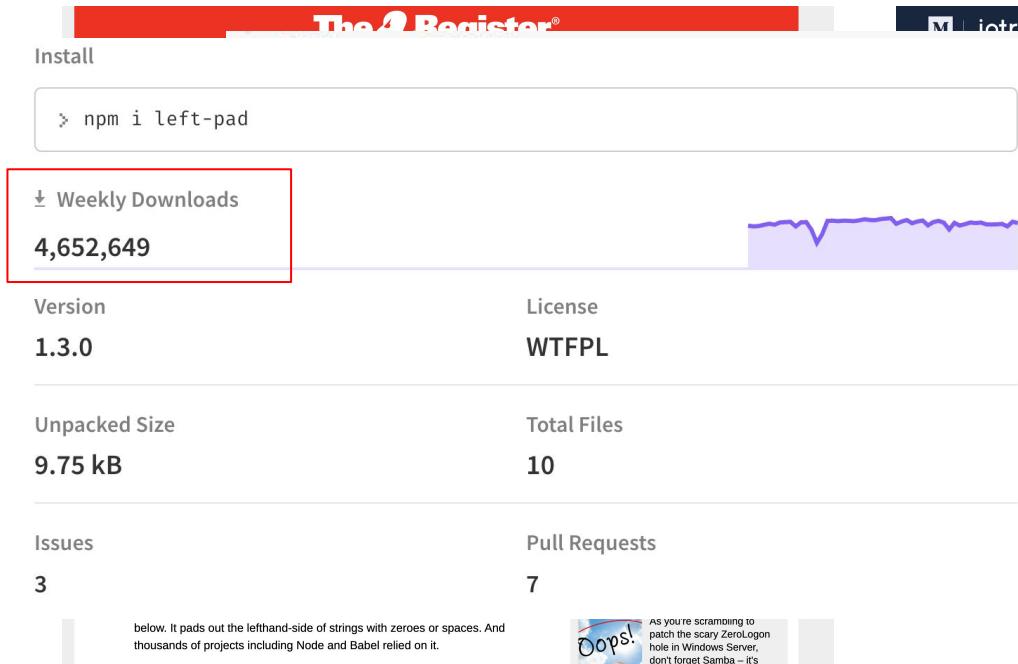
Transitive Dependency

- hidden from application developers
- hard to track

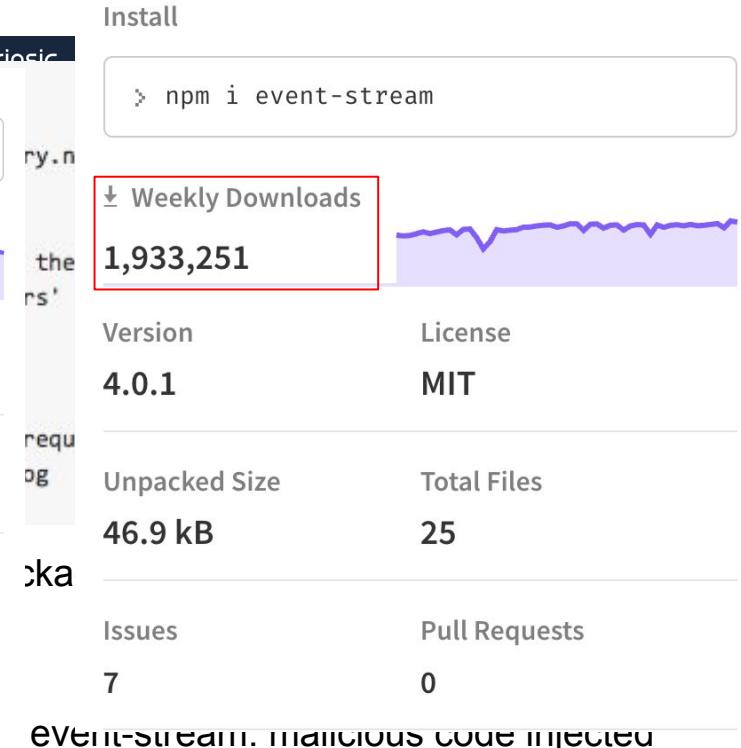
Collected dependency data on 50,000+ GitHub NPM applications:
huge number of transitive dependencies could be hiding in applications with small number of direct dependencies



