



Mahidol University
Faculty of Information
and Communication Technology



SEE TO BELIEVE: Using Visualization to Motivate Updating Third-party Dependencies



**C. Ragkhitwetsagul, V. Jarukitpipat, M. Choetkiertikul, K. Chhun, W.
Wanprasert, T. Sunetnanta, Faculty of ICT, Mahidol University, Thailand**

Raula Gaikovina Kula, NAIST, Japan



Software Engineering Laboratory
Graduate School of Information Science
Nara Institute of Science and Technology



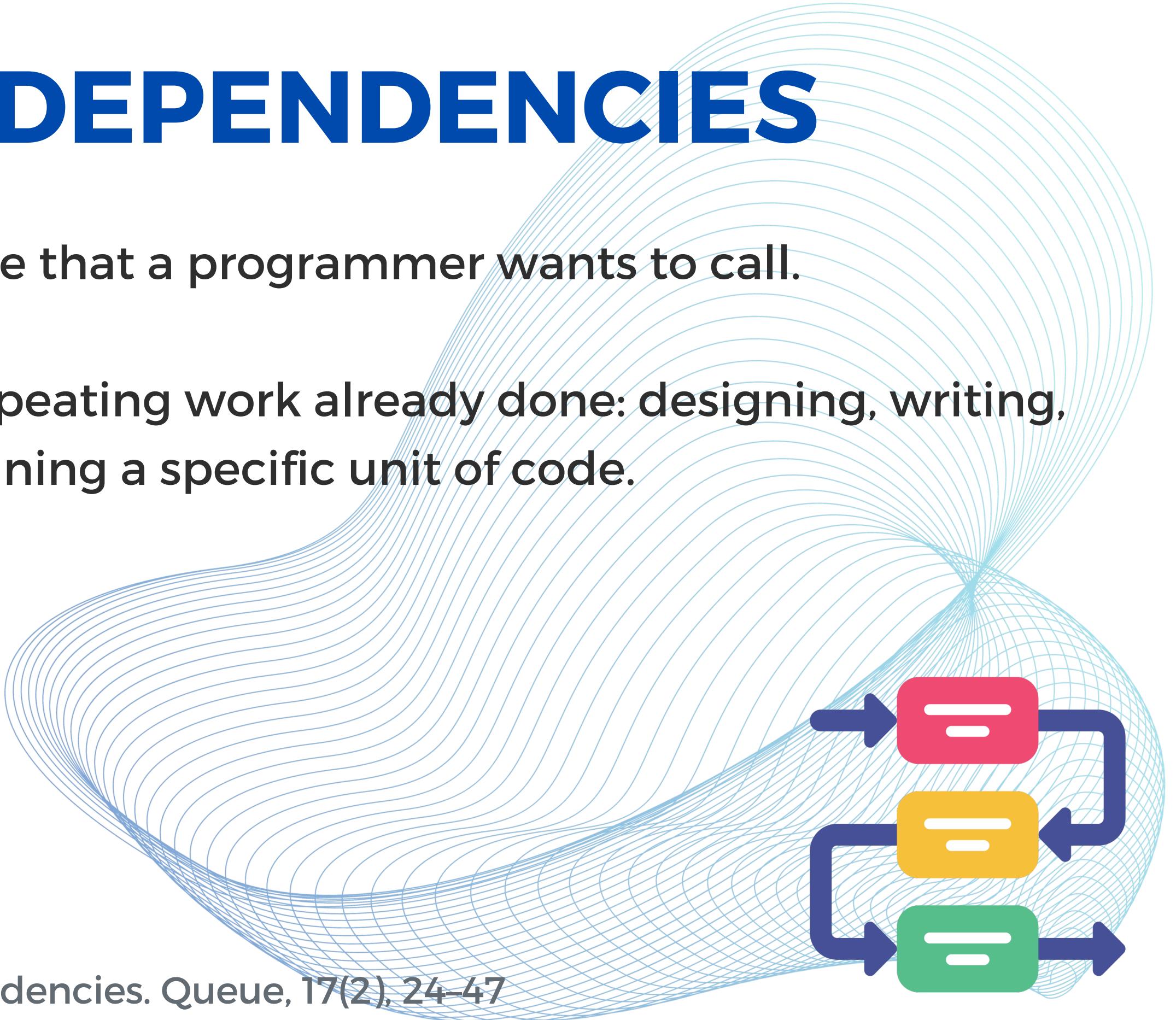
JCSSE 2024, 19-21 July 2024



THIRD-PARTY DEPENDENCIES

A **dependency** is additional code that a programmer wants to call.

Adding a dependency avoids repeating work already done: designing, writing, testing, debugging, and maintaining a specific unit of code.





master ▾

mocha / package.json

Code

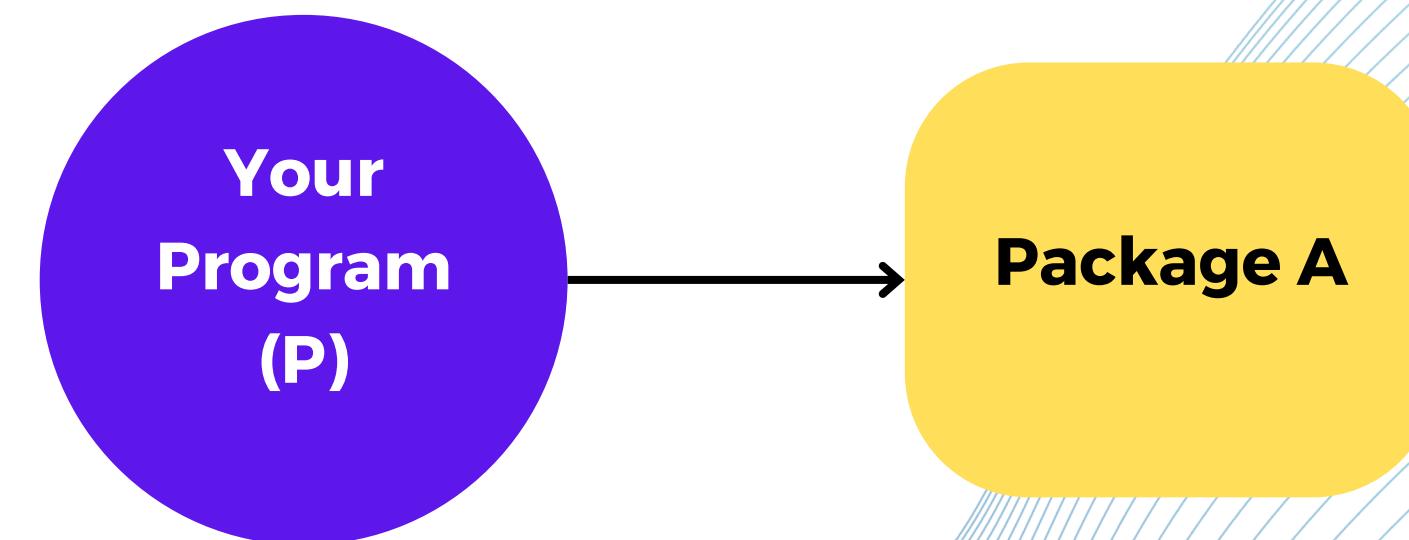
Blame

171 lines (171 loc) · 4.44 KB

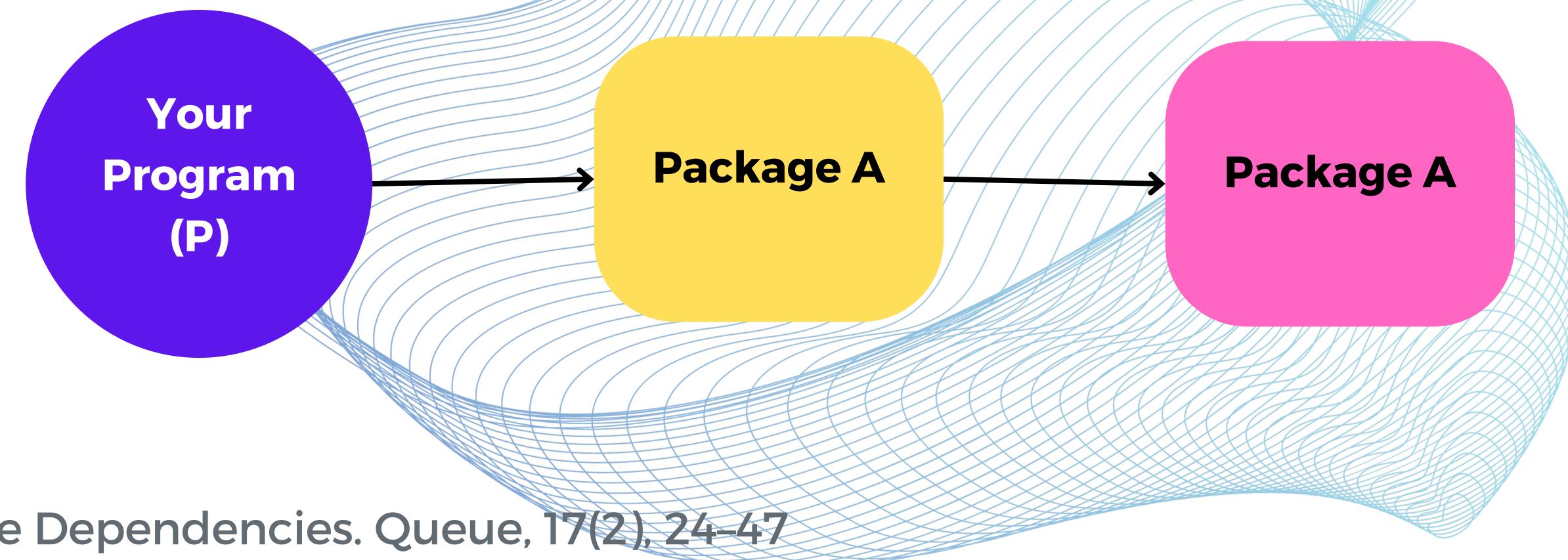
```
52      },
53      "dependencies": {
54        "ansi-colors": "4.1.1",
55        "browser-stdout": "1.3.1",
56        "chokidar": "^3.5.3",
57        "debug": "4.3.4",
58        "diff": "5.0.0",
59        "escape-string-regexp": "4.0.0",
60        "find-up": "5.0.0",
61        "glob": "8.1.0",
62        "he": "1.2.0",
63        "js-yaml": "4.1.0",
64        "log-symbols": "4.1.0",
65        "minimatch": "5.0.1",
66        "ms": "2.1.3",
67        "serialize-javascript": "6.0.0",
68        "strip-json-comments": "3.1.1",
69        "supports-color": "8.1.1",
70        "workerpool": "6.2.1",
71        "yargs": "16.2.0",
72        "yargs-parser": "20.2.4",
73        "yargs-unparser": "2.0.0"
74      },
```

