activestate

Improve Security With a Bill of Materials

Discover vulnerabilities in the Python, Perl, Ruby or Tcl dependencies in your applications. The ActiveState Platform's Bill of Materials (BOM) feature gives you a comprehensive view of your open source dependencies, including any disclosed vulnerabilities (aka CVEs or Common Vulnerabilities and Exposures) so they can be fixed sooner rather than later. After all, the cost of fixing a defect escalates the closer to production you discover it.

Despite the fact that open source software generally provides more chances of finding and fixing vulnerabilities quicker, according to the US National Vulnerability Database (NVD), the number of discovered open source vulnerabilities has been escalating dramatically:

- **2006-2016** - 4,000 to 8,000 vulnerabilities per year
- **2017** -14,600 vulnerabilities per year
- **2019** - 22,000 vulnerabilities per year

Attackers only need one unpatched vulnerability to exploit, while defenders need to patch everything.

UNDERSTANDING APPLICATION RISK

Application risk varies over time as issues are found and fixed. But when application risk increases, it's likely to be for one or more of the following reasons:

- **Software Decay** - the longer an open source component is in use, the more chance a vulnerability or other defect will be found.
- **Large Attack Surface** - most applications consist of dozens if not hundreds of open source packages. A critical vulnerability in just one package can pose a significant security risk if not remediated in a timely manner.
- **Typosquatting** - attackers may copy a popular open source package, rename it something similar, add their own malicious code, and then upload it to the community's package repository. Unsuspecting developers may then accidentally use the package and unwittingly introduce a back door into their application.

The result is an ever-escalating number of data breaches, ransomware attacks and other cyber attacks.

APPLICATION SECURITY WITH BOMS

One of the most effective strategies for mitigating software vulnerabilities that arise in your open source supply chain is the BOM, which is simply a comprehensive list of ingredients required to build your application. A BOM can include:

- A version of the programming language
- Open source packages from the language's ecosystem, as well as their dependencies
- Operating system-level dependencies
- Proprietary code packages (ie., code your developers have written)
- Configurations (ie., metadata like version number, open source license, etc)
- A CVE report, showing vulnerabilities for each component

A BOM provides deep insight into the software application, all its parts, as well as any supply chain vulnerabilities. You can't secure what you don't know, but BOMs also reduce costs by saving hundreds of hours in risk analysis and vulnerability management.

THE ACTIVESTATE PLATFORM BOM

The ActiveState Platform provides a BOM view for all your Python, Perl, Ruby and Tcl open source components, identifying vulnerabilities at multiple levels, including:

- Python, Perl, Ruby and Tcl programming language
- Python, Perl, Ruby and Tcl ecosystem packages and dependencies (as well as dependencies of dependencies)
- Windows and Linux OS-level dependencies
- Configuration/versions

However, the interrelated nature of open source components means that patching a vulnerability at one level (ie., upgrading a package to the latest version to resolve a CVE) can have a cascading effect on other components. The ActiveState Platform highlights all changes before you commit to them, ensuring you understand the ramifications.

And unlike other BOM solutions, the ActiveState Platform can help further reduce application risk by providing:

- **Maintenance Over Time** - restore older versions of ecosystem and OS-level dependencies so you can recreate your original development environment and fix vulnerabilities in older versions of your application.
- **Builds from Source Code** - prevent supply chain attacks by automatically building all packages and dependencies from source code, ensuring against the inclusion of malicious code.
- **Reduced Attack Surface** - ensure your software incorporates only those packages and dependencies required to run the application in production.

Enable all stakeholders to better manage open source supply chain vulnerabilities and application security risks.

ActiveState is the de-facto standard for millions of developers around the world who have been using our commercially-backed, secure open source language distributions for over 20 years. With the ActiveState Platform, developers can now automatically build their own Python, Perl, Ruby or Tcl Environments for Windows, Linux or Mac—all without requiring language or operating system expertise.

NORTHROP GRUMMAN NASA Honeywell GE aviation

Contact us to see how easy it is to replace Anaconda with ActiveState Python

activestate

www.activestate.com • Toll-free in NA: 1-866.631.4581 • solutions@activestate.com