THE TIDELIFT MAINTAINER ADVANTAGE

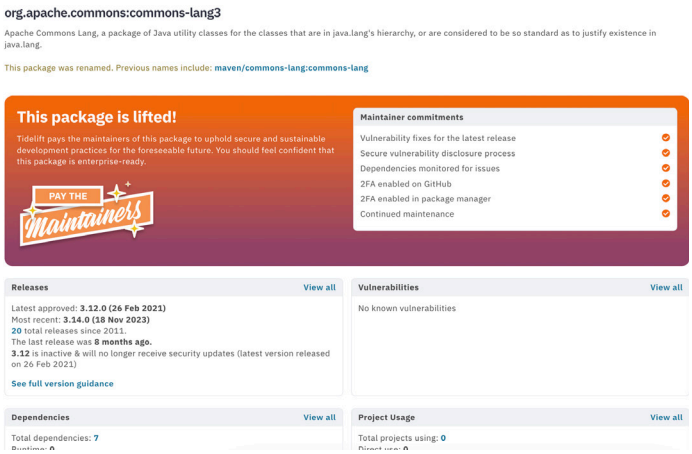
How Java maintainer Gary Gregory found more time to secure and maintain his open source projects

The Apache Commons Project is a well known Apache project aimed at creating and maintaining reusable Java components. With over twenty components, Apache Commons has a wide reach. The projects under its umbrella offer a range of capabilities within Java. For example, one project within Commons, Lang 3, is a package of utility classes created to extend the functionality of the Java API—the project is the 10th most downloaded project in Maven Central. Like many open source projects, Apache Commons components save time for Java developers.

Open source maintainer Gary Gregory has been a cornerstone of the Apache Commons community for years. What first started as a hobby project of contributing back patches to fix bugs grew into working on a component of Apache Commons. As time went on, tending to one component evolved into maintaining several Apache components alongside other Java projects. He's a maintainer on a number of open source initiatives: Apache Commons, Apache HttpComponents, Apache Xalan, Apache Mina, and the now infamous Log4j, the most downloaded logging library, directly and transitively.

Though, as time goes on, the number of responsibilities has increased. In Gary's words, "Most projects have hundreds of issues logged against them. The challenge is really filtering, especially when you're looking at older issues. Any project that you join will already have a huge backload of open issues. Some are valid, some are not."

This increase has been particularly felt since Log4Shell, the name given to the Log4j zero-day vulnerability incident in late 2021.



Here is the apache.commons:commons-lang3 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.

"It seems that there's a whole industry that has popped up where we're now on people's radar, not just for Log4j but everything. There's a lot of small consultancies that'll create these fat, 100 page PDF reports with charts—it's all machine generated. It's painful to sift through when there's two bug reports, and then you have to decide, well, is this the way the API is designed and that's just the way it works, or is this a real bug? But it takes time, and there's so much more now."

The importance of recurring income

The urgency and demand for quick fixes around the Log4Shell incident caused many Log4j maintainers to work overtime, clocking in dozens of hours unpaid with large corporations at their heels asking for an immediate solution. After Log4Shell, the team received grants in support of their efforts to maintain and secure the logging library. However, these were one-time deals, not dependable income. Once the money runs out, what happens if another Log4Shell event rounds the corner?

"I think the recurring income piece is critical for me, at least," Gary responded when talking about the difference between the income Tidelift provides and one-time project grants like the Log4j team received after the Log4Shell incident. Unlike a money drop to fix a broken bridge, open source needs financial support to fix the issue and recurring funds to maintain the project.

"Well, just imagine what it's like to have a job with a recurring income—it makes you feel safe, secure, and confident that you can keep on doing this work and that it's not time wasted. It also lets you plan ahead. I always maintain a list of the components I want to release in the near future, and then I have a longer term list of things that I want to work on, that I know I'll get to. Being in a partnership with Tidelift lets me build this and know that I'll get to it."

Professionalism: more support, more time

When an open source project comes second to a day job and issues and requests are piling up, it's difficult to meaningfully stay on top of the daily maintenance and security work. Since partnering with Tidelift, Gary has found that the support from Tidelift and its paying customers gives him the best motivation to act more professionally and more quickly on addressing bug reports and vulnerabilities.

"...my involvement with Tidelift has caused me to create a tighter feedback loop for any of these issues. I've created a lot more releases, which means that all the bug fixes and enhancements go out a lot quicker and with a lot more frequency. Whereas in the past, I would just release versions of components whenever I felt like it, or whenever I needed them.The way I look at it now is, I look at all these issues and people that submit them as customers—so I consider my support from Tidelift as a professional relationship. I want to behave like that towards anybody who interacts with all of the Apache projects that I maintain."

Additionally, while writing this case study, Gary provided us with recent stats from Apache Commons Lang to highlight how he's been able to nearly triple his release output since beginning his partnership with Tidelift.

Gary's GitHub contributor page for Apache Commons Lang

The work that Gary has done for Apache Commons is already having a huge impact on the health and security of these popular open source projects. Tidelift customers can use Apache Commons—and other Java packages that rely on it—with confidence, knowing that Gary is helping lead 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.