TWO TYPES OF DEPENDENCIES

Direct dependency:
 $(P \rightarrow A)$



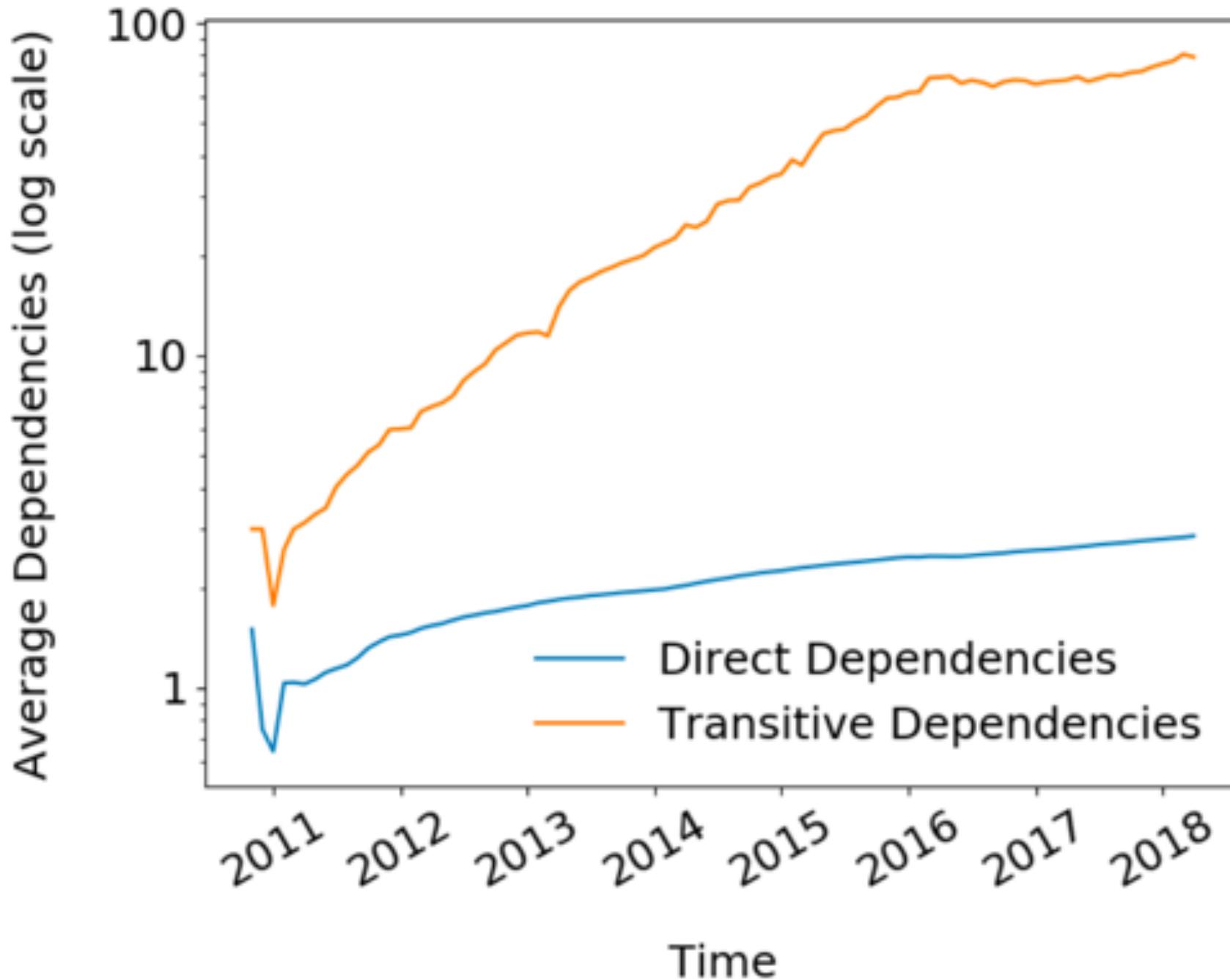
Transitive dependency:
 $(P \rightarrow A \rightarrow B)$



NPM ECOSYSTEM

Node.js dependency manager **NPM** (**Node Package Manager**) provides access to more than 750,000 packages

Number of **transitive dependencies per one direct dependency** is 80.



Zimmermann et al., (2019). Small world with high risks: A study of security threats in the NPM ecosystem. Proceedings of the 28th USENIX Security Symposium, 995–1010.

DEPENDENCY VULNERABILITIES

The usage of third-party dependencies may lead to security vulnerabilities.

GitHub Advisory Database (<https://github.com/advisories>) contains a curated list of security vulnerabilities



GITHUB ADVISORY DATABASE

[≡](#) [GitHub](#) [...](#) [+](#) [-](#) [↻](#) [⟳](#) [☰](#) [👤](#)

GitHub Advisory Database

Security vulnerability database inclusive of CVEs and GitHub originated security advisories from the world of open source software.

GitHub reviewed advisories

	All reviewed	19,314
Composer	3,956	
Erlang	29	TinyMCE Cross-Site Scripting (XSS) vulnerability using noneditable-regexp option Moderate
GitHub Actions	16	<small>CVE-2024-38356 was published for TinyMCE (Composer) 15 hours ago</small>
Go	1,740	TinyMCE Cross-Site Scripting (XSS) vulnerability using noscript elements Moderate
Maven	4,967	<small>CVE-2024-38357 was published for TinyMCE (Composer) 15 hours ago</small>
npm	3,507	socket.io has an unhandled 'error' event High
NuGet	609	<small>CVE-2024-38355 was published for socket.io (npm) 15 hours ago</small>
pip	3,064	curve25519-dalek has timing variability in `curve25519-dalek`'s `Scalar29::sub`/`Scalar52::sub` Moderate
Pub	10	<small>GHSA-x4gp-pqpj-f43q was published for curve25519-dalek (Rust) yesterday</small>
RubyGems	832	Moodle CSRF risks due to misuse of confirm_sesskey Moderate
Rust	780	<small>CVE-2024-38276 was published for moodle/moodle (Composer) yesterday</small>
Swift	34	Moodle HTTP authorization header is preserved between "emulated redirects" Moderate
		<small>CVE-2024-38275 was published for moodle/moodle (Composer) yesterday</small>
		Moodle BigBlueButton web service leaks meeting joining information Moderate
		<small>CVE-2024-38273 was published for moodle/moodle (Composer) yesterday</small>

Unreviewed advisories

Search by CVE/GHSA ID, package, severity, ecosystem, credit...

Severity ▾ CWE ▾ Sort ▾

19,314 advisories

TinyMCE Cross-Site Scripting (XSS) vulnerability using noneditable-regexp option Moderate

CVE-2024-38356 was published for TinyMCE (Composer) 15 hours ago

TinyMCE Cross-Site Scripting (XSS) vulnerability using noscript elements Moderate

CVE-2024-38357 was published for TinyMCE (Composer) 15 hours ago

socket.io has an unhandled 'error' event High

CVE-2024-38355 was published for socket.io (npm) 15 hours ago

curve25519-dalek has timing variability in `curve25519-dalek`'s `Scalar29::sub`/`Scalar52::sub` Moderate

GHSA-x4gp-pqpj-f43q was published for curve25519-dalek (Rust) yesterday

Moodle CSRF risks due to misuse of confirm_sesskey Moderate

CVE-2024-38276 was published for moodle/moodle (Composer) yesterday

Moodle HTTP authorization header is preserved between "emulated redirects" Moderate

CVE-2024-38275 was published for moodle/moodle (Composer) yesterday

Moodle BigBlueButton web service leaks meeting joining information Moderate

CVE-2024-38273 was published for moodle/moodle (Composer) yesterday

EXISTING TOOL SUPPORT

DEPENDABOT

Bump nokogiri from 1.13.3 to 1.13.9 #5

dependabot wants to merge 1 commit into `master` from `dependabot/bundler/nokogiri-1.13.9`

Merging this pull request will resolve 7 Dependabot alerts on nokogiri including a high severity alert.

dependabot (bot) commented on behalf of github on Oct 21, 2022

Bumps [nokogiri](#) from 1.13.3 to 1.13.9.

