EventTracker

Actionable Security Intelligence

Statement of Compliance for OWASP

Personal and Confidential

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 by following any standard security best practices that are available in the industry.

The Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software. The OWASP Top 10 Most Critical Web Application Security Risks represents a broad consensus about what the most critical web application security flaws are.

The EventTracker engineering team has adopted the OWASP Testing Guide v3 as a core standard. This document is a statement of compliance with this testing guide.

References

***OWASP Guidelines and Testing Guide**
https://www.owasp.org/index.php/Main_Page
https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

OWASP Guidelines

Category	Description	Supported Features
Input and Data Validation	All vulnerabilities that can occur through the input fields like SQL injection, XSS attack, and XML injection should be addressed.	Supported. EventTracker satisfies OWASP* guidelines and is well behaved in this situation. Please refer the link for OWASP Guidelines.
Authentication	Any attempt to bypass authentication or path traversal scenario to identify the unknown usernames and passwords should not be successful.	Not Applicable. EventTracker depends on Windows Authentication which can be either Active Directory or local host based
Authorization	Application should not provide access controls for resources and operations which are not authorized to any specific user.	Supported. EventTracker satisfies OWASP guidelines and allows access after verification of proper authorization.
Configuration Management	The overall configuration of the application with external and internal entities must be handled securely.	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
Sensitive Data	Application should protect sensitive data either in memory, over the network, or in persistent stores.	Supported. EventTracker will not expose any sensitive data.
Session Management	A session refers to a series of related interactions between a user and your Web application. Application should handle user sessions securely.	Supported. EventTracker satisfies OWASP guidelines and sessions are securely managed.
Denial of Service	Any attempt to make a machine or network resource unavailable to its intended users should not be successful.	Supported. EventTracker satisfies OWASP guidelines and is properly handled.