THE TIDELIFT MAINTAINER ADVANTAGE

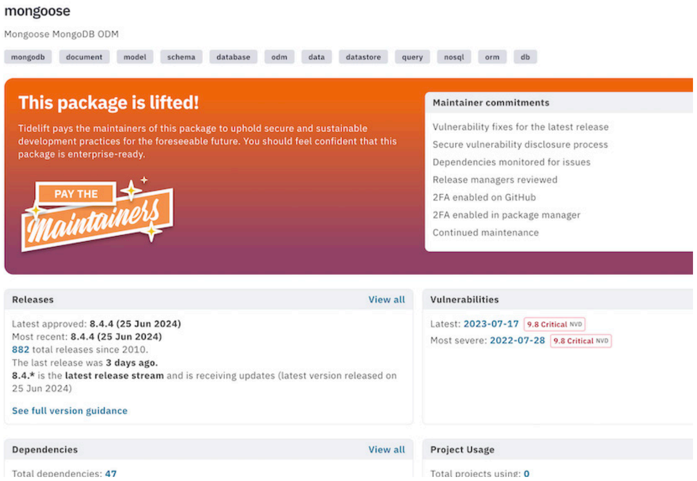
How Mongoose, an npm project with 2 million weekly downloads, improved security and increased its OpenSSF scorecard score

Mongoose is a Node.js Object Data Modeling (ODM) programming library for MongoDB that helps MongoDB users model data, enforce schemas, and manipulate data in a database without prior knowledge of the underlying database semantics of MongoDB.

Mongoose is relied on in over 4 million GitHub repositories and is downloaded on npm 2 million times a week.

In 2014, open source maintainer and then MongoDB employee, Valeri Karpov, or Val as he prefers, was scrolling Twitter while on the air train to his next flight. Serendipitously, while browsing his timeline, Val caught a tweet from former Mongoose maintainer, Aaron Heckman, asking if someone could take the Mongoose project over as he no longer had the time. Val expressed interest, boarded his plane, and by the time he landed, he had push access and was now the maintainer of Mongoose.

Immediately following receiving push access came a flood of GitHub issues. For Val, it was the most significant open source project for which he had taken on a maintainer role. Prior to Mongoose, he had published a few toy projects—but nothing to prepare him for the effort or the firehose of GitHub issues that started coming in.



This package is lifted!

Tidelift pays the maintainers of this package to uphold secure and sustainable development practices for the foreseeable future. You should feel confident that this package is enterprise-ready.

Maintainer commitments

- Vulnerability fixes for the latest release
- Secure vulnerability disclosure process
- Dependencies monitored for issues
- Release managers reviewed
- 2FA enabled on GitHub
- 2FA enabled in package manager
- Continued maintenance

Releases

Latest approved: 8.4.4 (25 Jun 2024)
Most recent: 8.4.4 (25 Jun 2024)
882 total releases since 2010.
The last release was 3 days ago.
8.4.* is the latest release stream and is receiving updates (latest version released on 25 Jun 2024)

Vulnerabilities

Latest: 2023-07-17 9.8 Critical NVD
Most severe: 2022-07-28 9.8 Critical NVD

Dependencies

Total dependencies: 47

Project Usage

Total projects using: 0

Here is the Mongoose package page inside of the Tidelift application, showing the secure development practices the project is following, and also including additional useful information about releases, vulnerabilities, dependencies, and where it is being used within an example organization.

With this workload, it was no wonder that in a couple of months, with MongoDB's consent, maintaining Mongoose became 20% of Val's day job. About a year later, Mongoose became his full time job—he would then be working with MongoDB Node.js Driver team with his primary focus on Mongoose.

When Val took the project over, Mongoose was receiving about 30,000 downloads per week on npm. That download number is now north of 2 million a week. Since 2014, every metric has gone up substantially, including GitHub issues. When he started working on the project, Val estimated that there were approximately 2,000 GitHub issues reported, and a backlog of issues that had not yet been resolved. Now the number of issues has risen above 15,000. All that is to say, Mongoose is a popular project that requires a lot of time and resources to keep running.

Meeting open source security standards

With Tidelift's help, Val and his team were able to learn more about the OpenSSF scorecard, and how, by following its recommendations as outlined in the Tidelift application, they could raise their scorecard score. Some of the first recommended tasks that Val completed were preventing force pushes to the master branch and establishing a stronger policy around code reviews. In Val's words:

The **OpenSSF scorecard** is an automated tool that assesses a number of important heuristics ("checks") associated with software security and assigns each check a score of 0-10, as well as an overall top-level 0–10 score.

“[Working to comply with OpenSSF Scorecards] was something that Tidelift really helped us out with. Both on the monetary perspective, with the extra work that we did put in on that front, but also with bridging the gap between maintainers like me and organizations like the OpenSSF. Which, if it wasn’t for Tidelift, I would have never heard of OpenSSF, or at least I probably wouldn’t have for at least another year or so.”

Since working with Tidelift, Mongoose’s OpenSSF scorecard score has gone from a 7 to an 8 out of 10 (comparatively, the average package score according to the OpenSSF scorecard as of May 2023 is 3.3 out of 10).

“I know all these open source standards communities and organizations are trying their best to do a good job. But I’m a software engineer. I got into working on Mongoose because I like to code, and sometimes keeping up on what some organization somewhere is doing is not something that I have the time or interest in. Tidelift helped me out with that. Bridging that gap [between maintainers and organizations] is as important as making sure that the standards are not too onerous, but also effective and sensible.”

Implementing security practices takes time

Prior to receiving income from Tidelift and its customers, the Mongoose team had put about 10 to 20% of their code through an independent code review. Now, about 70 to 80% of the code in Mongoose is put through an independent code review. It’s a change that made a huge impact for the team and a process that Val admits isn’t easy without contributors.

Independent code review, a recommended OpenSSF scorecard practice that requires that a project’s code be reviewed by someone other than the original author, improves code quality and ensures that consistent practices are made throughout. However, if you’re the sole maintainer of a project, which is often the case for many open source projects, it is not always easy to find a qualified, trusted person to review your code. Especially if you’re juggling other obligations and trying to ship things out the door as fast as you can.

“It’s not free. I hope to improve and formalize the core team practices and Tidelift’s funding will help on that front. Such as formalizing the responsibilities of things like, you’re responsible for reviewing this code, you’re responsible for reviewing that code.”

Finding vulnerabilities in a world of security noise

When it comes to finding and prioritizing security issues, Val expressed frustration with the disconnect between the software security space and the open source maintainer space, stating, “There are a lot of places where security issues are reported, and sometimes they don’t end up in a place where I’m looking for them.”

In January of 2022, an instance of prototype pollution—a class of vulnerabilities that enable bad actors to exploit JavaScript runtimes—was reported in the Mongoose project. Val received a security report from the Tidelift team along with actionable next steps. Without the Tidelift report, the vulnerability would have otherwise gone unseen.

The work that Val and the Mongoose team has done for this project is already having a huge impact on this popular ODM. Tidelift customers can use Mongoose—and other npm packages that rely on it—with confidence, knowing that Val is leading a team of experienced maintainers committed to ensuring the package follows a robust set of enterprise secure software development practices, and keeping it resilient and healthy into the future.