► Release notes

► Changelog

► Commits

compatibility 82%

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`.

► Dependabot commands and options

dependabot Bump nokogiri from 1.13.3 to 1.13.9 ...

Verified dce04b8

Reviewers
cragkit Request

Suggestions

Assignees
No one—assign yourself

Labels
dependencies

Projects
None yet

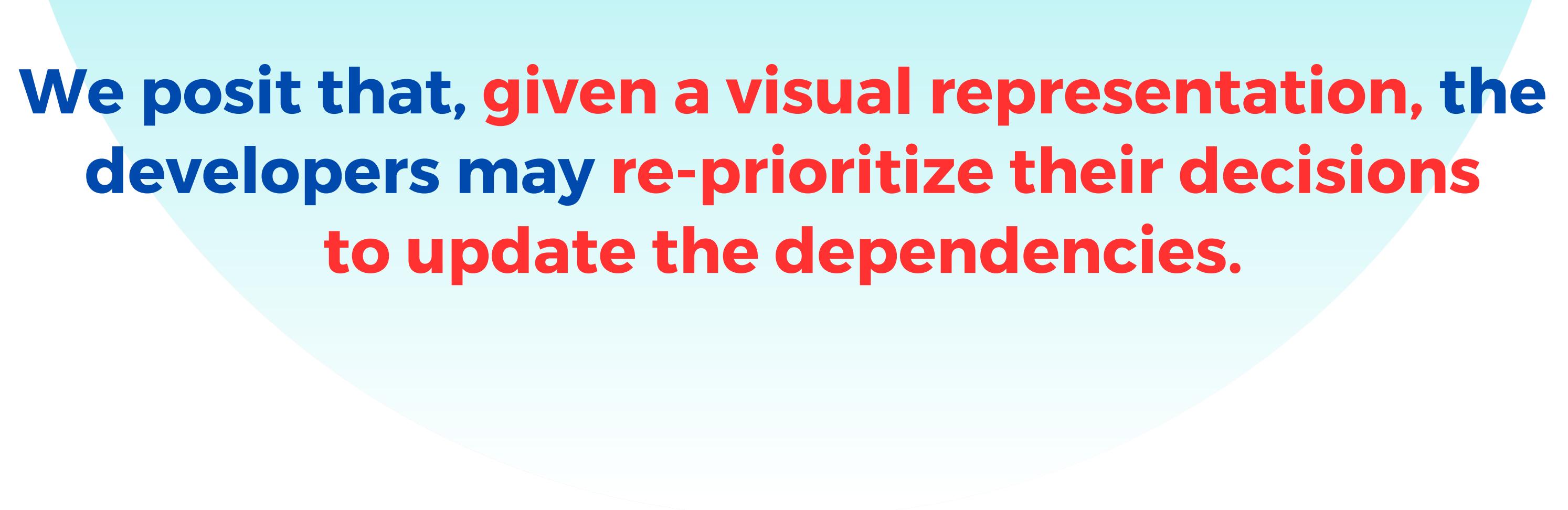
Milestone
No milestone

NPM AUDIT

== npm audit security report ==

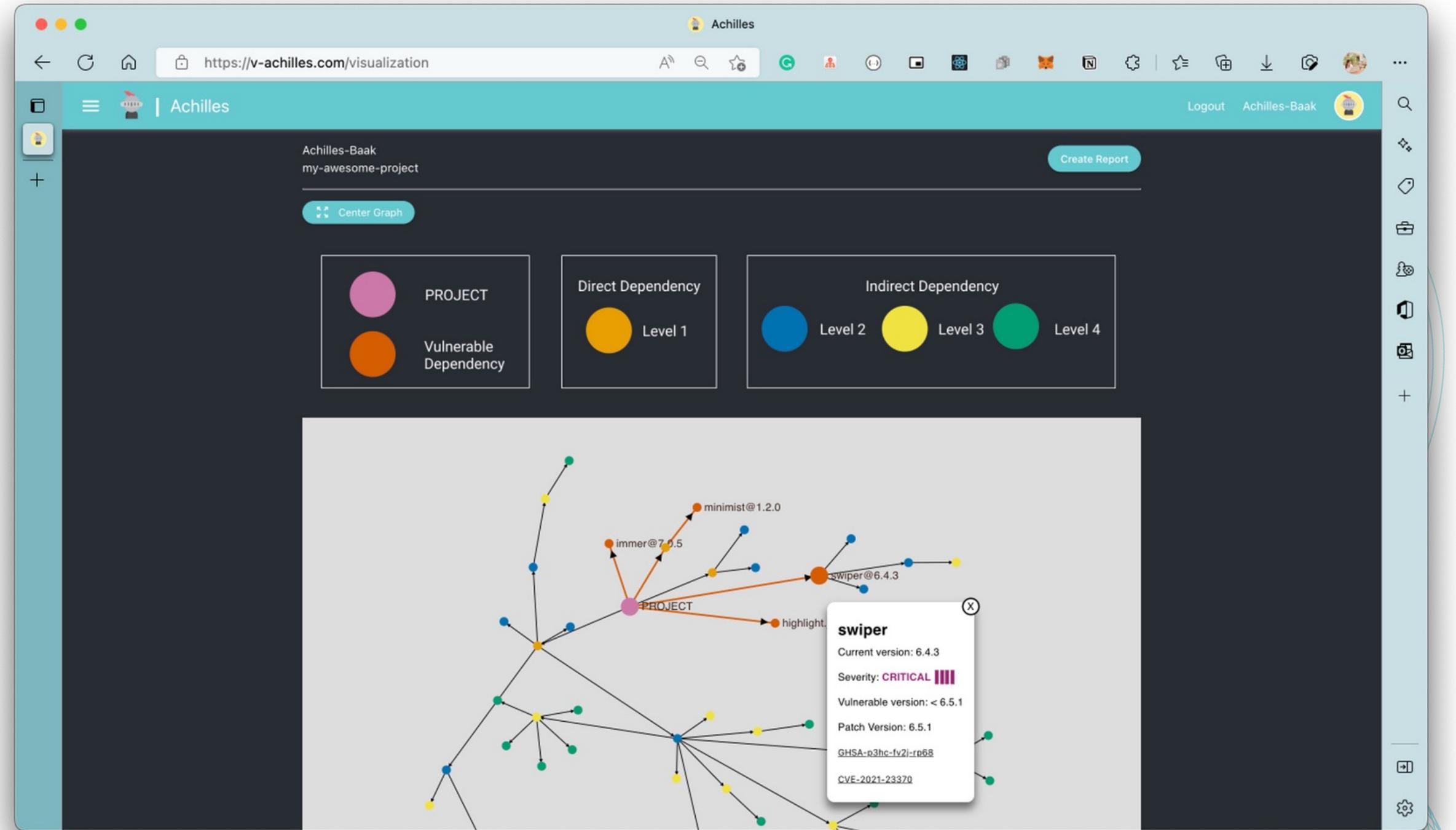
Run `npm install chokidar@2.0.3` to resolve 1 vulnerability
SEMVER WARNING: Recommended action is a potentially breaking change

Low	Prototype Pollution
Package	deep-extend
Dependency of	chokidar
Path	chokidar > fsevents > node-pre-gyp > rc > deep-extend
More info	https://nodesecurity.io/advisories/612



We posit that, given a visual representation, the developers may re-prioritize their decisions to update the dependencies.