Failures in Transitive Dependencies



left-pad: removal of a package



How NPM shows Problem

- Node Package Manager (NPM) for JavaScript/Node.js
- Overwhelming NPM build message
- unhelpful warning message

```
e.js
npm WARN deprecated graceful-fs@1.1.14: please upgrade to graceful-fs 4 for compatibility with current and future versions of Node.js
npm WARN deprecated npmconf@2.1.1: this package has been reintegrated into npm and is now out of date with respect to npm
npm WARN deprecated request@2.67.0: request has been deprecated, see https://github.com/request/request/issues/3142
npm WARN deprecated request@2.81.0: request has been deprecated, see https://github.com/request/request/issues/3142
npm WARN deprecated request@2.88.2: request has been deprecated, see https://github.com/request/request/issues/3142
npm WARN deprecated node-uuid@1.4.8: Use uuid module instead
npm WARN deprecated hoek@2.16.3: This version has been deprecated in accordance with the hapi support policy (hapi.im/support). Please upgrade to the latest version to get the best features, bug fixes, and security patches. If you are unable to upgrade at this time, paid support is available for older versions (hapi.im/commercial).
npm WARN deprecated hawk@1.1.1: This module moved to @hapi/hawk. Please make sure to switch over as this distribution is no longer supported and may contain bugs and critical security issues.
npm WARN deprecated minimatch@0.3.0: Please update to minimatch 3.0.2 or higher to avoid a RegExp DoS issue
npm WARN deprecated sntp@1.0.9: This module moved to @hapi/sntp. Please make sure to switch over as this distribution is no longer supported and may contain bugs and critical security issues.
npm WARN deprecated boom@2.10.1: This version has been deprecated in accordance with the hapi support policy (hapi.im/support). Please upgrade to the latest version to get the best features, bug fixes, and security patches. If you are unable to upgrade at this time, paid support is available for older versions (hapi.im/commercial).
npm WARN deprecated cryptiles@2.0.5: This version has been deprecated in accordance with the hapi support policy (hapi.im/support). Please upgrade to the latest version to get the best features, bug fixes, and security patches. If you are unable to upgrade at this time, paid support is available for older versions (hapi.im/commercial).
npm WARN deprecated tough-cookie@2.2.2: ReDoS vulnerability parsing Set-Cookie https://nodesecurity.io/advisories/130
npm WARN deprecated mkdirp@0.5.0: Legacy versions of mkdirp are no longer supported. Please update to mkdirp 1.x. (Note that the API surface has changed to use Promises in 1.x.)
npm WARN deprecated har-validator@4.2.1: this library is no longer supported
npm WARN deprecated chokidar@2.1.8: Chokidar 2 will break on node v14+. Upgrade to chokidar 3 with 15x less dependencies.
npm WARN deprecated har-validator@5.1.5: this library is no longer supported
npm WARN deprecated hoek@0.9.1: This version has been deprecated in accordance with the hapi support policy (hapi.im/support). Please upgrade to the latest version to get the best features, bug fixes, and security patches. If you are unable to upgrade at this time, paid support is available for older versions (hapi.im/commercial).
npm WARN deprecated boom@0.4.2: This version has been deprecated in accordance with the hapi support policy (hapi.im/support). Please upgrade to the latest version to get the best features, bug fixes, and security patches. If you are unable to upgrade at this time, paid support is available for older versions (hapi.im/commercial).
npm WARN deprecated cryptiles@2.0.2: This version has been deprecated in accordance with the hapi support policy (hapi.im/support). Please upgrade to the latest version to get the best features, bug fixes, and security patches. If you are unable to upgrade at this time, paid support is available for older versions (hapi.im/commercial).
npm WARN deprecated sntp@0.2.4: This module moved to @hapi/sntp. Please make sure to switch over as this distribution is no longer supported and may contain bugs and critical security issues.
npm WARN deprecated minimatch@0.4.0: Please update to minimatch 3.0.2 or higher to avoid a RegExp DoS issue
npm WARN deprecated circular-json@0.3.3: CircularJSON is in maintenance only, flattened is its successor.
npm WARN deprecated urix@0.1.0: Please see https://github.com/lydell/urix#deprecated
npm WARN deprecated resolve-url@0.2.1: https://github.com/lydell/resolve-url#deprecated
```



```
npm WARN deprecated minimatch@0.4.0: Please update to minimatch 3.0.2 or higher to avoid a RegExp DoS issue
npm WARN deprecated circular-json@0.3.3: CircularJSON is in maintenance only, flattened is its successor.
npm WARN deprecated urix@0.1.0: Please see https://github.com/lydell/urix#deprecated
npm WARN deprecated resolve-url@0.2.1: https://github.com/lydell/resolve-url#deprecated
```

