Certification Report

EAL 2+ Evaluation of

Prism Microsystems

EventTracker Version 6.3 Build 93

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-136-CR
Version:	1.0
Date:	10 September 2010
Pagination:	i to iii, 1 to 9

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1* Revision 3. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, General requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 10 September 2010, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarked or registered trademarks:

- Windows is a registered trademark of Microsoft Corporation in the United States and other countries; and
- Microsoft Access is a registered trademark of Microsoft Corporation.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

Prism Microsystems EventTracker Version 6.3 Build 93 (hereafter referred to as the EventTracker Version 6.3), from Prism, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

EventTracker Version 6.3 is an Enterprise-class Security Information and Event Management (SIEM) solution that automatically collects and provides real-time analysis of logs and events from Windows systems and other devices that support the Syslog protocol. EventTracker Version 6.3 also accepts batch feeds of log files.

EventTracker Version 6.3 performs analysis of the real-time feeds. The feeds are also correlated to detect composite events. Alerts are generated for both single-feed events and composite events according to the configured policy. A cache of recent real-time and composite events is maintained for dashboard displays to administrators. The original logs from all the sources (both real-time and batch) as well as composite events are retained in a secure repository for later analysis and reporting. EventTracker Version 6.3 supplies both analytics and reporting engines for forensic analysis. Reports may be used for long-term trend analysis or compliance purposes.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 11 August 2010 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for EventTracker Version 6.3, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 2 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1* Revision 3, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1* Revision 3. The following augmentation is claimed:

ALC_FLR.2 - Flaw Reporting Procedures.

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the EventTracker Version 6.3 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is Prism Microsystems EventTracker Version 6.3 Build 93 (hereafter referred to as EventTracker Version 6.3), from Prism.

2 TOE Description

EventTracker Version 6.3 is an Enterprise-class Security Information and Event Management (SIEM) solution that automatically collects and provides real-time analysis of logs and events from Windows systems and other devices that support the Syslog protocol. EventTracker Version 6.3 also accepts batch feeds of log files.

EventTracker Version 6.3 performs analysis of the real-time feeds. The feeds are also correlated to detect composite events. Alerts are generated for both single-feed events and composite events according to the configured policy. A cache of recent real-time and composite events is maintained for dashboard displays to administrators. The original logs from all the sources (both real-time and batch) as well as composite events are retained in a secure repository for later analysis and reporting. EventTracker Version 6.3 supplies both analytics and reporting engines for forensic analysis. Reports may be used for long-term trend analysis or compliance purposes.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the EventTracker Version 6.3 is identified in Section 6 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Prism Microsystems EventTracker Version 6.3 Build 93 Security Target
Version: 1.6
Date: 22 June 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1* Revision 3 for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1* Revision 3.

EventTracker Version 6.3 is:

a. Common Criteria Part 2 extended, with functional requirements based on functional components in Part 2, except for the following explicitly stated requirements defined in the ST;
   - IDS_ADC.1, Analyser Data Collection;
   - IDS_ANL.1, Analyser Analysis;
   - IDS_RCT.1, Analyser React;
   - IDS_RDR.1, Restricted Data Review;
   - IDS_STG.1 Analyser Data Storage; and
   - IDS_STG.2 Analyser Data Storage.

b. Common Criteria Part 3 conformant, with security assurance requirements based on assurance components in Part 3; and

c. Common Criteria EAL 2 augmented, with all the security assurance requirements in the EAL 2, as well as the following: ALC_FLR.2 - Flaw Reporting Procedures.

6 Security Policy

Administrators configure policies to specify how the TOE will generate alerts to real time feeds or to information that has been received as batch files and stored for later analysis.