V-ACHILLES

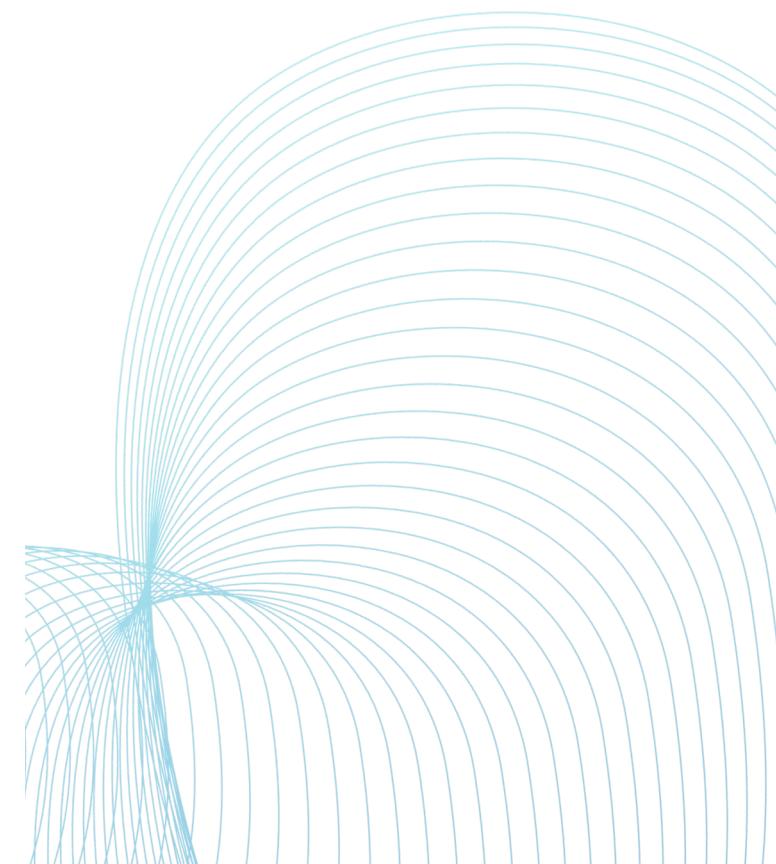
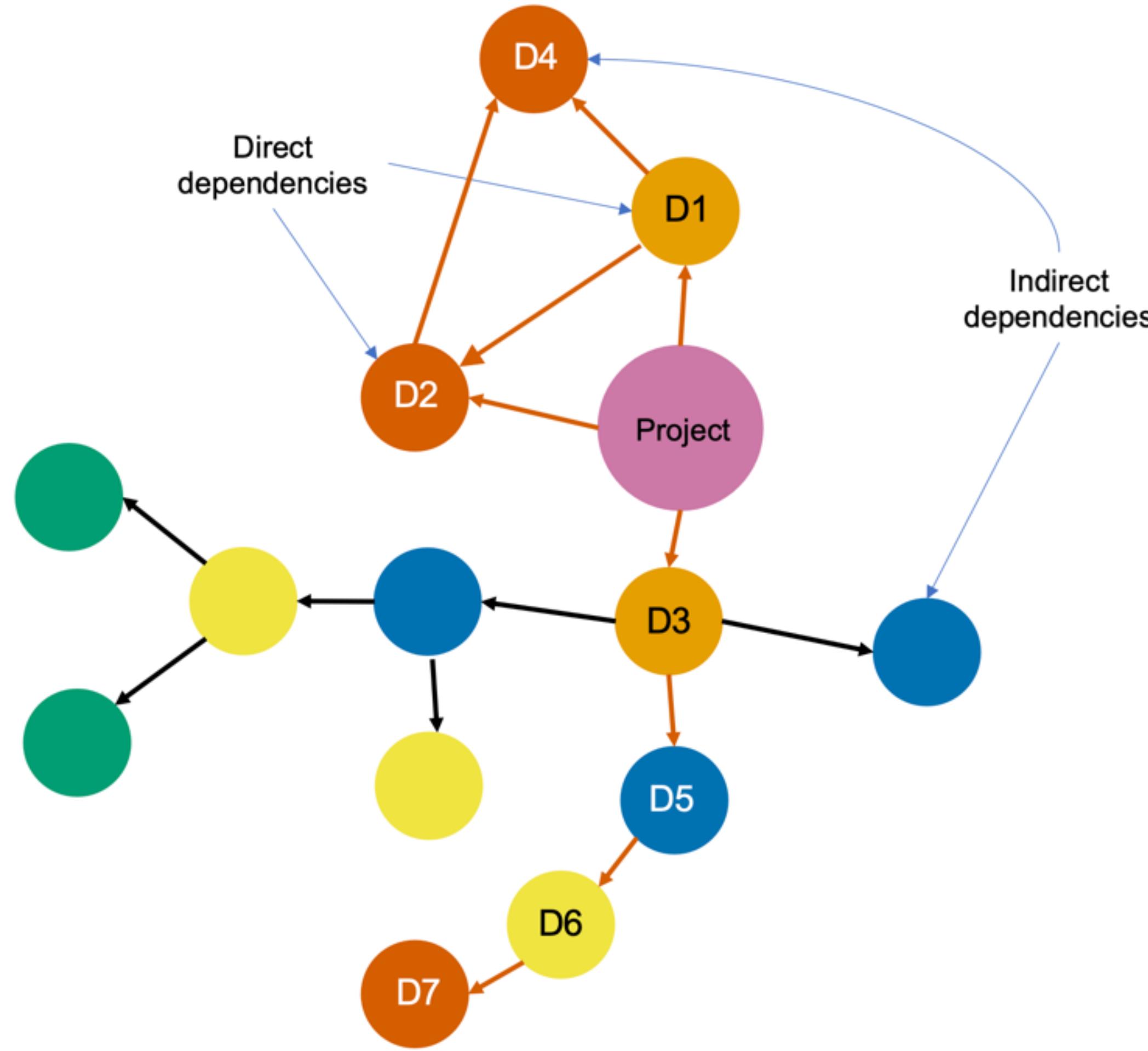
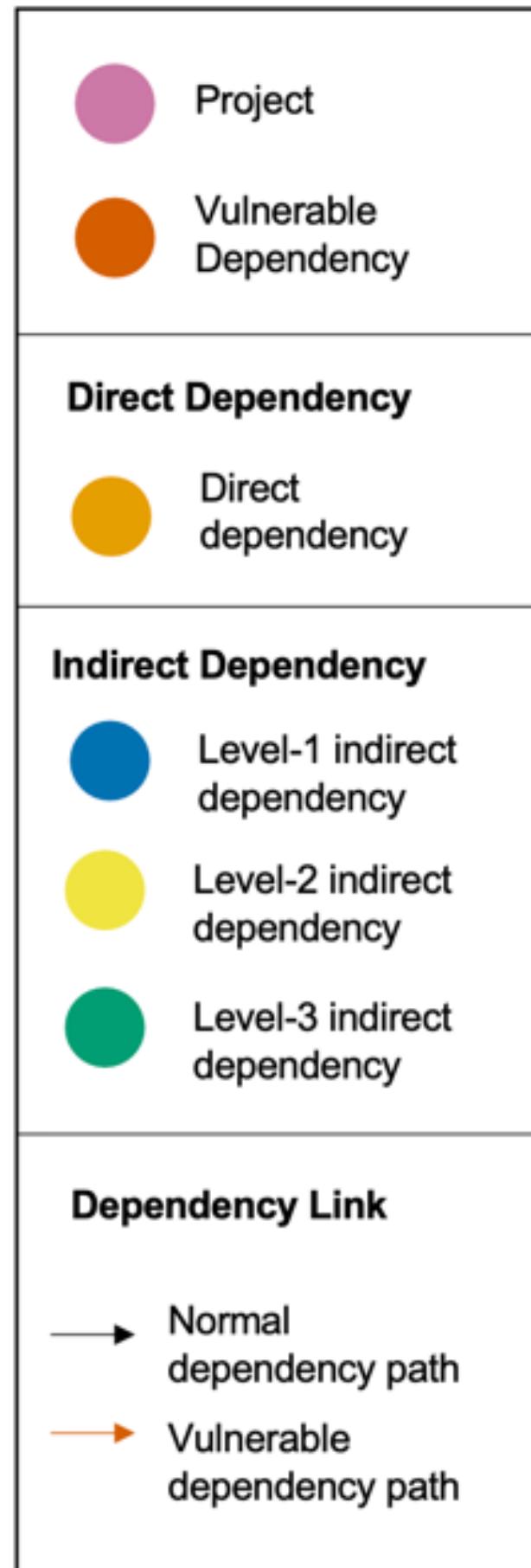


Jarukitpipat, V., Chhun, K., Wanprasert, W., Choetkertikul, M., Sunetnanta, T., Kula, R. G.,
Chinthanet, B., Ishio, T., & Matsumoto, K. (2022).

V-Achilles: An Interactive Visualization of Transitive Security Vulnerabilities.

The 37th IEEE/ACM International Conference on Automated Software Engineering (ASE).

DEPENDENCY GRAPH VISUALIZATION



Achilles

achillestool.com

Incognito

Logout cragkit

Achilles

Which GitHub repository do you want to find vulnerabilities?

Search repositories by name...



Personal Repositories

- 2021-IST-Achilles
- achilles-react
- campaign-critic
- covid-dashboard
- cv
- ESCheckerM
- FileConverters
- GitHub-Crawler
- iwsc2018
- MethodExtractor
- mozanalysis
- MyLife
- Raandee
- SimCal
- StackoverflowChecker
- achilles-bootstrap
- appengine-autotweeter
- Chips-n-Salsa
- cragkit.github.io
- deeplearning4j
- es_exp
- GACloneAgreement
- hello-github-actions
- JavaTokenizer
- MethodParser
- musicg
- onlineclone_processor
- Rational
- sortingalgo
- Thai-IT-community
- achilles-demo
- CalAgreedLOC
- cloverflow-web
- crjk-iwsc17
- demo-for-achilles
- evoESParamSearch
- ghtorrent.org
- hijack
- jpacman
- MinHashCloneDetector
- my-awesome-project
- r-community-explorer
- SiameseX
- ssbsechallenge2016
- the_facebook_scandal

RESEARCH QUESTION

To what extent does our visualization influence
the developer's decision to update?