How GitHub handles this Problem

1. Marketplace Plugin - GitHub **dependabot**
2. Via automated Pull Requests
 - a. Version bumps
 - b. Temporary dependency file to fix dependencies being used transitively
3. No visual aid on how dependencies are structured

The screenshot shows a GitHub pull request page for a repository. The title of the PR is "[Security] Bump sshpk from 1.13.1 to 1.16.1 #23". The PR has 18 commits and 1 check. The message from dependabot states: "Bumps sshpk from 1.13.1 to 1.16.1. This update includes security fixes." It lists three changes: "Vulnerabilities fixed", "Release notes", and "Commits". A compatibility section shows "compatibility 92%". Below the message, it says: "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.". The PR has a "Verified" status with 7471864 reviews. Labels "dependencies" and "security" are applied. The review section shows "All checks have passed" with 1 successful check and "This branch has no conflicts with the base branch". The sidebar on the right shows the PR has 9 approvals and 5 reviews pending. It also lists reviewers (none), assignees (none), labels (dependencies, security), projects (none), milestones (none), notifications (none), and 1 participant.

A version bump PR created by dependabot

Metrics of Health

A measurement of aspects of development process

- Scores used in ranking search results maintained by NPM
 - popularity - downloads
 - quality - presence of quality code
 - maintenance - activities
 - final (optimal) - combined
- Package deprecation flag
 - Package is no longer maintained
 - Do not recommend using the package

