EMPLOYERS® insurance works with Tidelift to improve technical hygiene and remediate Log4Shell vulnerability

When news of the critical vulnerability in popular Java logging tool Log4j broke, the team at EMPLOYERS® was ready. The level 10, zero-day vulnerability, dubbed Log4Shell, sent alarm bells ringing across enterprise organizations around the world in December 2021, and stole months of productivity as organizations scrambled to identify where the vulnerability might be lurking.

But not at EMPLOYERS, the century-old company that specializes in workers' compensation insurance. Steve Smythe, who leads the DevOps CI/CD team, evaluated over 150 projects overnight, and quickly identified which projects needed to be fixed right away. How?

"We could take Tidelift's information and put it in a JIRA™ ticket and assign it to the teams," Smythe said. "We did the big stuff first. We were very quickly able to identify the problem products we have."

That's the main reason EMPLOYERS brought Tidelift into their workflows. In Smythe's own words: they wanted to have the right tools to deal with the next zero-day fire drill. In Smythe's own words: "We didn't want to be the next [big breach in the news]."

Before Tidelift, Smythe's team was using server side scanning tools, which could bring in a lot of false positives—say someone downloaded a component and didn't actually end up using it—and didn't actually offer any clue as to where a vulnerability might be located, in which project, and how to fix it. Some of the other tools were rather intrusive, as well. They'd waste a lot of CPU time and not provide direct information when identifying an issue.

"When we picked Tidelift, the fact that I could drop in a couple of command line calls into my build scripts seamlessly and then replicate that out through all the rest of the fleet for all the build times—that was amazing," Smythe said.

Tidelift provides data straight from open source maintainers

When the security remediation team evaluated Tidelift originally, they were looking to deal with all CVEs level 7.5 and up, as well as license violations—an organization-wide attempt to clean up their technical debt and improve the health of their open source supply chain.

And from a security remediation point of view, Smythe said, no other vendor came close to the level of detail Tidelift provides—because Tidelift works directly with the open source maintainers of the projects EMPLOYERS and other enterprise organizations depend on.

"That relationship is pure gold," Smythe said. "The openness you have with the open source maintainers and the ability to talk with the consumers about how we're using their products—we have a direct line of communication from their fixes and what versions we should be using."

Smythe said that when they brought Tidelift in, they had a "firehose of data." But because they were able to see what information the maintainers provided, they could prioritize the most important fixes. And now they have a robust remediation process that their developers are responding to because Tidelift is filtering and prioritizing for them.

"We have specific cycles in the remediation process now," Smythe said. "We meet every week where we transfer the information from our remediation team to the engineering teams. Then the engineering teams have special sprints where they'll go through and do the remediation process."

A healthy software supply chain increases developer velocity

The number of CVEs for the team to deal with is shrinking—and soon they'll have time to deal with some of the smaller stuff. It's nice to have an agreed balance on feature development versus fixing issues, Smythe said. Before, security issues only got addressed when "word from up high comes down to stop the presses, fix this problem."

"Development hygiene has increased a lot in the last year," said Edwin Miller, EMPLOYERS InfoSec Operations Manager. "We're not creating as many problems to begin with as we used to. We're not adding fuel to the flame, and it's easier to keep everything under control as we go forward."

Tidelift also helps the team when choosing new components. The developers read the guidance from Tidelift and use the recommended version. "The hygiene there is amazing," Smythe said.

"We're getting good information in," said Miller. "So we're getting better information out."

This proactive and preventative approach is paying off. Instead of wasting months tracking down where EMPLOYERS was impacted by Log4Shell, Smythe and his team sorted everything out quickly.

Smythe won't hazard a guess about how long they would have been dealing with the Log4Shell situation without Tidelift. "A lot of it was transitive dependencies," Smythe said. Transitive dependencies are the open source components that an open source component you are using relies on—and it's really hard to track those down without Tidelift.

"The big problem is trying to find that mess by hand across 158 projects," Smythe said. "That means we'd have to run the materials generated across all of our Java maven projects and see where Log4j was in use."

But with Tidelift, everything was resolved in a few days. Now they continue to chip away at old issues, and the list is dwindling. Tidelift provides the tools, data, and strategies driving EMPLOYERS' organization-wide approach to improving the health and security of the open source powering their applications.

EMPLOYERS® is a registered trademark of EIG Services, Inc. Employers Holdings, Inc. is a holding company with subsidiaries that are specialty providers of workers' compensation insurance and services focused on select, small businesses engaged in low-to-medium hazard industries. The Company operates throughout the United States, with the exception of four states that are served exclusively by their state funds. Insurance is offered through Employers Insurance Company of Nevada, Employers Compensation Insurance Company, Employers Preferred Insurance Company, Employers Assurance Company and Cerity Insurance Company, all rated A- (Excellent) by the A.M. Best Company. Not all companies do business in all jurisdictions. See www.employers.com and www.cerity.com for coverage availability.