TIDELIFT

Open-Source Security Through the Lens of Tidelift

BY: STEVE LANG

The software transparency movement is a catalyst driving positive change throughout the industry. At Cisco, we see the value of software transparency and we intend to play a leadership role in this space. We will continue to engage with customers, standards bodies and policy advisors to help define best practices and guidance related to software transparency. Today, we wanted to share some exciting improvements related to open-source security that our development teams are now able to leverage.

In a previous post regarding Third-Party Software Security Scanning, we described Cisco's internal service Corona that uses proprietary and commercially available scanning solutions to identify third-party software components. Corona also provides validation of applicable security posture characteristics within released Cisco software through forensic analysis of software components and associated risks. Since the original post, the Corona platform has evolved considerably and provides the foundation for Cisco to tackle recent initiatives such as the Software Bills of Materials and NIST's Secure Software Development Framework.

We have recently gone live with a new data source in Corona that gives us visibility into the secure development practices used by open-source maintainers, a risk vector for which we previously had limited data. This new data source is provided by Tidelift, a company that partners directly with open-source maintainers to implement and validate industry-leading secure software development practices. Tidelift's approach provides funding directly to open-source maintainers to develop secure software.

Cisco's internal development teams, using Corona enhanced with open-source metadata provided by Tidelift, can now access insightful package metadata and gain additional insights into vulnerabilities, including guidance directly from maintainers on severity, exposure and remediation. Cisco developers can quickly review recommended versions of packages in application languages such as Java, JavaScript and Python. Developers can run quality checks, read first-hand supplier (maintainer) data, retrieve accurate end-of-life information and also review OpenSSF scorecards. This enhanced visibility enables Cisco to drive a more innovative and strategic use of open source within our development pipelines while simultaneously reducing the overall cost of managing open source in our supply chain.

The Corona Third-Party Management platform is built on Cisco Vulnerability Management (formerly Kenna) to strategically prioritize development based on risk. With our newly integrated Tidelift data, Cisco's development teams now have a unified view of risk. This includes both package level exploits defined by CVEs and supplier specific risks such as secure development practices, maintainer counts and end of life information. Our developers also have a more comprehensive view of risk, including the transitive dependencies of open-source projects where they have little control over choices that upstream open-source developers are making. This broader perspective enables development teams to remediate risk more efficiently in our software.

As organizations increase the use of open source in their applications, they face the growing challenge of keeping it well maintained and secured at scale. We are excited to build upon our existing relationship with Tidelift as a Cisco Investments portfolio company by making Tidelift's capabilities available to internal developers across Cisco through the Corona service.

Further reading

Cisco blog

Explore the Tidelift Subscription

Learn more about the Tidelift maintainer advantage

Book a demo