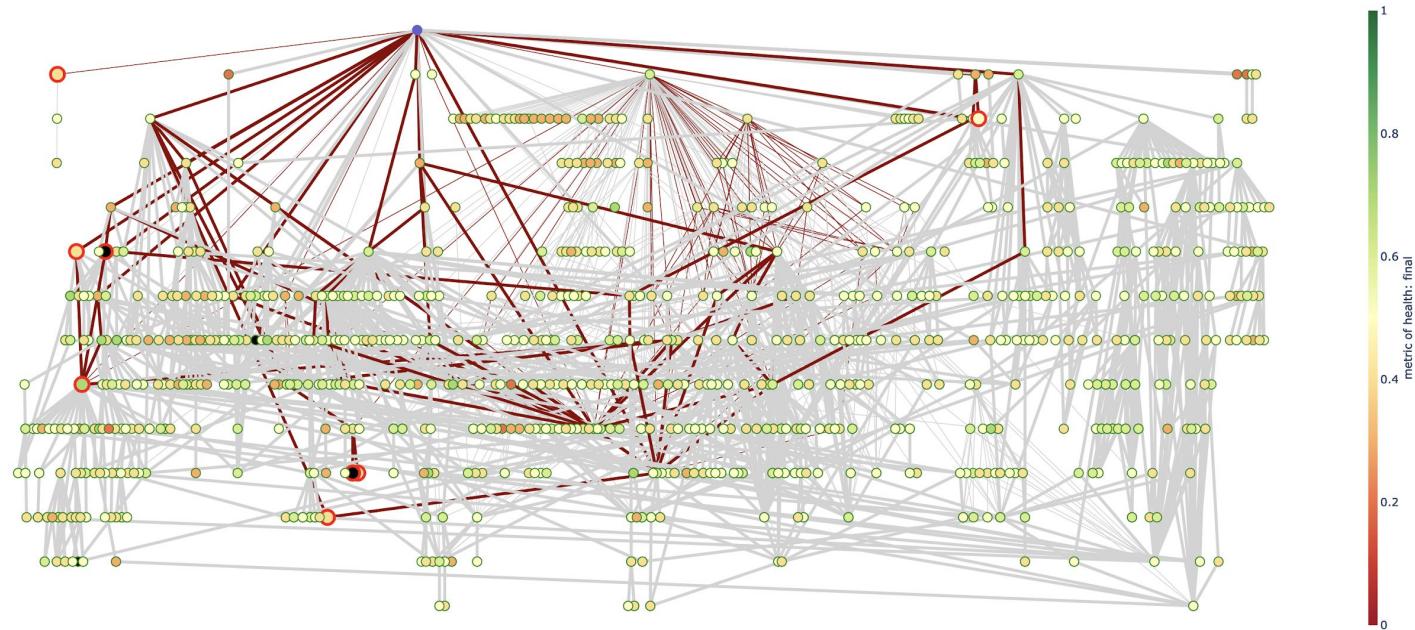
The screenshot shows the npm search interface with the query 'visualization'. The results page displays 2775 packages found, with sorting options for Optimal, Popularity, Quality, and Maintenance. The first result is 'visualization' (exact match), published by 'kaizhu' 3 years ago. The second result is 'd3'. A prominent red banner at the bottom of the results section states 'This package has been deprecated'. Below this, an 'Author message:' box contains the text 'use String.prototype.padStart()'. The package 'left-pad' is also visible at the bottom of the page.

left-pad

1.3.0 • Public • Published 2 years ago

Ripple Effect of Metrics (REM)

full REM dependency graph for adobe:brackets(master)

