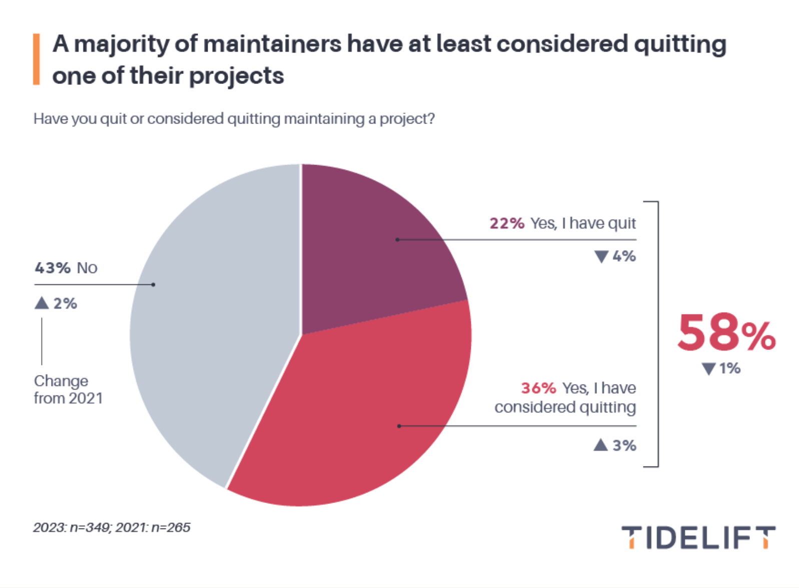
TIDELIFT

The xz backdoor hack, Tidelift, and paying maintainers: What you need to know

In late March 2024, a developer noticed some unusual behavior on their computer, investigated it, and uncovered a hack of epic scope in an obscure but important library called xz. The attack was technically sophisticated, but perhaps worse, it was socially sophisticated. The attackers took advantage of an open source maintainer over a long period of time to slowly, but steadily, win his trust—and then subvert the security mechanisms that he had previously put in place.

What does the xz hack mean for organizations using open source and for open source maintainers?

For organizations heavily reliant on open source in their applications (which is most if not all organizations), the xz hack is a wakeup call. It is a warning sign that they need to become increasingly vigilant in ensuring that the open source they are using is secure, and **that the people who create and maintain the software they use are properly supported in their work.**


A majority of maintainers have at least considered quitting one of their projects

Have you quit or considered quitting maintaining a project?

2023: n=349; 2021: n=265

Tidelift's 2023 state of the open source maintainer report found that **60% of open source maintainers describe themselves as unpaid hobbyists,** while only 13% report earning most or all of their income from maintaining their projects.

Meanwhile 44% of maintainers describe themselves—like the xz maintainer—as solo maintainers. So it is no surprise that, when asked what they dislike most about being a maintainer, they reported that it is stressful, lonely, demanding, and financially unrewarding work.

In fact, almost **60% of maintainers have either quit or considered quitting** maintaining their projects.

How can Tidelift—and our customers—help?

Tidelift is improving the security and resilience of the open source software supply chain, specifically focused on the most depended upon application development libraries in popular ecosystems like JavaScript, Java, Python, Ruby, and Go.

Tidelift is the only company that partners with open source maintainers and pays them to:

- ✓ Implement industry-leading secure software development practices and validate the practices they follow so organizations can have the same confidence in the security of their open source that they have in their own code.
- ✓ Contractually commit to continue these practices into the future so that organizations can confidently make long term investments in the packages they use.

While we do not cover C/C++ packages like xz today, we can help organizations prepare for issues like this in the future across our supported ecosystems. Here are some of the ways Tidelift can help:

- **We pay maintainers to reach security and licensing goals.** Put simply, we pay maintainers to help them become better maintainers, and to keep maintaining the software.
- **We pay *known* maintainers** and work to ensure that the money goes to the people already doing the maintenance.
- **We pay based on project usage.** We pay maintainers based on an analysis of how many of our customers use their software.
- When a maintainer partner needs to move on, **we help ensure project continuity**. Sometimes, for perfectly good reasons, a maintainer wants to stop working on their project. When this happens, we help find trusted maintainers from our network interested in getting paid to continue the work.
- **We focus on the middle of the stack.** The traditional operating systems vendors have built a lot of infrastructure to vet and support core operating system features, and the Linux Foundation and others have put in a lot of work around the biggest high-level development tools and frameworks. But that has left a huge number of relatively untouched packages in every modern language stack that need Tidelift-style attention. We believe our highest impact, on open source and for our customers, lies in supporting those packages.

When SockJS maintainer Bryce Kahle took a new job that didn't involve JavaScript, Asif Saif Uddin stepped in as maintainer, ensuring the project wasn't abandoned.

Maintainer Jordan Harband used income from Tidelift and its customers to save the popular Minimist JavaScript project from deletion when its previous maintainer decided to delete their projects from GitHub.

Maintainer Tatu Saloranta used income from Tidelift and its customers to completely re-architect jackson-databind, and extremely popular Java data-binding package, to eliminate the risk of remote code execution vulnerabilities.

The maintainers of urllib3 used income from Tidelift and its customers to significantly improve the security practices of a Python project that is downloaded a staggering **450 million** times a month.