Certification Report

EAL 2+ Evaluation of

Triumfant Resolution Manager 4.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-83-CR
Version: 1.0
Date: 4 February 2009
Pagination: i to iv, 1 to 11

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 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. 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 (CSEC), 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 CSEC, 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 (CSEC).

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 Standard 17025, General requirements for the accreditation of calibration and testing 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 DOMUS IT Security Laboratory, a division of NUVO Network Management, 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 4 February 2009, 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 at: http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-eng.html and http://www.commoncriteriaportal.org/

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

- Triumfant and Resolution Manager are registered trademarks of Triumfant, Inc.
- Windows is registered trademark of Microsoft Corporation

TABLE OF CONTENTS

Executive Summary

Triumfant Resolution Manager 4.2 (hereafter referred to as Resolution Manager 4.2) is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Resolution Manager 4.2 is a software-only incident and problem detection and resolution management system. Agents are installed onto workstations, laptops, and servers to gather detailed state and status information. Resolution Manager 4.2 extracts statistically significant relationships from this information, analyzes the state of each machine on a routine basis to discover anomalies, or deviations from normal for a specific customer environment, and triggers a variety of automated responses to notify administrators or automatically and optionally remediate the condition by precision removal or replacement of the files and registry settings that uniquely identify the condition.

DOMUS IT Security Laboratory, a division of NUVO Network Management, is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on January 8 2009, 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 Resolution Manager 4.2, 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 IT Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to *Common Criteria for IT Security Evaluation, version 2.3*. The following augmentations are claimed:

- ALC_FLR.1 – Basic flaw remediation; and
- ADV_SPM.1 - Informal TOE Security Policy Model.

Communication Security Establishment Canada, as the CCS Certification Body, declares that

[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.

the Resolution Manager 4.2 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 the Triumfant Resolution Manager 4.2, (hereafter referred to as Resolution Manager 4.2) from Triumfant, Inc.

2 TOE Description

Resolution Manager 4.2 is a software-only incident and problem detection and resolution management system. Agents are installed onto workstations, laptops, and servers to gather detailed state and status information. Resolution Manager 4.2 extracts statistically significant relationships from this information, analyzes the state of each machine on a routine basis to discover anomalies, or deviations from normal for a specific customer environment, and triggers a variety of automated responses to notify administrators or automatically and optionally remediate the condition by precision removal or replacement of the files and registry settings that uniquely identify the condition.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Resolution Manager 4.2 is identified in Section 5 of the Security Target (ST).

4 Security Target

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

Title: Triumfant, Inc. Resolution Manager 4.2 Security Target
Version: 1.2
Date: 22 December 2008

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.3,* incorporating all final CC interpretations.

The Resolution Manager 4.2 is:

a. Common Criteria Part 2 extended, with security functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - RES_SDC.1 – System Data Collection;
    - RES_ANL.1 – Analyser Analysis;

- RES_RCT.1 – Analyser React;
- RES_SEL.1 – Selective Data Collection; and
- RES_STG.2 – Prevention of System Data Loss.

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

c. Common Criteria EAL 2 augmented, containing all security assurance requirements in the EAL 2 package, as well as the following:
   - ALC_FLR.1 – Basic Flaw Remediation; and
   - ADV_SPM.1 – Informal TOE Security Policy Model.

6 Security Policy

The Resolution Manager 4.2 implements an access control policy, functionality which is provided by the Resolution Manager 4.2 WebUI and Admin Console, by controlling access by operators to the data collected for analysis. Further details of the security policy can be found in Section 5.1 of the ST.

In addition, the Resolution Manager 4.2 implements other Security policies relating to:

- Incident and problem detection and resolution;
- Identification and authentication;
- Resource Management;
- Security management; and
- Protection of TOE Security Functions.

Further details on these security policies may be found in Section 5.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the Resolution Manager 4.2 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment.

7.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- Operators are non-hostile, appropriately trained, and follow all operator guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE components (Analytic Engine, the Collector, and the MySQL database) will be located within controlled access facilities, which will prevent unauthorized physical access;
- The TOE Environment will identify and authenticate console operators prior to allowing access to TOE administrative functions and data; and
- The TOE Environment will identify and authenticate Remedy helpdesk operators prior to allowing access to TOE administrative functions and data.

For more information about the TOE security environment, refer to section 3 of the ST.

7.3 Clarification of Scope

The TOE provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks to violate system security, particularly from within the physical zone or domain of deployment. The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel and communications security.