EMPIRICAL STUDY

TASKS

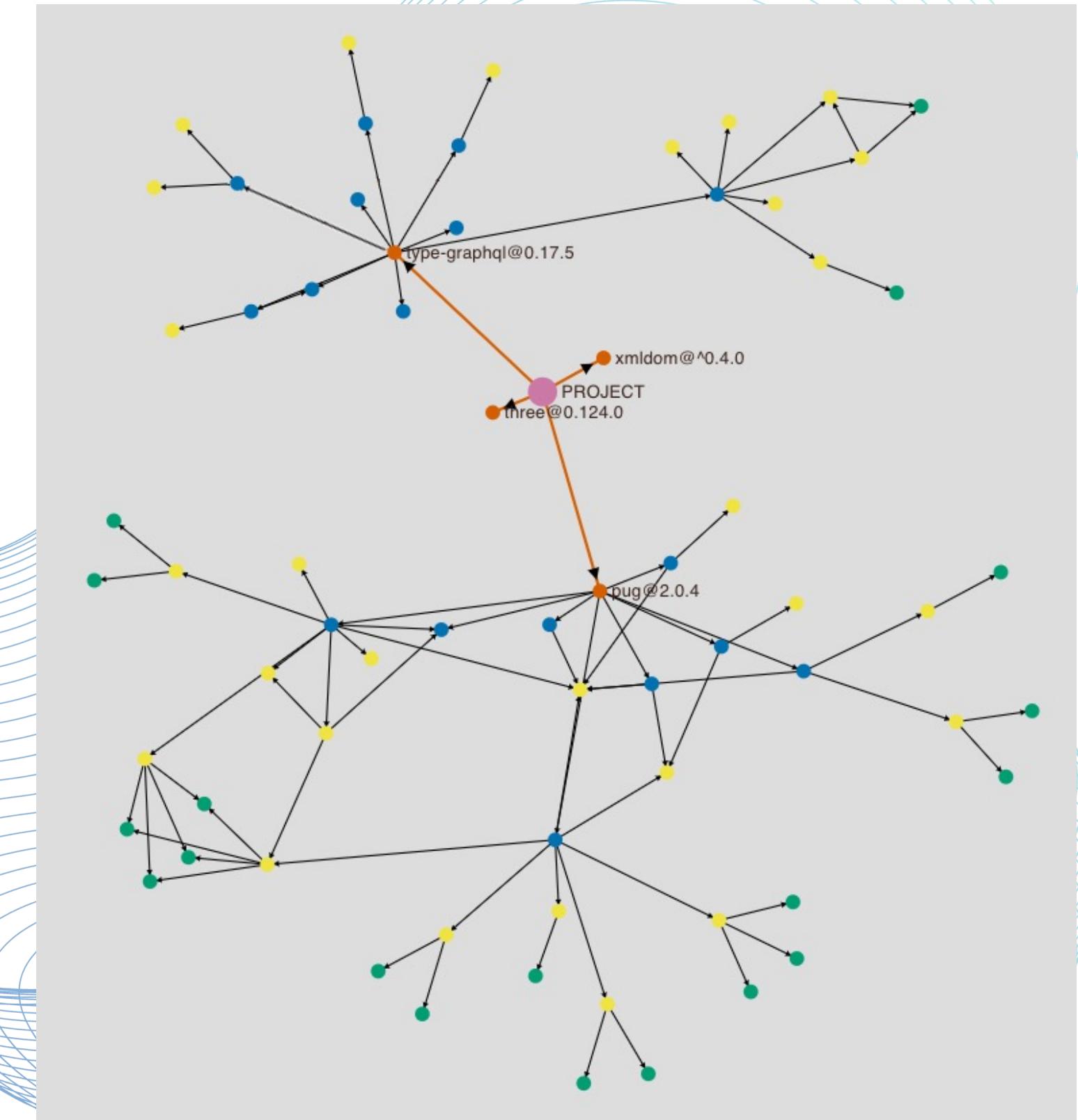
We compare V-Achilles to Dependabot and npm audit, using two tasks

Task 1: Navigating dependencies with complex graphs

Task 2: Navigating transitive dependencies with vulnerabilities

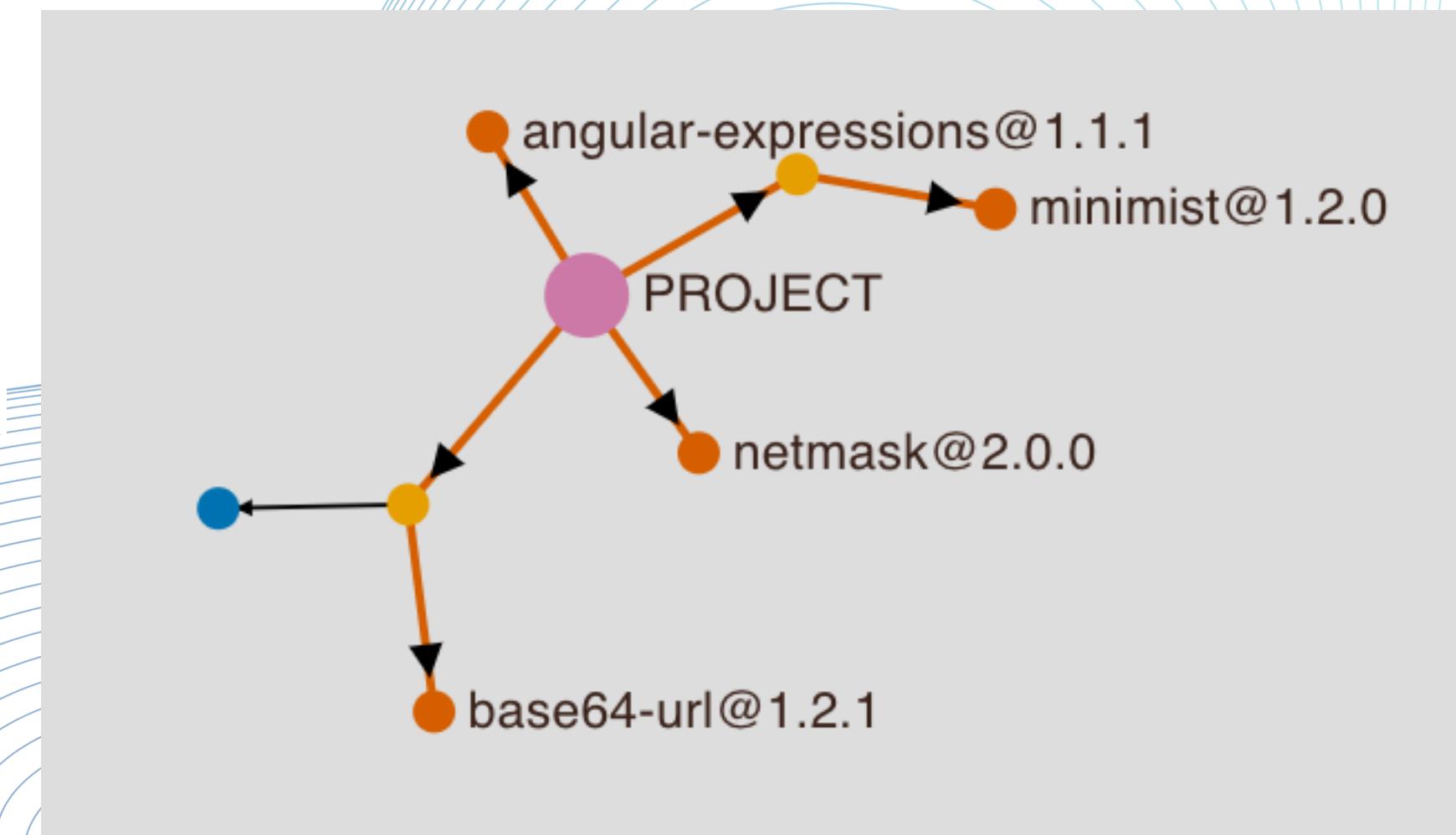
TASK 1: NAVIGATING DEPENDENCIES WITH COMPLEX GRAPHS

No	Dependency	Version	Severity	Type
1	three	0.124.0	High	Simple
2	pug	2.0.4	High	Complex
3	xmldom	^0.4.0	Low	Simple
4	type-graphql	0.17.5	Low	Complex