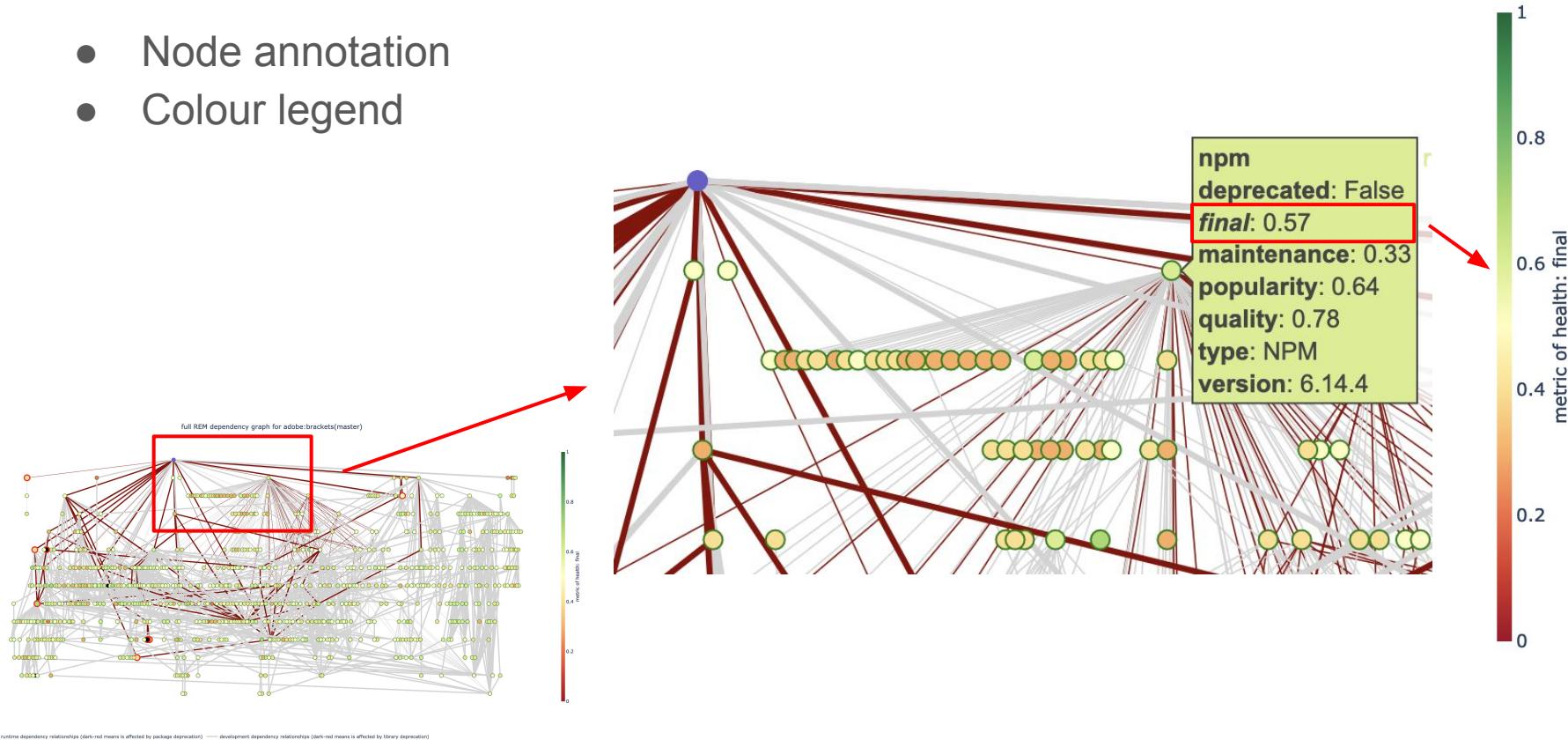


— runtime dependency relationships (dark-red means is affected by package deprecation)
● runtime dependencies (red outline means deprecation)

— development dependency relationships (dark-red means is affected by library deprecation)
● development dependencies (red outline means deprecation)

REM - Metrics of Health

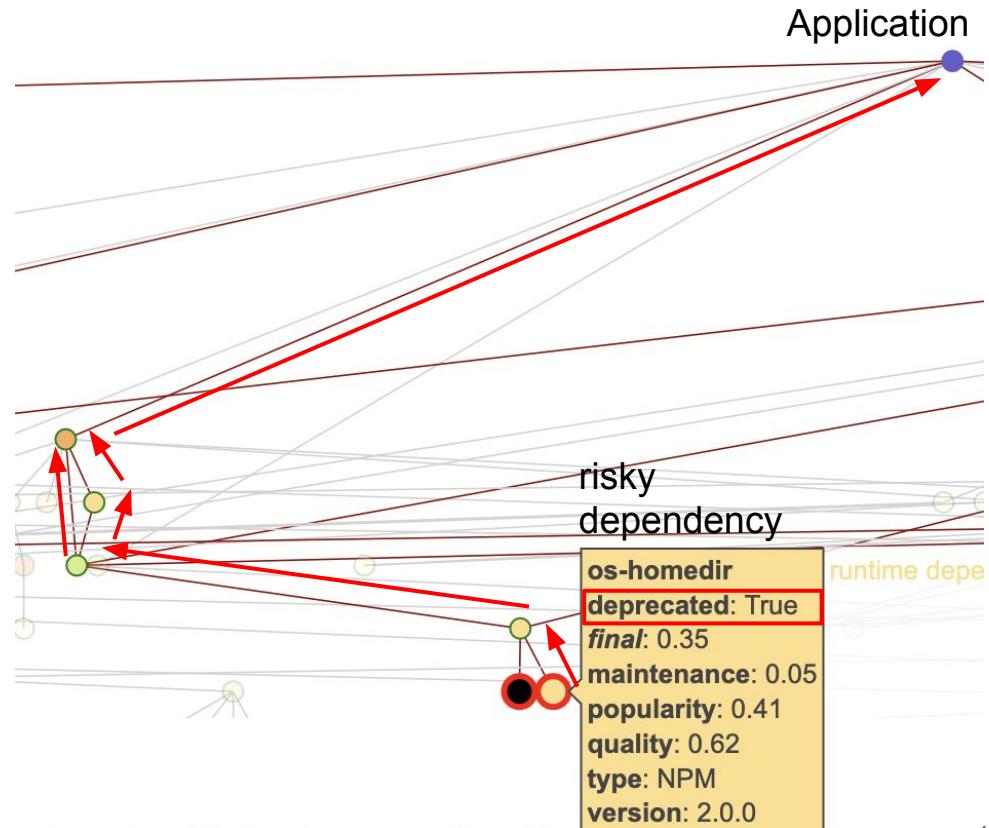
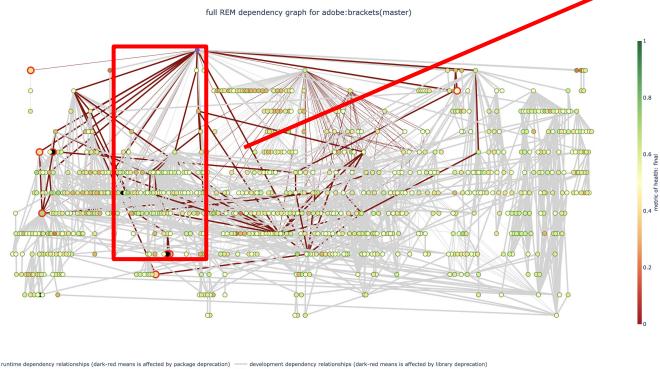
- Node annotation
- Colour legend



