How to manage “hard-to-manage” OSS vulnerabilities

Almost **80%** of all software is made up of open source

Let’s be real - managing open source vulnerabilities is tough. In 2022 alone, there were over 28 000 new vulnerabilities published in Debricked’s monitored sources. And as your organization grows, this difficulty becomes more apparent. So, how should you go about tackling this hurdle?

One way to do this is to adopt a trustworthy SCA tool that won’t overload you with complexity and instead helps you streamline the process at scale, automatically.

Simplify the process

Know

This isn’t Pokemon: you do not need to catch ‘em all. It's essential to differentiate between "your" and "vulnerabilities."

Each open source package has about 500 dependencies, making it nearly impossible to manually keep track of known vulnerabilities and associated risks in your software. You'll want to focus on those that affect you, directly and indirectly. Overwhelmed by irrelevant alerts? No, thank you.

Prevent

Every time you add a new dependency, you take on a new risk. Inconvenient, huh?
But there are a few things you can look at that will help you make smarter choices: commit frequency, developer experience, past vulnerability handling, and dependency popularity.

Yet, predicting the future of a dependency isn’t easy. Take advantage of automation to shorten response time when risks are in sight.

Fix

Knowing about an open source vulnerability doesn't guarantee a fix. For example, a patched version might exist but updating the dependency without understanding the actual context will most likely break things downstream. On top of that, trying to find the right fix is like navigating a maze.

A reliable SCA tool identifies which version to update, saving you from manual, time-consuming, headache-triggering and error-prone tasks.

Next-gen SCA

The Debricked SCA goes beyond scanning, monitoring and warning. Just like you, we want working with secure, well-maintained and compliant open source to be a breeze.

With our cutting-edge solution, you have full control over all open source software integrated into your repositories and automatically keep out unwanted risks right from the outset. This means your team can code at speed while adhering to your organization’s policy. Shifting security to the early stage of your software development doesn’t cut it anymore. It’s better to make informed decisions and start left.

The Debricked database features:

+128M
repositories indexed

+12 000
open source licenses detected

+3.8M
projects scanned

debricked
by opentext™