Secure Development Lifecycle

Summary

JAMS Software
108 Patriot Drive, Suite A
Middletown, DE 19709

JAMS Secure Development Lifecycle

Overview

JAMS has invested in security processes and practices that follow industry standards. Processes, security tools, and testing methods employed help address issues such as the OWASP Top 10 most critical web application flaws and CWE/SANS Top 25 most dangerous software errors. Our layered process includes training, testing and security expertise, tools, and automation to produce secure products. This process enables prevention, detection, and response to security issues that are identified. The latest threat intelligence is used to keep our secure development processes up to date with the newest threats and vulnerabilities. JAMS continually works to incorporate new security features into our products as part of its development strategy.

Training

Secure development training is required for personnel involved in software development. Training includes general software security principles and concepts as well as technology specific guidance. SAFECode and OWASP developer education frameworks strongly influence this training.

Security Assessments

The JAMS team is tasked with performing periodic assessments to verify that required secure processes, policies and practices are being followed. Periodic secure software assessments are performed by JAMS team members based on the OWASP Application Security Verification Standard (ASVS).

Independent, 3rd party security testing vendors, perform external scans and penetration tests periodically to help ensure software meets or exceeds industry standards.

Test results are delivered to development teams and findings are remediated based on severity, impact, and likelihood of exploitation.

JAMS Software
108 Patriot Drive, Suite A
Middletown, DE 19709

Security Requirements & Architecture

During requirements gathering, security, privacy, and quality targets are defined and reviewed as needed and appropriate to the development cycle and software components being developed. An assessment of the application risk is performed to understand the likelihood and impact of attacks against the software. Strategies and controls are implemented to mitigate the identified threats.

JAMS reviews the design and deployment standards for our applications to determine appropriate security configurations. Requirements such as encrypted payloads, SSL certificate checks, at rest encryption, and application security checks are reviewed. End user access points and credential input methods are reviewed and verified. Applications are designed to minimize the potential attack surface. JAMS reviews the types and amounts of data that are expected to be created and/or retained by the end user to ensure that the recommended application configuration is appropriately sized and secure.

Code Review

During the development process, changed or impacted code is reviewed and tested by trusted and experienced team members as part of the Secure Development Lifecycle.

Vulnerability and Defect Management

Issues identified by JAMS and 3rd party testing are logged in the defect tracking system, scheduled for remediation, and prioritized by severity. Security issues receive priority attention based on severity, impact, and likelihood of exploitation.

Secure Build

JAMS developers utilize approved tools and components during application creation. Industry standard development environments are used which contain processes like compile time checks for proper coding standards. Source is kept in a version control system and consistent build environments are maintained. Defects, source code artifacts, and design documents are archived at each build point within the development process.

JAMS Software
108 Patriot Drive, Suite A
Middletown, DE 19709

Testing

Verification of product quality is performed by various qualified team members. Multiple tools and automated testing techniques are utilized throughout the Agile development process to ensure product and configuration consistency and quality. Security functionality is explicitly tested following industry guidelines such as those outlined by OWASP and NIST. Tests are based on functional specifications and requirements and include negative tests, load, input boundary analysis, and input combinations.

Secure Deployment

JAMS follows a formal release process that leverages input and approval from multiple stakeholders within the company. Once designees have affirmed that the product is ready to be used by end customers, a formal designation of Generally Available is declared and announcements are made to all relevant internal and external parties. Product maintenance releases are produced as warranted to address critical issues or incorporate new and updated product features. Throughout the build and deployment process, JAMS employs numerous controls and checks to ensure supply chain security.

JAMS Software
108 Patriot Drive, Suite A
Middletown, DE 19709