REM - Ripple Effect

Risky dependency to application root

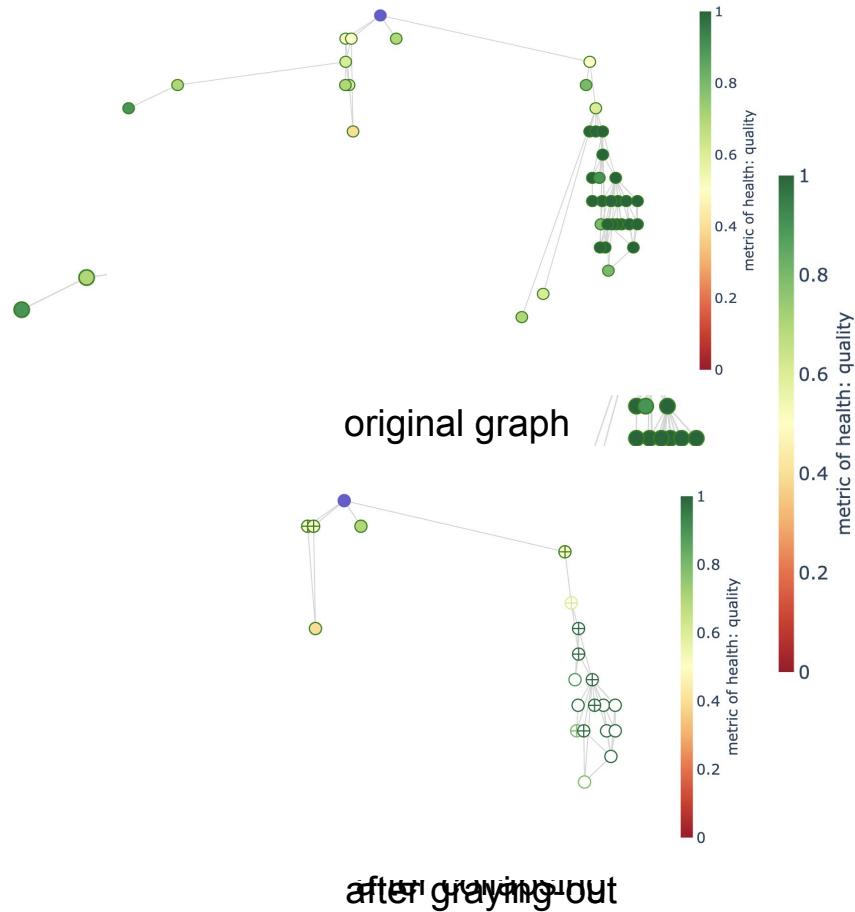
- Ripple-Effect Metric: node outline
- Ripple-Effect Path: affected edge