TASK 2: NAVIGATING TRANSITIVE DEPENDENCIES WITH VULNERABILITIES

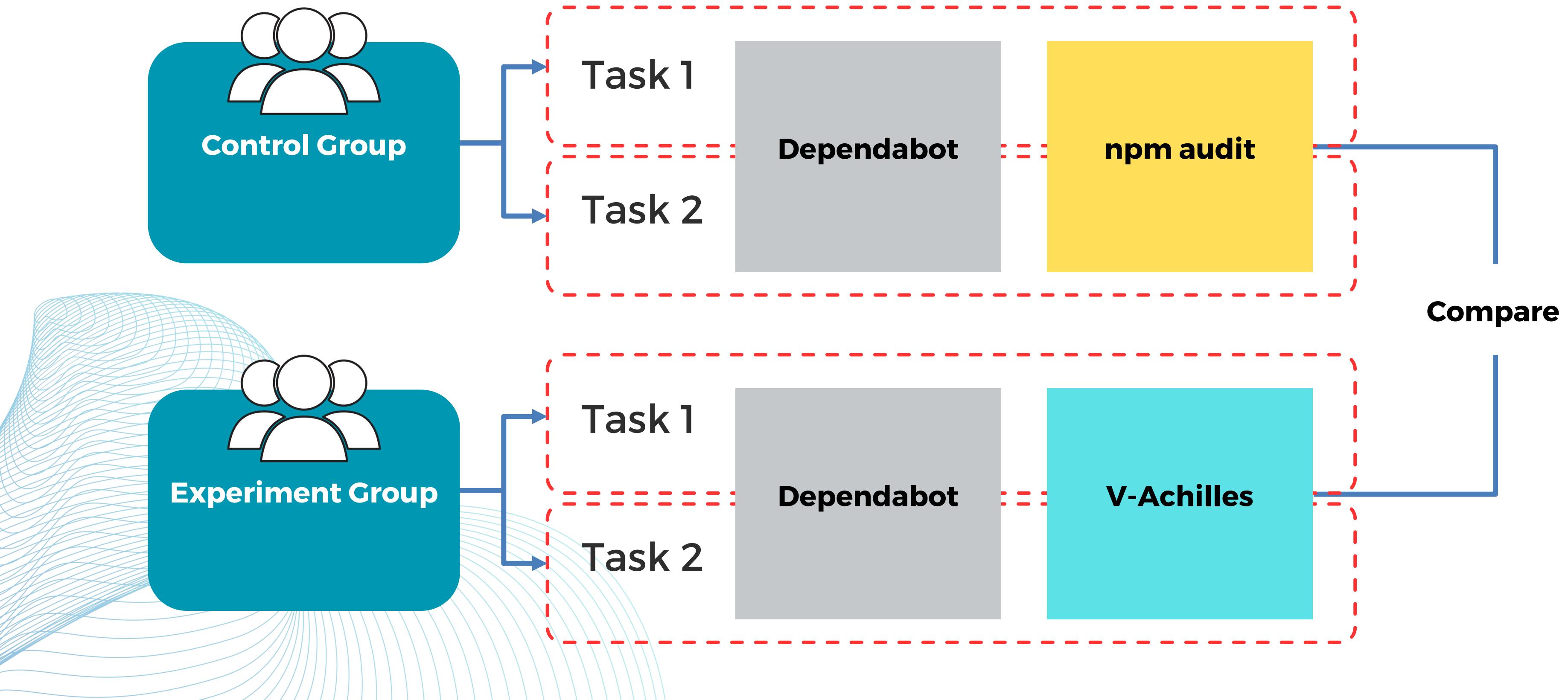
No	Dependency	Version	Severity	Type
1	netmask	2.0.0	High	Direct
2	base64-url	1.2.1	High	Transitive
3	angular-expressions	1.1.1	Low	Direct
4	minimist	1.2.0	Low	Transitive



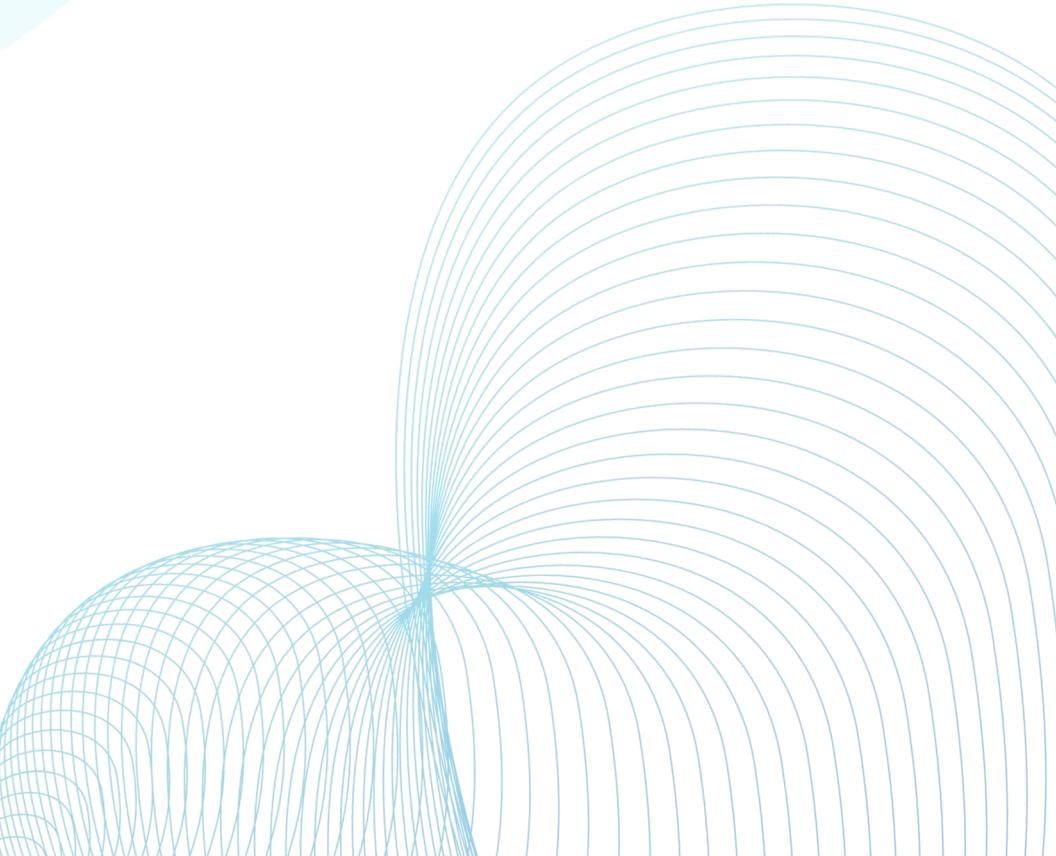
PARTICIPANTS' DEMOGRAPHIC AND TOOLS ASSIGNMENT

Group	Participants	Know Trans. Dep.	Tools Assignment
V-Achilles (Experimental Group)	E1	No	Dependabot followed by V-Achilles
	E2	Yes	
	E3	Yes	
	E4	No	
	E5	Yes	
	E6	No	
	E7	No	
	E8	No	
	E9	No	
	E10	No	
npm-audit (Control Group)	C1	Yes	Dependabot followed by npm audit
	C2	No	
	C3	Yes	
	C4	No	
	C5	No	
	C6	Yes	
	C7	No	
	C8	No	
	C9	No	
	C10	No	

