

Statement of Compliance for SAFECode Development Practices

Abstract

EventTracker is a powerful and dynamic Security Information Event Management (SIEM) and event log management solution that processes hundreds of millions of discrete log messages to distill and deliver the most vital and actionable data to your organization. EventTracker provides a 360 degree view of the entire IT infrastructure, offering real-time alerting and reporting. EventTracker allows organizations to maintain continuous compliance, improve the IT security posture, and increase operational uptime.

EventTracker architecture mainly comprises of two components, Web and Engine. EventTracker and its components rely on Operating System, IIS webserver and SQL database for its functional requirements.

With the increase in data management, it is important to safeguard EventTracker application and its pre-requisites against various known security threats and hence follow any standard security best practices that are available in the industry.

The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services.

EventTracker has adopted SAFECode development practices as one standard while implementing various best practices for a secure software code development. EventTracker is designed after having considered the various dynamic and complex security threats that exist within the modern enterprise environment.

This document describes compliance with SAFECode Development Practices.

References

*MSLOGO Guidelines

<http://msdn.microsoft.com/en-us/windowsserver/hh833799>

*OWASP Guidelines

https://www.owasp.org/index.php/Main_Page

SAFECode Guidelines

http://www.safecode.org/publications/SAFECode_Dev_Practices1108.pdf

Statement of Compliance with SAFECode Development Practices

S.No.	SAFECode	Supported Features
1	Minimize unsafe function use	Supported by ongoing effort. Continuous security process adopted across the Development, Testing, Release, Install, Maintenance phases. EventTracker adheres to MSLOGO* guidelines; these use cases are specifically targeted.
2	Use the latest compiler toolset	Supported by ongoing effort. Continuous security process adopted across the Development, Testing, Release, Install, Maintenance phases. EventTracker adheres to MSLOGO* guidelines; these use cases are specifically targeted.
3	Use static and dynamic analysis tools	Supported by ongoing effort. Continuous security process adopted across the Development, Testing, Release, Install, Maintenance phases. EventTracker adheres to MSLOGO* guidelines; these use cases are specifically targeted.
4	Manual code review	Supported by ongoing effort. Continuous security process adopted across the Development, Testing, Release, Install, Maintenance phases. EventTracker adheres to MSLOGO* guidelines; these use cases are specifically targeted.
5	Validate input and output	Supported. EventTracker satisfies OWASP* guidelines and is well behaved in this situation. Please refer the link mentioned above for OWASP guidelines.
6	Use anti-cross site scripting libraries	Supported by ongoing effort. Continuous security process adopted across the Development, Testing, Release, Install, Maintenance phases. EventTracker adheres to MSLOGO* guidelines; these use cases are specifically targeted.

S.No.	SAFECode	Supported Features
7	Use canonical data formats	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
8	Avoid string concatenation for dynamic SQL	Supported by ongoing effort. Continuous security process adopted across the Development, Testing, Release, Install, Maintenance phases. EventTracker adheres to MSLOGO* guidelines; these use cases are specifically targeted.
9	Eliminate weak cryptography	Supported. EventTracker uses FIPS compliant cryptography modules and algorithms.
10	Use logging and tracing	Supported.