8 Architectural Information

Resolution Manager 4.2 is a software-only incident and problem detection and resolution management system. It is composed of four main components and subsystems:

- Agent;
    - Agent Subsystem
- Collector;
    - Agent Management Subsystem
    - Data Bridge Subsystem
    - Web User Interface Subsystem

  - Remedy Subsystem
  - Web Service Subsystem
  - Remediation Subsystem
  - Business Objects Subsystem
- MySQL Database; and
  - MySQL Database Subsystem
- Analytic Engine/Admin console.
  - Admin Console Subsystem
  - Task Processor Controller Subsystem
  - Task Processor Subsystem
  - Resolution Manager Monitor Subsystem

Agents are installed onto workstations, laptops, and servers to gather detailed state and status information. The Collector manages the actions of the agents and collects and process snapshots from the agents. The MySQL Database provides non-volatile storage for all non-configuration server data. The Analytic Engine/Admin Console performs data analysis and provides an administrative console for the console operator to perform management functions on the system.

9 Evaluated Configuration

The evaluated configuration comprises the following Resolution Manager 4.2 software: Agents, running on Microsoft Windows XP SP2 operating systems; Collector, MySQL database, and Analytic Engine/Admin Console, which are running on Microsoft Windows 2003 server operating systems.

For all components except the WebUI, the version for the TOE is 4.2.67. The WebUI version is 4.2.25.

For this CC evaluation, the Collector, MySQL Database, and Analytic Engine/Admin Console components of the TOE shall reside on a single server. Meanwhile, for the CC evaluated version of the TOE, a Triumfant engineer (either a sales engineer or a customer service engineer) is to deliver the TOE to the customer directly and install the TOE at the customer's site. This will ensure the proper and secure operation of the TOE.

For evaluated configuration detail refer to Section 2.3 of the ST.

10 Documentation

The Triumfant, Inc. documents provided to the consumer are as follows:

- Triumfant, Inc. Resolution Manager 4.2 Guidance Supplement;
- Triumfant Resolution Manager Release 4.2 Web Interface User's Guide; and
- Triumfant Resolution Manager Release 4.2 System Administration Guide.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Resolution Manager 4.2 including the following areas:

Configuration management: An analysis of the Resolution Manager 4.2 configuration management system and associated documentation was performed. The evaluators found that the Resolution Manager 4.2 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.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the Resolution Manager 4.2 during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the Resolution Manager 4.2 functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the Resolution Manager 4.2 administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators reviewed the flaw remediation procedures used by Triumfant for the Resolution Manager 4.2. 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 Resolution Manager 4.2 ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the Resolution Manager 4.2 and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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

12 ITS Product Testing

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

12.1 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 and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

12.2 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 DOMUS IT Security Laboratory test goals:

[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.

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. User Data Protection: The objective of these tests is to determine the TOE's ability to enforce access control on the data gathered from the targeted workstations;

c. Identification and Authentication: The objective of these tests is to determine the TOE's ability to establish and verify the claimed identity of an operator who accesses the WebUI interface of the TOE;

d. Security Management: The objective of these tests is to determine the TOE's ability of management of several aspects of the TOE Security Functions (TSF), including security attributes, TSF data, and security function behaviour;

e. Protection of the TSF: The objective of these tests is to determine the TOE's ability to provide the integrity and management of the mechanisms that provide the TSF;

f. Resource Utilization: The objective of these tests is to determine the TOE's ability to support the availability of required resources;

g. TOE Access: The objective of these tests is to determine the TOE's ability to control the establishment of an operator's session; and

h. Resolution Management Functions: The objective of these tests is to determine the TOE's ability to provide the incident and problem management of the data gathered by the Agents.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Network scanning;
- Network traffic monitoring and analysis;
- Web application vulnerabilities; and
- Database vulnerabilities.

The methods used by the evaluator were:

- Port Scanning;
- Monitoring the network traffic;
- Manual SQL injection (login); and
- Automated SQL injection and Database vulnerability attacks.

The independent penetration testing did not uncover any exploitable vulnerabilities in the anticipated operating environment.

12.4 Conduct of Testing

The Resolution Manager 4.2 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at DOMUS IT Security Laboratory located in Ottawa, Ontario, 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.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the Resolution Manager 4.2 behaves as specified in its ST and functional specification.

13 Results of the Evaluation

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

14 Evaluator Comments, Observations and Recommendations

Consumers of the Resolution Manager 4.2 should consider assumptions about usage and environmental settings, defined in the Section 3 of ST, and the TOE protection scope, clarified in the Section 7.3 of this document, as requirements for the product's installation and its operating environment.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management

Acronym/Abbreviation/ Initialization	Description
CSEC	Communications Security Establishment Canada
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
WebUI	Web User Interface

16 References

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

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

b. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, CCMB-2005-08-002, Version 2.3, August 2005.

c. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, CCMB-2005-08-003, Version 2.3, August 2005.

d. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-2005-08-004, Version 2.3, August 2005.

e. Triumfant, Inc. Resolution Manager 4.2 Security Target, Version 1.2, 22 December 2008.

f. Evaluation Technical Report for EAL2+ Evaluation of Triumfant Resolution Manager 4.2, Version 0.7, 8 January 2009.