THE TIDELIFT MAINTAINER ADVANTAGE

How a popular Python project established a documented and streamlined security process

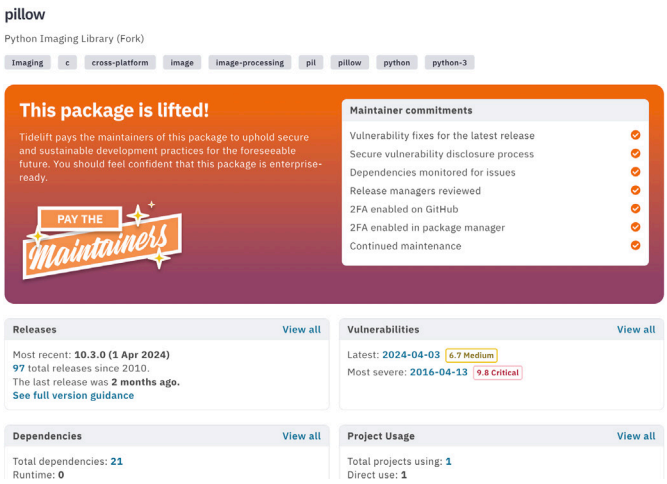
Pillow is a friendly fork of the Python Image Library (PIL) and a powerful library for working with images. Typical uses of Pillow include:

- Image archival such as creating thumbnails, converting file formats, printing images
- Image display
- Image processing / manipulation

Pillow is relied on by many to process images, with the package being downloaded 3 million times a day. It is considered the top image processing package for Python.

The creation of Pillow is a familiar story in the open source world—it was born from the desire to simplify. In 2010, maintainer Jeffrey A. Clark, who goes by Alex, was performing Plone CMS installations and found that most but not all components of Plone could be found on the Python Package Index (PyPI), making the installation process harder. Thus, via the Pillow fork, PIL was available and installable from PyPI and for the next couple of years, Alex would maintain the popular forked project on his own.

In 2013, Brian Crowell, a Pillow user, contributed a pull request to add support for Python 3 to Pillow, however at that point, PIL did not address any of its packaging issues let alone add support for Python 3. Meanwhile, Pillow released Python 3 support, eventually funneling a large portion of PIL traffic into Pillow, in doing so, creating more requests for Alex. Eventually, the requests grew beyond what could be completed by one person, so as time went on, several other maintainers would join Pillow's core team.



Here is the pillow 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.

Tackling security issues can be difficult without a streamlined process and finding the time to formalize one can be even more difficult when you're handling requests and doing this all as an unpaid volunteer in addition to a day job and whatever else life demands.

"Getting paid in 2019 with Tidelift was like getting a record deal. I made it," said Alex.

Not only was Alex receiving pay, with help from Tidelift and its paying customers, he's now able to make sure that his security co-maintainer, Eric, gets paid as well:

"Eric does a lot of "fuzzing" and is our go-to security person on the team, primarily because he is most familiar with the C code in Pillow. The fact that I know Eric is getting paid and is there if we need him is great."

Additionally most of the day to day development work is now done by Hugo van Kemenade and Andrew Murray, also partnered maintainers getting paid by Tidelift.

One of the biggest benefits Tidelift customers get in return for investing in the work of the Pillow maintainer team is better documentation around security issues. Prior to receiving income, the Pillow team wasn't able to invest any time in documenting security issues. Now that has changed for the better.

"Since we've joined Tidelift in 2019, we've dealt with many security issues over the years, probably at least a few a year. Being able to make those meaningful changes with Tidelift's help would probably be the highlight. In fact, I would say that's the most important thing that we do at this point."

Even more importantly, security has become part of the normal process for doing business for the Pillow team, now that they are being paid by Tidelift and its customers to put in place and document the project's secure software development practices.

The team has made numerous upgrades to their security processes, including documenting security fixes, and with tooling provided by Tidelift, it's become much more streamlined to tackle security issues with Tidelift's help.

"Tidelift is doing a huge part of the unpleasant stuff that, if I actually had to do this, I would probably be a whole different person. Having a partner in the stuff that is serious is very helpful."

While Pillow—and its users—continues to benefit from the increased investment in its maintenance, the real dream for Alex is to be able to spend even more of his time on writing and maintaining open source.

"This should be my full time job," said Alex. "I'm fortunate that I get paid from Tidelift. I have the luxury of being able to say that I should be able to make a living doing Pillow for other people [meeting requirements and standards]."

The work the Pillow team has already done is having a huge impact on this heavily used Python package. Tidelift customers can use Pillow—and other packages that rely on it—with confidence, knowing that a team of experienced maintainers are committed to ensuring the package follows a robust set of enterprise secure software development practices, and keeping it resilient and healthy into the future.