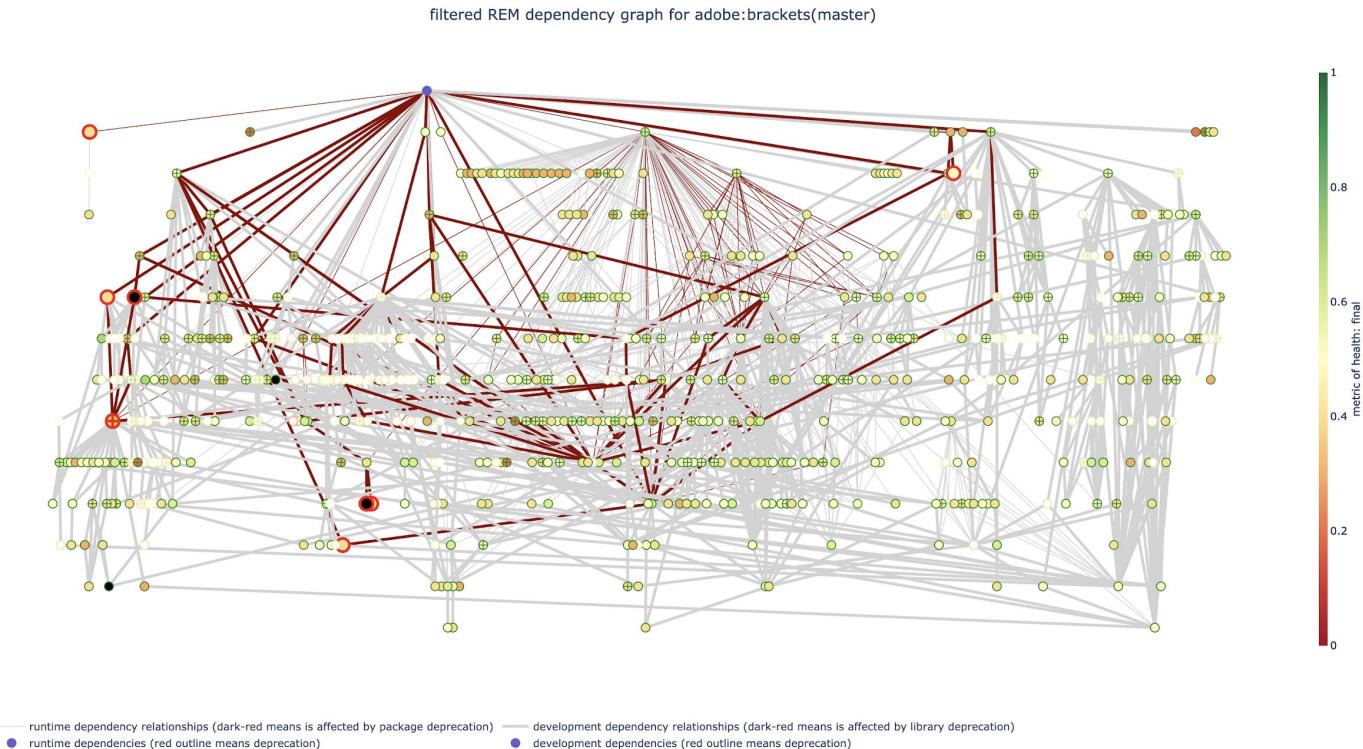
REM - Filtering

Reduce the number of nodes to highlight those considered more risky

1. Collapsing - nodes healthier than parent nodes
2. Graying-out - nodes healthier than ancestors in direct dependency nodes



REM - Filtering



DEMO

turingmachine.org/rem_demo

REM: Visualizing the Ripple Effect on Dependencies Using Metrics of Health