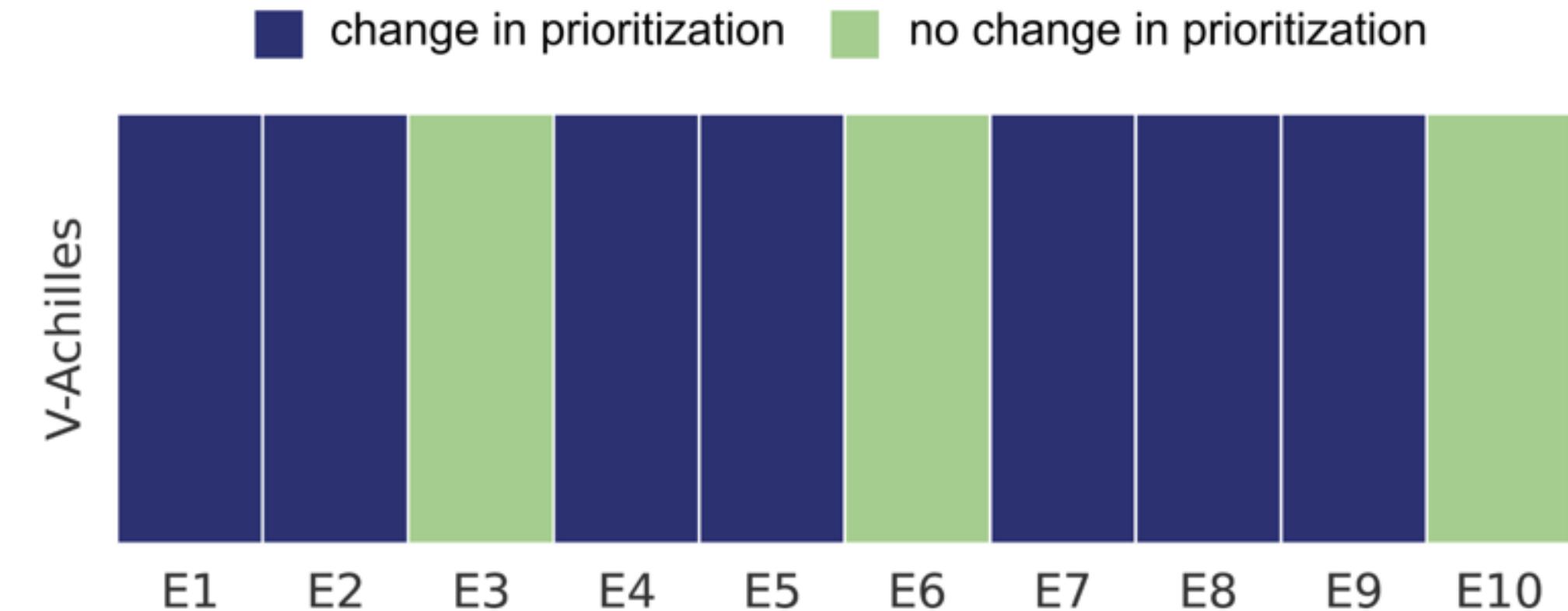
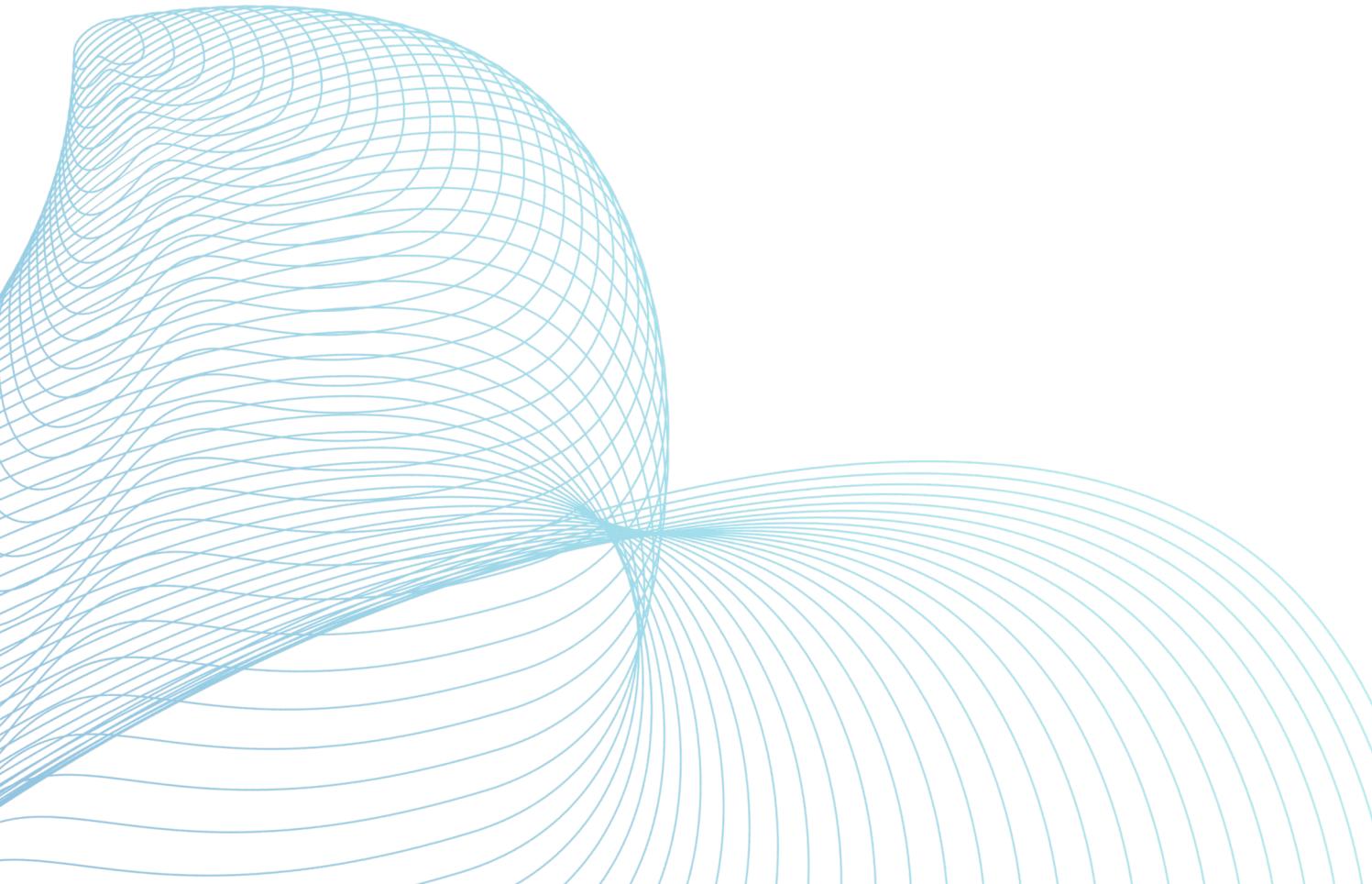
EXPERIMENTAL SETTINGS



