WhiteSource

When it comes to securing your open source components,

WhiteSource has you fully covered

Why Invest in Open Source Security?

Open source components are the core building blocks of modern applications. Recent studies show that open source components account for 60-80% of the software codebase.

Despite their heavy reliance on open source components and OWASP's Top 10 warning about the risk of using open source components with known vulnerabilities, development teams have generally been neglectful when it comes to ensuring that the open source components they use in their products meet basic security standards.

The risk of using open source components with known vulnerabilities increases as hackers understand the potential for mass destruction that lies in targeting open source vulnerabilities. This means that, once reported, an open source vulnerability becomes a ticking time bomb in your application.

The Challenges of Open Source Security

Application security testing technologies, like SAST, cannot detect vulnerabilities in open source components. A different approach is needed for securing open source components, which utilizes the publicly available information from the open source community as the resource for detecting and fixing vulnerabilities.

The good news is that the open source community is doing a great job securing open source projects. However, given the decentralized nature of open source, information about vulnerabilities is spread out across multiple resources. Some of these sources are not easily searchable, making it impossible for organizations to manually match vulnerabilities listed in these dispersed listings to those in their applications.

Added to this challenge is the issue of open source dependencies - since manual tracking usually doesn't cover transitive dependencies and, as all manual processes, is prone to error, organizations do not have accurate visibility as to which open source components they are using in their products. Without full transparency, organizations cannot detect all vulnerable components, leaving them exposed to exploitation.

Only automated tools are capable of continually monitoring the open source components in your applications and alerting of vulnerable or problematic components in real-time.

The Two Pillars of Open Source Security

VULNERABILITY DETECTION

You can't fix what you don't know you have. It's that simple. Accurate detection is critical in order to identify all the vulnerable open source components in your code, so that action can be taken to fix them.

Prioritizing Effective Vulnerabilities

Our Effective Usage Analysis **reduces 70% of open source vulnerabilities alerts**, helping development teams prioritize the issues that truly need fixing. By adding this never seen before technology we're able to reach better resolution in understanding which vulnerable functionalities are indeed effective (i.e. getting calls from the proprietary code).

The End to False Positives

Thanks to our proprietary algorithm, we match reported vulnerabilities to the actual affected open source libraries in your code, **ensuring no false positive alerts** that only waste your time and resources.

Comprehensive Database

Our database provides the largest coverage of vulnerability listings, with **more than 200 programming languages** supported and continuous monitoring of **multiple vulnerability databases** including the CVE/NVD, a wide range of security advisories, and popular open source projects issue trackers.

VULNERABILITY REMEDIATION

The challenge of open source vulnerability remediation is two-fold: Primarily, time is of the essence as hackers are exploiting open source vulnerabilities faster than ever before, especially when it comes to popular open source projects. Secondly, it is challenging for developers to fix a vulnerability in a code they did not write and are not familiar with.

Pinpointing the Path

WhiteSource provides **full trace analysis, pinpointing the vulnerable functionality in your code** and mapping out the way the vulnerability is being used in your application.
These actionable insights cuts remediation efforts significantly.

Suggested Fixes

Beyond sourcing vulnerabilities reported throughout the open source community, we also **aggregate their remediation possibilities as recommended by the community.** Ranging from links to patches to new versions, recommendations for system configuration changes to blocking a specific function, we list all known fixing options for you to choose from.

Automated Workflows

Automatically **initiate issue tickets on newly discovered vulnerabilities** or recently added vulnerable components and assign action items to ensure proper follow up and remediation of all urgency levels.

Automation is King

Enforce Policies Automatically Throughout The SDLC

WhiteSource enables you to automatically enforce your security, quality and license compliance policies to block vulnerable or problematic components and gain full control over your open source usage.

Setting up automated policies can reduce the number of new components you must manually review by 75-90%, thereby speeding up your software development process and freeing your developers to focus on building great products.

Shift Left & Shift Right Your Open Source Security

Shifting left helps teams to reduce costs and shorten time to fix by discovering issues earlier in the process. When it comes to open source, WhiteSource helps your developers to shift left as much as possible by alerting on vulnerable components while browsing the web with our browser extension - the Web Advisor.

The “shift right” approach is even more critical when it comes to open source, since in many cases vulnerabilities in open source projects are discovered years after the vulnerable version was released. This is why WhiteSource automatically tracks the last inventory of every deployed version and continuously monitors it for newly discovered vulnerabilities, alerting users if one of their historic versions becomes vulnerable.

Integrate Open Source Security Into Your CI/CD Pipeline

WhiteSource integrates out-of-the-box with all common software development and testing platforms to speed up your software development process and automate the entire process of open source components selection, approval, detection and remediation of open source security vulnerabilities.

THINK WE’RE EXAGGERATING? TRY US OUT!

Sign up for a free trial and be amazed by the ease and accuracy of the WhiteSource solution.

www.whitesourcesoftware.com