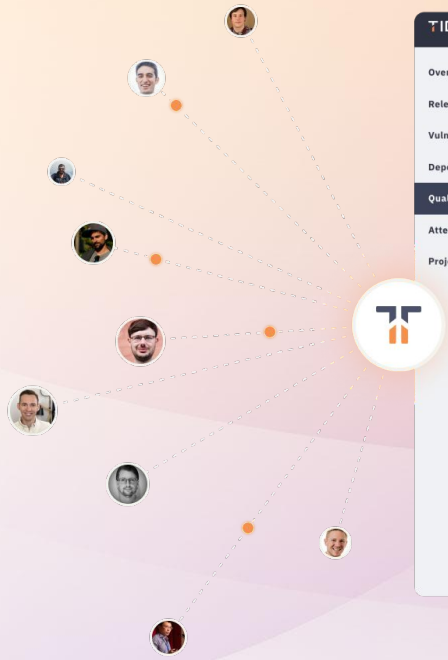
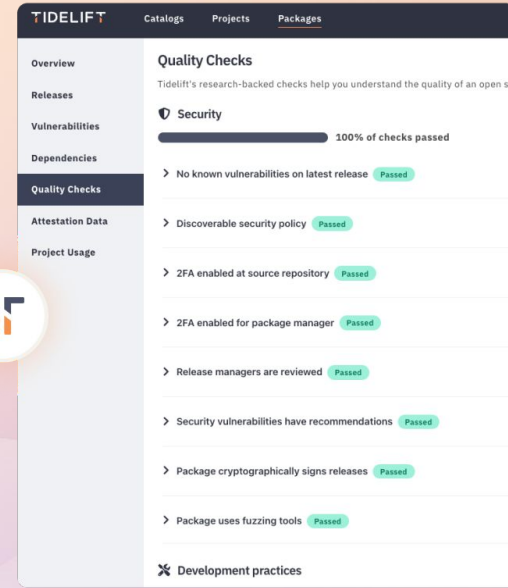
MAY 2024

TIDELIFT

THE TIDELIFT GUIDE TO

Reducing security risk from bad open source packages





What's covered in this guide

TIDELIFT

Introduction

The benefits of open source

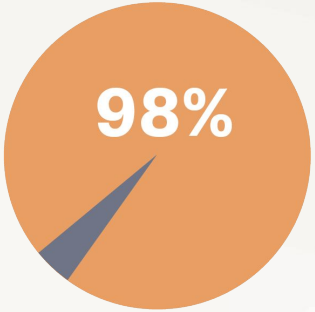
Open source is the modern application development platform

These days, open source is everywhere.

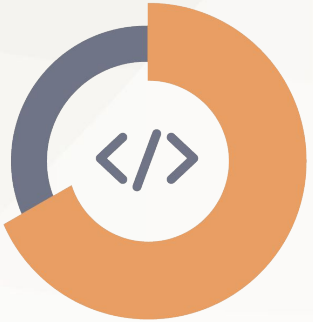
Using open source gives anyone trying to innovate with software a head start, with billions of lines of code freely available, developed, and shared through an open community of creators, collaborators, and maintainers.

Open source helps increase developer productivity, accelerates development and deployment, and reduces application development costs.

However, it comes with hidden costs related to keeping it secure and well maintained.



of applications maintain open source components[1]



open source code makes up 70% or more of the average application[2]

[1] Sources: Tidelift and Harvard
[2] Sources: Tidelift and Synopsis

INTRODUCTION

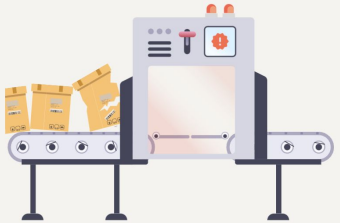
The hidden cost of bad packages

Many orgs don't have a continuous view of where abandoned, insecure, or end-of-lifed packages exist in their applications.

These bad-for-enterprise-use packages create **security risk** that could potentially impact the organization's revenue, data, and business continuity.

They also **suck up valuable development cycles** when organizations have to replace them, work around them, or deal with endless cycles of vulnerability remediation.

WHAT MAKES A PACKAGE "BAD" FOR ENTERPRISE USE?



We use the word *bad* as shorthand for a risky package that may lead to bad security outcomes or slow down development.

A package may be bad for enterprise use if it is unmaintained, deprecated or end-of-lifed, missing published security policies, unresponsive to security issues, or has been removed from the package manager.

