

DATASHEET

Veracode Fix for SCA

Automated Remediation for Open-Source Security that Doesn't Break Your Code

The reliance on open-source libraries accelerates innovation but introduces significant security risk. A single vulnerable dependency can create a ripple effect across an entire application portfolio. Identifying these vulnerabilities is only the first step. Manually researching, selecting, and testing secure library updates is a time-consuming and complex process that slows down development pipelines and increases security debt. Veracode Fix for SCA automates this entire workflow, enabling you to secure your third-party code with confidence and precision.

Take Control with Veracode Fix

Veracode Fix for Software Composition Analysis (SCA) extends our AI-powered remediation capabilities to your software supply chain. It automatically identifies and generates secure code fixes for vulnerabilities in open-source dependencies, empowering you to manage risk without slowing down development. By analyzing the impact of library upgrades on your first-party code, Veracode Fix ensures that every recommended change secures your application without introducing changes that break your code.

Why Veracode Fix for SCA?

- **Automated, Context-Aware Fixes:** Generates ready-to-merge pull requests that suggest the optimal secure library version while minimizing the risk of breaking your builds.
- **Proprietary Intelligence:** Leverages Veracode's industry-leading vulnerability database, curated by our in-house security research team, for the most accurate and comprehensive data.
- **Seamless Workflow Integration:** Integrates directly into Git-based source code management systems (e.g., GitHub, GitLab), meeting developers where they work.
- **Developer-First Experience:** Provides clear, actionable fixes that reduce security chores and allow teams to focus on delivering new features.



KEY USE CASES & BENEFITS

Reduce Risk Quickly: Remediate open-source risk with automated, context-aware fixes that integrate directly into developer workflows.

Increase Efficiency: Substantially reduce the manual effort required to fix open-source vulnerabilities. Automated pull requests with secure library versions eliminate tedious research and testing.

Accelerate Development: Fix security flaws in minutes, not months. By delivering ready-to-merge pull requests, developers can remediate vulnerabilities without context switching or disrupting their workflow.

Reduce Risk & Prevent Breaking Changes: Systematically reduce security debt from third-party code. Our contextual analysis evaluates the impact of upgrades on your first-party code, ensuring application stability and building developer trust.

Empower Developers: Equip your team with a tool that makes it easy to secure open-source dependencies. Seamless integration into their existing toolchains drives adoption and improves productivity.

Veracode Fix

Save time with AI-Powered Automated Code Remediation.



TECHNICAL SPECS

Supported Languages:

Supports popular programming languages and ecosystems. Contact us for a complete, up-to-date list.

Integration Points:

Command Line Interface (CLI): Enables powerful, scriptable interactions.

Source Code Management (SCM): GitHub, GitLab, and other Git-based systems.

Supported Scans:

Software Composition Analysis (SCA) Agent-Based Scans



KEY FEATURES

- ✓ **Automated Pull Requests:** Generates ready-to-merge pull requests with secure library versions to accelerate remediation.
- ✓ **Contextual Analysis of First-Party Code :** Prevents breaking changes and ensures application stability by analyzing the impact of library updates.
- ✓ **Integration with Developer Toolchains:** Seamlessly fits into existing Git-based workflows, enhancing productivity and driving adoption. .
- ✓ **Proprietary Vulnerability Database:** Provides accurate and comprehensive vulnerability intelligence for precise, reliable fixes.
- ✓ **Simple Execution:** A single “fix” command delivers secure patches without manual effort.

How It Works



SCAN & IDENTIFY

Veracode SCA scans your application and detects vulnerabilities in open-source libraries.

AI ANALYSIS

Veracode Fix analyzes the vulnerability, cross-references it with our proprietary database, and evaluates the impact of potential upgrades on your first-party code. It then generates a pull request with the optimal secure version.



GENERATE FIX

Produces a secure patch (e.g., URLEncoder for log sanitization).

APPLY SEAMLESSLY

The developer reviews the automated pull request within their source code management tool, sees that all checks have passed, and merges the change.

VALIDATE

The vulnerability is fixed in minutes with minimal disruption, reducing security debt and keeping development velocity high.

Contact Us

Contact us today to learn more about how Veracode Fix can help you reduce risk and secure your application security. Contact our team at www.veracode.com schedule a demo or request additional information.

VERACODE