EventTracker

Actionable Security Intelligence

Statement of Compliance for CWE/SANS Top 25 Software Errors

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.

The CWE/SANS Top 25 Most Dangerous Software Errors is the result of collaboration between the SANS Institute, MITRE, and many top software security experts in the US and Europe. It leverages experiences in the development of the SANS Top 20 attack vectors (http://www.sans.org/top20/) and MITRE's Common Weakness Enumeration (CWE) (http://cwe.mitre.org/). MITRE maintains the CWE web site, with the support of the US Department of Homeland Security's National Cyber Security Division, presenting detailed descriptions of the top 25 programming errors along with authoritative guidance for mitigating and avoiding them. The CWE site contains data on more than 800 programming errors, design errors, and architecture errors that can lead to exploitable vulnerabilities.

As part of the development phase, EventTracker incorporates this list. This document is a statement of compliance with the list.

References

***MSLOGO Guidelines**
http://msdn.microsoft.com/en-us/windowsserver/hh833799

***OWASP Guidelines**
https://www.owasp.org/index.php/Main_Page

***SANS Top 25 Most Dangerous Software Errors**
http://www.sans.org/top25-software-errors/

SANS Top 25 Software Errors – EventTracker Security Statement

CWE ID	Description of the Vulnerability	Supported Features
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Supported. EventTracker satisfies OWASP* guidelines and is well behaved in this situation. Please refer the link mentioned below for OWASP guidelines
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Supported. EventTracker satisfies OWASP guidelines and is securely coded against XSS attack.
CWE-434	Unrestricted Upload of File with Dangerous Type	Not Applicable EventTracker does not support this feature
CWE-352	Cross-Site Request Forgery (CSRF)	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	Not Applicable EventTracker does not support this feature
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Supported. EventTracker satisfies OWASP guidelines and allows access after verifying for proper authorization

CWE ID	Description of the Vulnerability	Supported Features
CWE-494	Download of Code Without Integrity Check	Not Applicable EventTracker does not support this feature
CWE-829	Inclusion of Functionality from Untrusted Control Sphere	Not Applicable EventTracker does not support this feature
CWE-676	Use of Potentially Dangerous Function	Continuous security process been adopted EventTracker adheres to MSLOGO* guidelines and was handled this vulnerability as a part of it. Also it is maintained as a part of Security Development Life Cycle process. Please refer the link for MSLOGO guidelines.
CWE-131	Incorrect Calculation of Buffer Size	Continuous security process been adopted EventTracker adheres to MSLOGO* guidelines and was handled this vulnerability as a part of it. Also it is maintained as a part of Security Development Life Cycle process. Please refer the link for MSLOGO guidelines.
CWE-134	Uncontrolled Format String	Continuous security process been adopted EventTracker adheres to MSLOGO* guidelines and was handled this vulnerability as a part of it. Also it is maintained as a part of Security Development Life Cycle process. Please refer the link for MSLOGO guidelines.
CWE-190	Integer Overflow or Wraparound	Continuous security process been adopted EventTracker adheres to MSLOGO* guidelines and was handled this vulnerability as a part of it. Also it is maintained as a part of Security Development Life Cycle process. Please refer the link for MSLOGO guidelines.

CWE ID	Description of the Vulnerability	Supported Features
CWE-306	Missing Authentication for Critical Function	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
CWE-862	Missing Authorization	Supported. EventTracker satisfies OWASP guidelines and it authorizes the resources and operations in a secured way.
CWE-798	Use of Hard-coded Credentials should be avoided.	Supported. EventTracker will not hard-code any credentials.
CWE-311	Missing Encryption of Sensitive Data should be handled properly	Supported. EventTracker satisfies OWASP guidelines and does not expose any sensitive data.
CWE-807	Reliance on Untrusted Inputs in a Security Decision should be taken care properly	Supported. EventTracker satisfies OWASP guidelines. EventTracker sessions and cookies are securely handled.
CWE-250	Execution with Unnecessary Privileges	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.
CWE-863	Incorrect Authorization	Supported. EventTracker satisfies OWASP guidelines and allows access after verifying for proper authorization.
CWE-732	Incorrect Permission Assignment for Critical Resource	Supported. EventTracker satisfies OWASP guidelines and is well behaved in this situation.

CWE ID	Description of the Vulnerability	Supported Features
CWE-327	Use of a Broken or Risky Cryptographic Algorithm	Supported. EventTracker uses FIPS compliant certificates.
CWE-307	Improper Restriction of Excessive Authentication Attempts	Not Applicable EventTracker depends on Windows Authentication which can be either Active Directory or local host based
CWE-759	Use of a One-Way Hash without a Salt	Not Applicable EventTracker does not support this algorithm