TIDELIFT

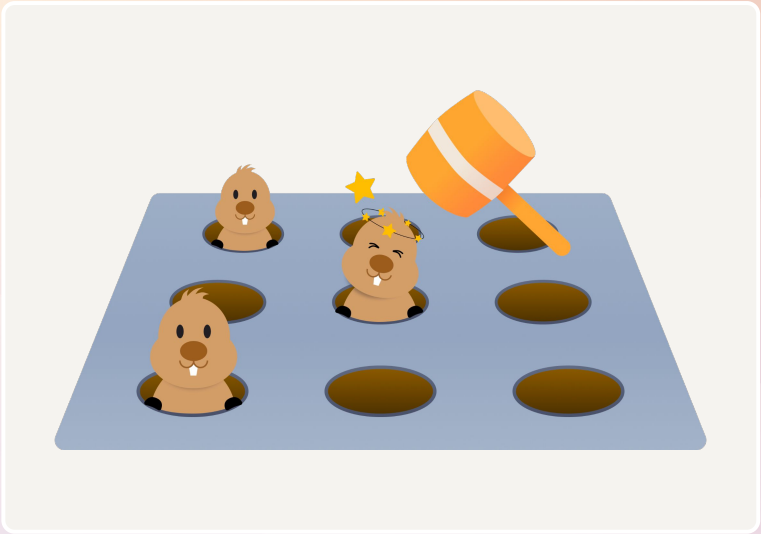
How are organizations managing open source software risk today?

A reactive approach: vulnerability remediation

Many organizations use **software composition analysis (SCA) tools** to identify and remediate open source vulnerabilities.

This is an effective way to ensure risk from existing vulnerabilities is reduced.

But it is also a game of whack-a-mole, involving triaging long lists of security vulnerabilities that are difficult to prioritize and separating false positives from real security risks.

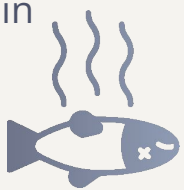


Flagging known vulns: necessary, but not sufficient

SCA tools have been a common way for organizations to manage open source security issues, **but are only part of the solution**.

DON'T EAT SPOILED FOOD

There are many options for helping your organization identify and fix known vulnerabilities in open source.



AND

SOURCE BETTER QUALITY FOOD

But you also can make active decisions to bring in open source components that are being developed securely in the first place!

TIDELIFT

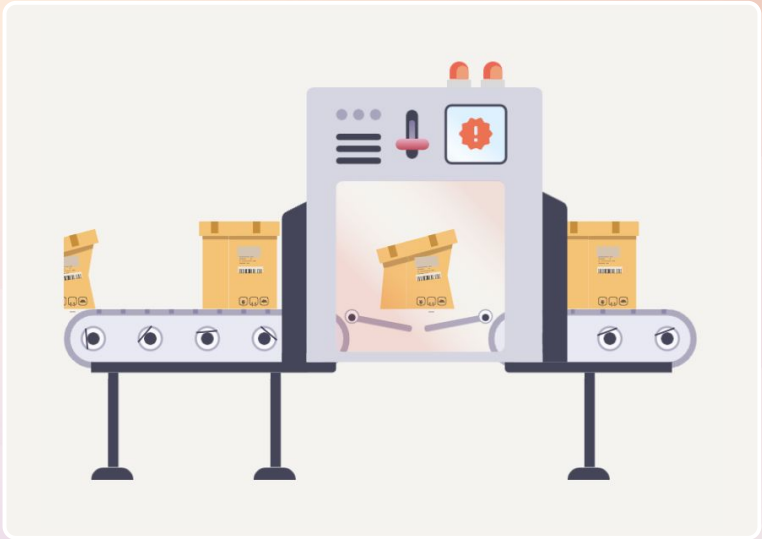
How can organizations reduce security risk from bad open source packages?

A proactive approach: reducing reliance on bad packages

Tidelift takes a unique, data-driven approach to reducing reliance on bad packages:

We **partner with the maintainers** of thousands of the most-relied-upon open source packages and we **pay them** to implement industry-leading secure software development practices and document the practices they follow.

