Certification Report

EAL 3+ Evaluation of AccessData Cyber Intelligence and Response Technology v2.1.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-158-CR
Version: 1.0
Date: 03 January 2013
Pagination: i to iii, 1 to 8

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, the 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.

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 03 January 2013, 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).

TABLE OF CONTENTS

Executive Summary

AccessData Cyber Intelligence and Response Technology v2.1.2 (hereafter referred to as CIRT v2.1.2), from AccessData Group, LLC, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

CIRT v2.1.2 provides the means to identify and manage inappropriate data hosted on an organization's end user workstations, file shares, and email message servers. This evaluation focused on the Authentication Services and Logging Services for the CIRT v2.1.2.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 22 November 2012 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 CIRT v2.1.2, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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 3 augmented 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.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the CIRT v2.1.2 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is AccessData Cyber Intelligence and Response Technology v2.1.2 (hereafter referred to as CIRT v2.1.2), from AccessData Group, LLC.

2 TOE Description

CIRT v2.1.2 provides the means to identify and manage inappropriate data hosted on an organization's end user workstations, file shares, and email message servers. This evaluation focused on the Authentication Services and Logging Services for the CIRT v2.1.2. The Authentication Services instantiates and enforces security management functions for the TOE. The Logging Service provides an entry point for submitting, storage and retrieval of security events.

A detailed description of the CIRT v2.1.2 architecture is found in section 1.6.2 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for CIRT v2.1.2 is identified in Section 6 of the ST.

4 Security Target

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

Title: AccessData Cyber Intelligence and Response Technology v2.1.2 Security Target
Version: Version 0.9.5
Date: 26 September 2012

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.*

CIRT v2.1.2 is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

CIRT v2.1.2 implements an access control policy to control user access to management operations; details of this security policy can be found in Section 6 of the ST.

In addition, CIRT v2.1.2 implements policies pertaining to security audit, identification and authentication, security management, and TOE access. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of CIRT v2.1.2 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:

- The installation procedures are carried out by trained AccessData staff to install and configure the product, either on the customer's site, or off-site at a central installation and distribution site.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
- Authenticated users possess the necessary authorization rights to access at least some of the information or resources managed by the TOE and act in a cooperative manner.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- All network communication between components of the TOE that operate within a private network, with those outside the private network, is conducted over secure network communication sessions.

7.3 Clarification of Scope

CIRT v2.1.2 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. CIRT v2.1.2 is not

intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

It should be noted that while CIRT v2.1.2 provides the means to identify and manage inappropriate data hosted on an organization's end user workstations, file shares, and email message servers, this evaluation focused on the Authentication Services and Logging Services for the CIRT v2.1.2.

8 Evaluated Configuration

The evaluated configuration for CIRT v2.1.2 comprises CIRT v2.1.2 build 10 (web application software component and authentication and logging services components) running on Microsoft Windows Server 2008 R2 Service Pack 1.

9 Documentation

The AccessData Group, LLC documents provided to the consumer are as follows:

a. AccessData CIRT 2.1.2 User Guide, September 13, 2012; and

b. AccessData CIRT 2.1.2 Installation Guide, February 28, 2012.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of CIRT v2.1.2, including the following areas:

Development: The evaluators analyzed the CIRT v2.1.2 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 CIRT v2.1.2 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the CIRT v2.1.2 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 CIRT v2.1.2 configuration management system and associated documentation was performed. The evaluators found that the CIRT v2.1.2

configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well-developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the CIRT v2.1.2 design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of CIRT v2.1.2 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by AccessData Group, LLC for CIRT v2.1.2 . During a site visit, the evaluators 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 CIRT v2.1.2. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to CIRT v2.1.2 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 3 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].

[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.

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 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 is the following list of EWA-Canada test goals:

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

b. Install agent with push: The objective of this test goal is to verify that an endpoint agent can be installed using a push job from the TOE;

c. Remediation: The objective of this test goal is to verify that the endpoint agent can be instructed to remove sensitive files from a target host PC; and

d. Memory Operation: The objective of this test goal is to demonstrate the agent's ability to capture endpoints memory content and save it for further investigation.

11.3 Independent Penetration Testing

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

a. Port Scan: The objective of this test goal was to scan the TOE using a port scanner to determine what ports were open and what services were running and to compare against those ports that should be open and services running;

b. Information Leakage Verification: The objective of this test goal was to monitor the TOE during start-up, shutdown, login, and other scenarios to determine if sensitive information is leaked which could be used by an attacker;

c. Review login screen: The objective of this test case is to verify that there are no visible vulnerabilities in the TOE's main interface; and

d. Agent stop and start: The objective of this test case is to verify that the TOE can gracefully stop and launch the agent service without giving away sensitive information.

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

11.4 Conduct of Testing

CIRT v2.1.2 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 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 CIRT v2.1.2 behaves as specified in its ST and functional specification and TOE design.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+ 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

The usual method of deployment for the TOE is to have a Technical Account Manager (TAM) representative from AccessData install and configure the product. This was witnessed during a visit to the developer's site.

The developer maintains a high-level of end user support for the product. This was exercised by the evaluator during this evaluation.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CIRT	Cyber Intelligence and Response Technology
CPL	Certified Products list

Acronym/Abbreviation/ Initialization	Description
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
SFR	Security Functional Requirement
ST	Security Target
TAM	Technical Account Manager
TOE	Target of Evaluation
TSF	TOE Security Functionality

15 References

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

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

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 3.1 Revision 3, July 2009.

d. AccessData Cyber Intelligence and Response Technology v2.1.2 Security Target, Version 0.9.5, 26 September 2012.

e. Evaluation Technical Report for EAL 3+ Common Criteria Evaluation of AccessData Group LLC AccessData Cyber Intelligence and Response Technology v2.1.2 Version 1.4, 22 November 2012.