In addition, EventTracker Version 6.3 implements policies pertaining to Audit and Security Management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the EventTracker Version 6.3 product should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

a. There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains;

b. The authorized administrator is not careless, willfully negligent or hostile, and will follow and abide by the instructions in the TOE documentation; and

c. The TOE is located in a controlled access facility and can only be accessed by authorized users.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

a. The IT Environment will protect information transmitted to the TOE from remote systems;

b. The IT Environment will protect TOE data from modification from outside the TOE Scope of Control;

c. The IT Environment will restrict access to authorized administrators that must be identified and authenticated prior to accessing TOE functions and data;

d. The IT Environment must collect and forward to the TOE information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets; and

e. Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE and must ensure its physical security.

7.3 Clarification of Scope

The TOE depends on the operational environment to protect the integrity of the communication between the TOE and the remote systems supplying real-time security events to the TOE. The TOE does not perform Identification and Authentication. The operating system EventTracker Version 6.3 is installed on must perform that function, and control what users have access to the EventTracker Version 6.3 executables. EventTracker Version 6.3 considers all users with access to it to be a single role – administrators.

8 Evaluated Configuration

The evaluated configuration comprises Prism Microsystems EventTracker Version 6.3 Build 93 running on Windows 2003 Server and Windows 2008 Server.

The publication entitled *EventTracker Common Criteria Installation Supplement v1.0* contains instructions for installing this system in the evaluated configuration.

9 Documentation

The Prism documents provided to the consumer are as follows:

a. EventTracker User's Guide Version 6.3;

b. EventTracker Installation Guide Version 6.3;

c. EventTracker v6.3 Direct Log Archiver v1.0; and

d. EventTracker Common Criteria Installation Supplement v1.0.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the EventTracker Version 6.3, including the following areas:

Development: The evaluators analyzed the EventTracker Version 6.3 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the EventTracker Version 6.3 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance Documents: The evaluators examined the EventTracker Version 6.3 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support: An analysis of the EventTracker Version 6.3 configuration management system and associated documentation was performed. The evaluators found that the EventTracker Version 6.3 configuration items were clearly marked. The developer’s configuration management system was observed during a site visit, and it was found to be mature and well developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of EventTracker Version 6.3 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Prism for EventTracker Version 6.3. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of EventTracker Version 6.3. Additionally, the evaluators conducted a review of public domain vulnerability databases. The evaluators did not identify and potential vulnerabilities for testing applicable to EventTracker Version 6.3 in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer’s test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification and TOE design was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach was the following list of EWA-Canada test goals:

a. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer’s Installation and Administrative guidance;

b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator’s TOE installation; and

c. Independent Evaluator Testing: The objective of this test goal is to exercise the TOE’s claimed functionality through evaluator independent testing and to augment any areas that were not covered during the repeat of developer testing including areas surrounding system initialization, application monitoring and Service restart.

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

11.3 Independent Penetration testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, the independent vulnerability assessment did not uncover any exploitable vulnerabilities in the intended operating environment. Based on this assessment, the usual penetration testing was not conducted, however tests were run to assure that device settings were proper, such that USB functionality could be disabled on the Agent PC, if so configured.

11.4 Conduct of Testing

EventTracker Version 6.3 was subjected to a comprehensive suite of formally documented, independent functional tests. The testing took place at the Information Technology Security Evaluation and Testing (ITSET) Facility at EWA-Canada. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that EventTracker Version 6.3 behaves as specified in its ST, functional specification, TOE design, and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

EventTracker Version 6.3 is straightforward to configure, use and integrate into a corporate network by following the comprehensive Installation and User guidance.

Assumptions regarding the installation of the TOE and its operational environment must be met to ensure a secure deployment.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
ACLs	Access Control Lists
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme

Acronym/Abbreviation/ Initialization	Description
CPL	Certified Products list
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
SIEM	Security Information and Event Management
SFP	Security Function Policy
SFR	Security functional requirements
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

15 References

This section lists all documentation used as source material for this report:

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1Revision 3, July 2009.

d. Prism Microsystems EventTracker Version 6.3 Build 93 Security Target, Version 1.6, 22 June 2010.

e. Evaluation Technical Report (ETR) EventTracker Version 6.3 Build 93, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-136, Document No. 1636-000-D002, Version 1.5, 11 August 2010.