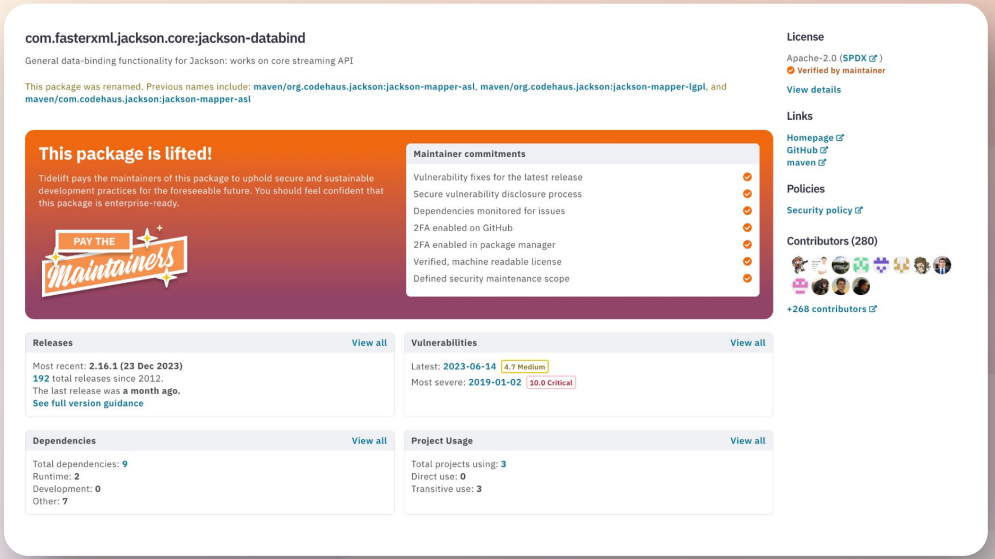
The result is a valuable source of cross-ecosystem package intelligence that customers can use to identify and eliminate bad packages AND ensure the packages they rely on most keep getting better.



The Tidelift maintainer advantage

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.



Tidelift helps leading organizations use open source with confidence.

Reduce security risk

by eliminating attack entry points through bad packages.

Improve productivity

by reducing vulnerability fire drills from insecure or undermaintained packages.

Improve application quality

by building with healthy and resilient open source packages.

Increase operational efficiency

by saving costly manual package evaluation time.

Case story: the ROI for proactively improving open source security

One large enterprise customer had a strategic initiative to **reduce time and money spent** managing the open source dependency lifecycle.

Scanning to discover and fix vulnerabilities was **not** getting them to the goal fast enough.

So they undertook an effort to **prioritize proactively preventing bad packages from entering production**, while also cleaning up risk from packages already in place.

RETURN ON INVESTMENT

- Saved $1,650,000 in time that would have been otherwise spent manually evaluating packages
- Avoided 50,000 bad releases that had been formally deprecated, abandoned, or were otherwise unfit for use
- Benefitted from 300 vulnerabilities fixed by maintainers in accordance with Tidelift's maintainer contract
- The remediation of these vulnerabilities by partnered maintainers removed 3000 points of risk in applications running in production

Fastest paths to value with Tidelift

Evaluating packages
before pulling them in for application development

Actively monitoring
the open source packages in use

Identifying and eliminating bad packages
already adopted

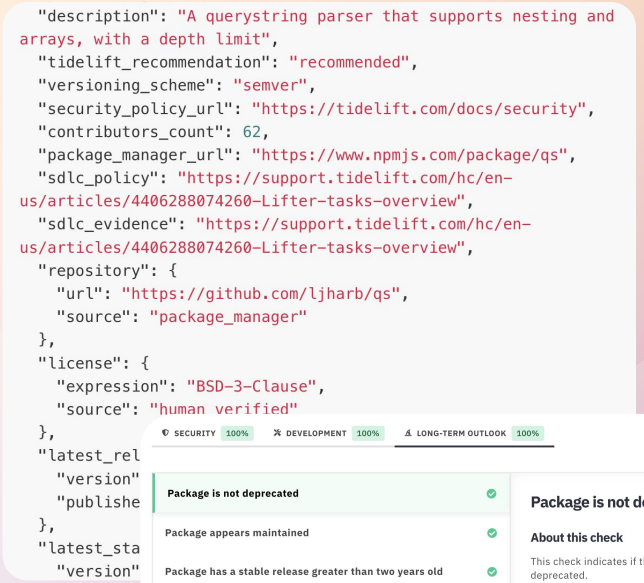
Reinforcing at-risk packages
to keep them from becoming bad