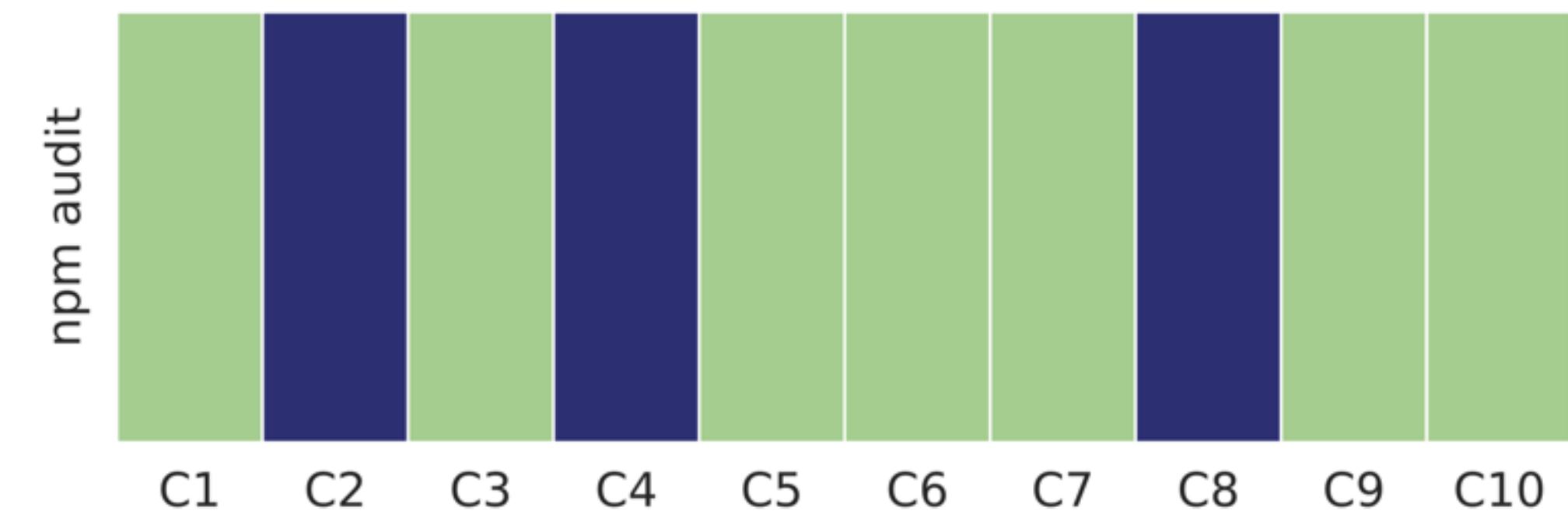
RESULTS



TASK 1: NAVIGATING DEPENDENCIES WITH COMPLEX GRAPHS



(a) Experimental Group: V-Achilles



(b) Control Group: npm audit

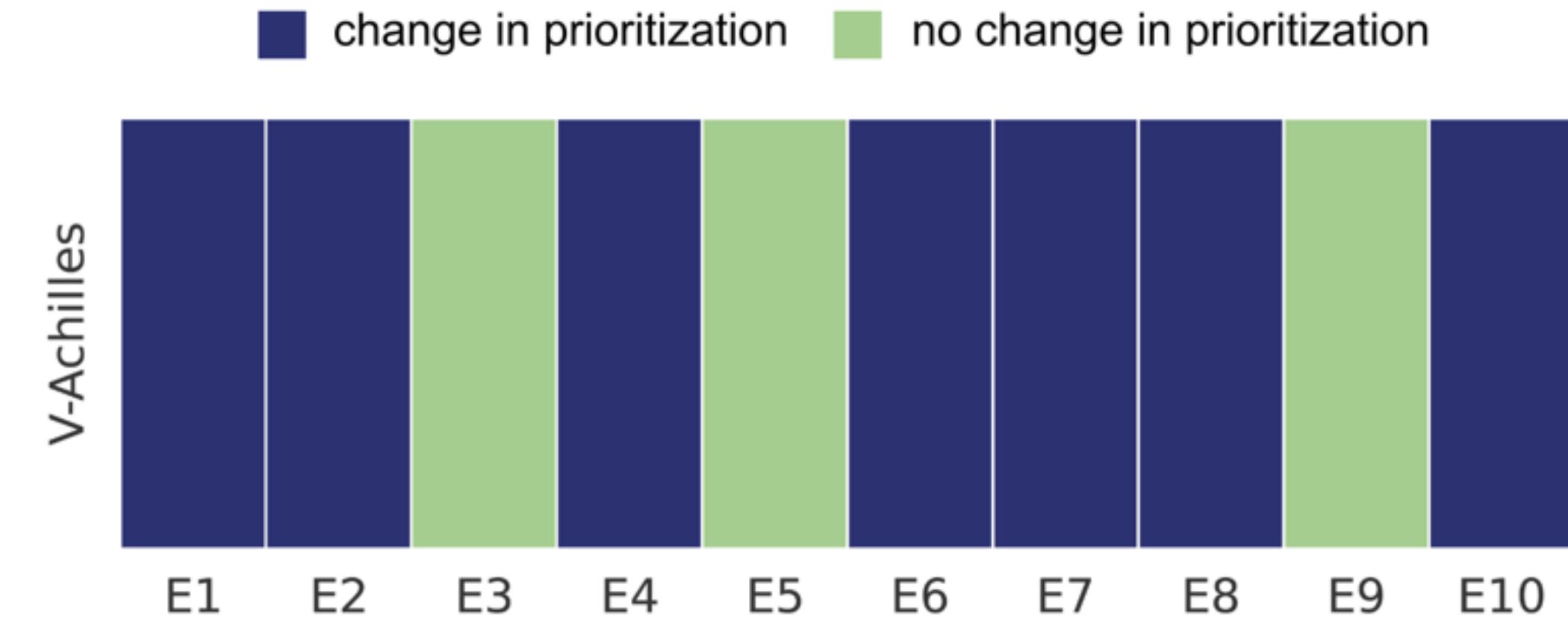
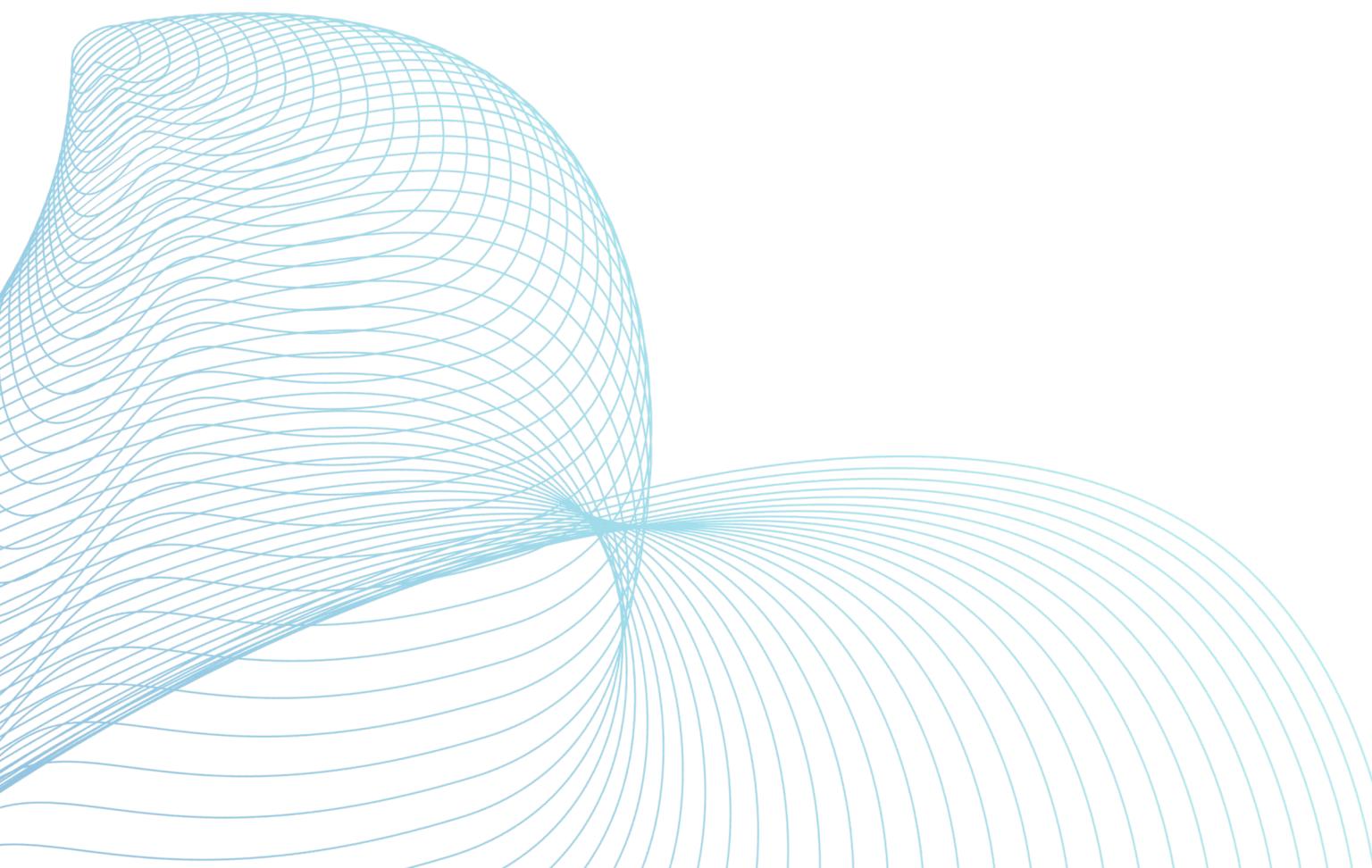
PARTICIPANTS FEEDBACK

“I added more emphasis on high severity and **complex dependency** because of its complexity”.

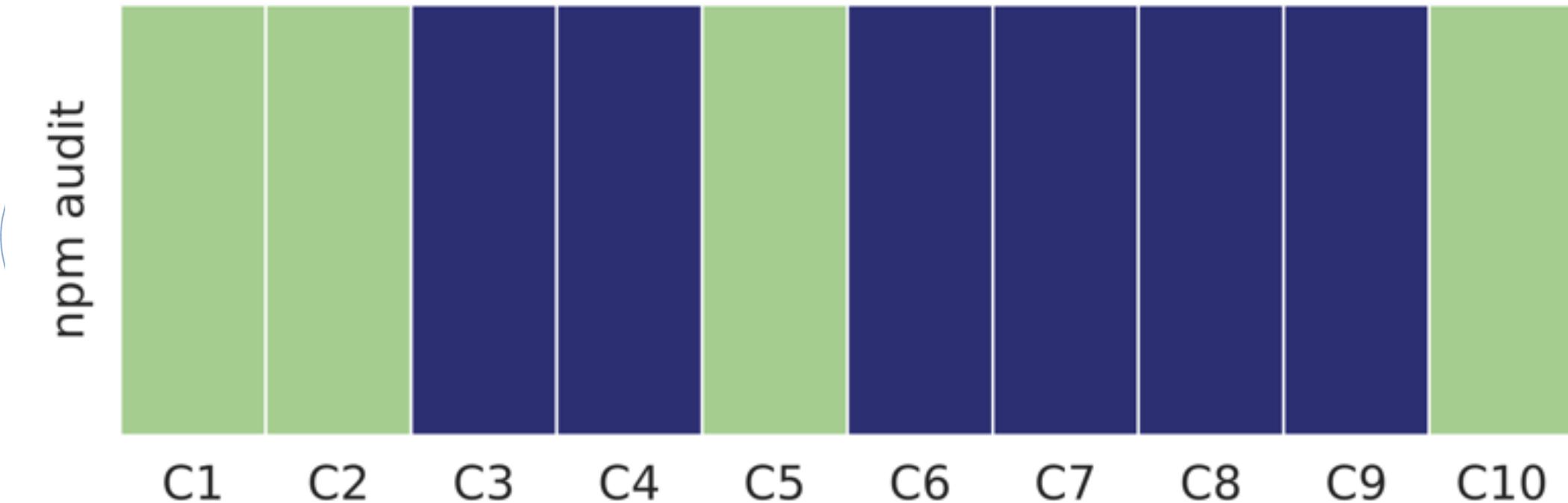
“[After seeing V-Achilles’s visualization, I can see the] **number of transitive dependencies in each library**. If the number is high, it may interrupt other libraries once updated.”

TASK 2:

NAVIGATING TRANSITIVE DEPENDENCIES WITH VULNERABILITIES



(a) Experimental Group: V-Achilles



(b) Control Group: npm audit

PARTICIPANTS FEEDBACK

“[After seeing the visualization] I checked **their severity and the dependency whether direct or not.** netmask and base64-url are high severity but netmask is direct dependency. **I think direct dependency is easier to fix than transitive dependency**, then I think it is the highest priority than others.”.

SEE TO BELIEVE: USING VISUALIZATION TO MOTIVATE UPDATING THIRD-PARTY DEPENDENCIES

We study the effectiveness of a **dependency graph visualization (DGV)** to motivate developers to update vulnerable dependencies.

7 out of the 10 participants who used our visualization changed their prioritization in the two tasks of a project with vulnerable complex dependencies and a project with vulnerable direct and indirect dependencies.