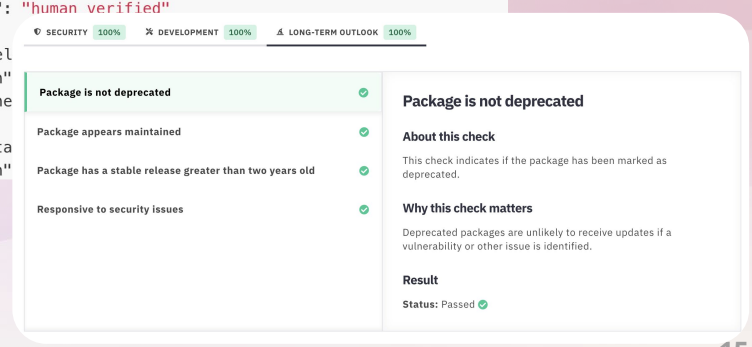
Evaluating packages before pulling them in for application development

When researching and evaluating open source packages to use, Tidelift's package recommendations provide an excellent starting point. The recommendation is a holistic evaluation of the package, and whether it is developed and maintained in a way that would make it a good fit for application development.

It is also easy to undertake deeper package analysis with answers to questions such as:

- Is it actively maintained or is it deprecated?
- Are the maintainers actively responding to security issues?
- Does it conform to my organization's license policies?

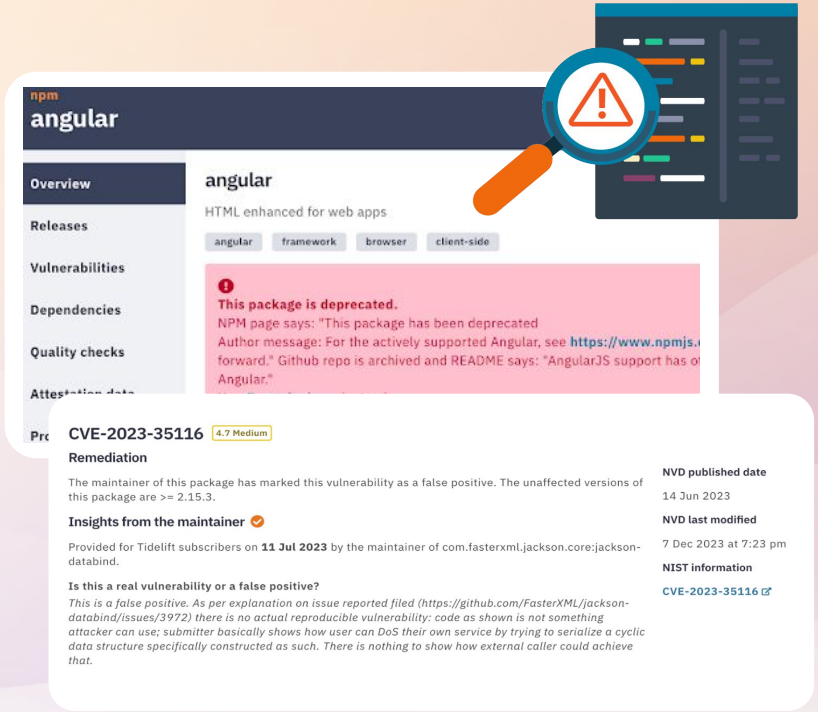




Actively monitoring the open source packages in use

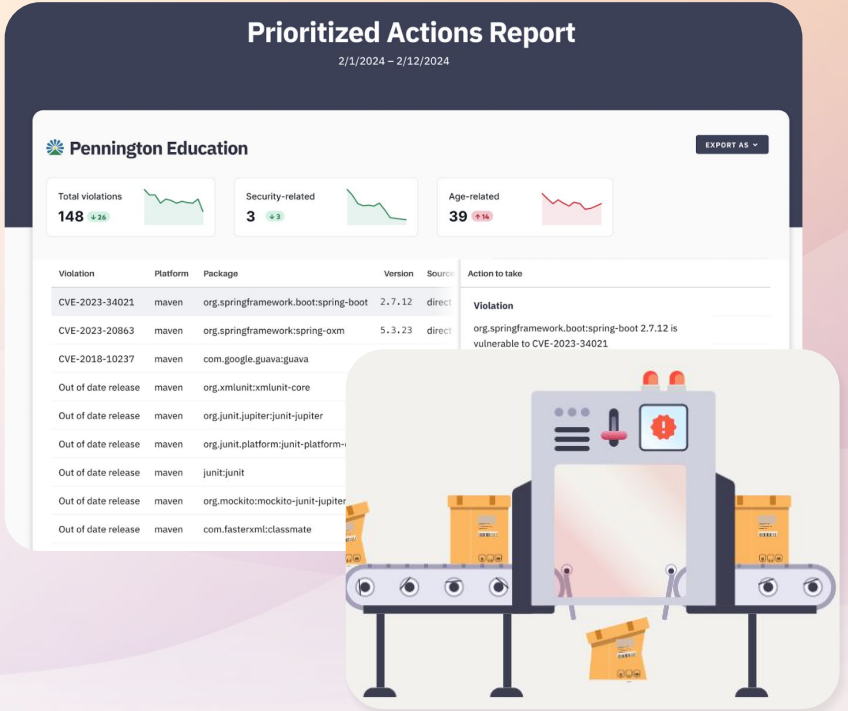
Open source packages are constantly changing and it is important to monitor and review updates after making the initial decision to use a package. **Tidelift makes it possible to identify bad packages through early warning signs such as**:

- New release availability, leading to end-of-support for older versions
- New versions released under different license types
- Package maintenance status changes
- Packages or versions getting impacted by vulnerabilities



Identifying and eliminating bad packages already adopted

- While it is ideal to identify and avoid bad packages in the first place, most organizations will have already adopted a significant number of packages without having done the upfront research.
- Tidelift helps organizations evaluate their existing open source dependencies and prioritize the work to migrate away from bad packages.
- Many maintainer partners also provide additional insights that can be used for prioritizing vulnerability remediation



Reinforcing at-risk packages to keep them from becoming bad

TIDELIFT

Maintainer case stories

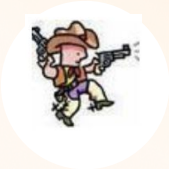
Case story: minimist

Maintainer Jordan Harband saved minimist from deletion when its maintainer decided to erase their projects from GitHub.

minimist is a highly relied upon JavaScript package used by many Tidelift customers and was a transitive dependency the Tidelift maintainer partner **Jordan Harband** pulled into his projects.

The minimist maintainer did not want to comply with npm's new 2FA requirement because he did not own a mobile phone, and rather than comply, **he decided to simply delete his entire GitHub account**, which would have impacted any organization that relied on minimist or his other packages.

Jordan stepped in to take over ownership of minimist and ensure it meets enterprise-grade secure software development practices. **Thanks to income from Tidelift and its customers**, Jordan has been to ensure minimist stays secure and reliable, and he was even able to bring on a co-maintainer for the project.



Case story: jackson-databind

Maintainer Tatu Saloranta used income from Tidelift and its customers to completely re-architect jackson-databind and eliminate the risk of RCE vulnerabilities.

jackson-databind is an extremely popular general purpose java data-binding package that is important to many Tidelift customers, several of whom had expressed concerns that it was being impacted by a large number of remote code execution (RCE) vulnerabilities. At least one customer was planning to re-architect jackson-databind out of their infrastructure because of this increased risk.

Thanks to income from Tidelift and its customers, Tatu was not only able to implement enterprise-grade secure software development practices for jackson-databind, he was able to re-architect to eliminate the risk of RCE vulnerabilities once at for all.

The customer previously planning to re-architect reported that the risk score had been reduced so much **they no longer needed to replace the package**.

TIDELIFT

About Tidelift

About Tidelift

Tidelift helps organizations reduce risk to their revenue, data, and business continuity by proactively improving the resilience of the open source powering their applications.

Tidelift partners with leading open source maintainers and pays them to implement industry-leading secure development practices and validate the practices they follow. With Tidelift, organizations have the tools and intelligence they need to confidently make long-term investments in the open source they depend on.

SELECTED CUSTOMERS

HUGHES An EchoStar Company
DARPA
AIR FORCE
JPL Jet Propulsion Laboratory California Institute of Technology
Fannie Mae
USGS

INVESTORS

FOUNDRY
GENERAL CATALYST
Dorilton Ventures
ae HORIZONX
ATLASSIAN Ventures
CISCO investments
KAISER PERMANENTE
Gartner COOL VENDOR 2022
IDC Innovator

Getting started

Watch a demo of the Tidelift Subscription

See how the Tidelift Subscription can help your organization avoid bad packages and use open source with confidence, so you can create more incredible software, even faster.

WATCH THE DEMO

Learn about the Tidelift maintainer advantage

Read maintainer case stories and learn how paying the maintainers *works*.

READ THE STORIES

Get detailed technical information about the Tidelift Subscription.

VISIT OUR TECHNICAL DOCUMENTATION

Get in touch

Contact us to schedule a time to chat live and learn more about how Tidelift can help you.

CONTACT US