Certification Report

Trend Micro Deep Discovery Inspector 3.2, build 1118

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-252-CR
Version: 1.0
Date: 21 January 2014
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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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.

The evaluation facility that carried out this evaluation is CygnaCom Solutions.

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 21 January 2014, 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

Trend Micro Deep Discovery Inspector 3.2, build 1118 (hereafter referred to as Trend Micro DDI v3.2), from Trend Micro Incorporated, is the Target of Evaluation for this evaluation.

Trend Micro DDI v3.2 is an Intrusion Detection System (IDS) that protects customers' IT networks. This solution is deployed offline in the IT network of customers to monitor network traffic. It can identify both file-based and network-based attacks and malicious behavior. The TOE also takes proactive or preventive measures to ensure the security of the detection, such as:

- Storing detection logs
- Sending alarms to administrators
- Sending cleaning requests to mitigation servers of Trend Micro if they are deployed with the TOE

The TOE is able to protect itself and associated data from unauthorized access or modification and provides an audit trail to ensure accountability for authorized actions.

CygnaCom Solutions is the evaluation facility that conducted the evaluation. This evaluation was completed on 31 December 2013 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 Trend Micro DDI v3.2, 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 requirements outlined in the U.S. Government Protection Profile Intrusion Detection System for Basic Robustness Environments, Version 1.7, July 25, 2007. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Trend Micro DDI v3.2 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 is Trend Micro Deep Discovery Inspector 3.2, build 1118 (hereafter referred to as Trend Micro DDI v3.2), from Trend Micro Incorporated.

2 TOE Description

Trend Micro DDI v3.2 is an Intrusion Detection System (IDS) that protects customers' IT networks. This solution is deployed offline in the IT network of customers to monitor network traffic. It can identify both file-based and network-based attacks and malicious behavior. The TOE also takes proactive or preventive measures to ensure the security of the detection, such as:

- Storing detection logs
- Sending alarms to administrators
- Sending cleaning requests to mitigation servers of TrendMicro if they are deployed with the TOE

The TOE is able to protect itself and associated data from unauthorized access or modification and provides an audit trail to ensure accountability for authorized actions.

A detailed description of the Trend Micro DDI v3.2 architecture is found in 1.4 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Trend Micro DDI v3.2 is identified in Section 1.4.2 of the ST.

4 Security Target

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

Title:	Trend Micro Deep Discovery Inspector 3.2 Security Target (EAL2+) v2.0
Version:	v2.2
Date:	20 January 2014

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

Trend Micro DDI v3.2 is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - IDS_SDC.1 System Data Collection (EXT);
    - IDS_ANL.1 Analyser Analysis (EXT);
    - IDS_RCT.1 Analyser react (EXT);
    - IDS_RDR.1 Restricted data review (EXT);
    - IDS_STG.1 Guarantee of System Data Availability (EXT);
    - IDS_STG.2 Prevention of System data loss (EXT);
    - FAV_ACT_(EXT).1 Anti-Virus actions; and
    - FAV_ALR_(EXT).1 Anti-Virus alerts.

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

c. *Common Criteria EAL 2 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures; and

d. *Demonstrable conformance to the* U.S. Government Protection Profile Intrusion Detection System for Basic Robustness Environments, Version 1.7, July 25, 2007.

6 Security Policy

Trend Micro DDI v3.2 implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Section 7.1 of the ST.

In addition, Trend Micro DDI v3.2 implements other policies pertaining to security audit, IDS, identification and authentication, and anti-virus. Further details on these security policies may be found in Section 7.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Trend Micro DDI v3.2 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 authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation;
- The TOE can only be accessed by authorized system administrator and administrators;
- The TOE has access to all the IT System data it needs to perform its functions; and
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access;
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification; and
- The TOE is appropriately scalable to the IT System the TOE monitors.

8 Evaluated Configuration

The evaluated configuration for Trend Micro DDI v3.2 comprises one of three configurations:

- The TOE software pre-installed on a DD 1000 or DD 500 appliance;
- The TOE software installed on a bare metal server with the following requirements;
  - CPU: Two Intel™ Core™ Quad Core processors
  - RAM: 8GB
  - Hard disk space: 100GB
  - Network interface card (NIC): Two NICs
- A virtual appliance installed on a virtual machine with the following requirements;
  - CPU: Two Intel™ Core™ Quad Core processors
  - RAM: 8GB
  - Hard disk space: 100GB
  - Network interface card (NIC): Two NICs

9 Documentation

The Trend Micro Incorporated documents provided to the consumer are as follows:

a. Trend Micro Deep Discovery Inspector 3.2 Administrator's Guide, 19 December 2013;

b. Common Criteria Evaluation Addendum, 19 December 2013; and

c. Common Criteria Preparative Procedures, 31 December 2013.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Trend Micro DDI v3.2, including the following areas:

Development: The evaluators analyzed the Trend Micro DDI v3.2 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 Trend Micro DDI v3.2 security architectural description and determined that the initialization process is secure, 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 are correct.

Guidance Documents: The evaluators examined the Trend Micro DDI v3.2 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 Trend Micro DDI v3.2 configuration management system and associated documentation was performed. The evaluators found that the Trend Micro DDI v3.2 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.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Trend Micro DDI v3.2 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Trend Micro DDI v3.2. 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.

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

11 ITS Product Testing

Testing 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 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 CygnaCom Solutions test goals:

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

[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.

b. Administrator role restrictions: The objective of this test goal is to test the restrictions placed up the administrator account such as account deletion and expired credentials;

c. Audit functionality: The objective of this test goal is to confirm that the audit functionality works as expected and is able to recover/re-start from unplanned shutdowns; and

d. IDS functionality: The objective of this test goal is to exercise the IDS functionality of the TOE and confirm that it functions as expected.

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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;

b. Checking input validation for login fields by inputing special character strings in an attempt to force the TOE into a vulnerable error state;

c. Inspecting the TOE web interface for undocumented web pages that might provide a backdoor into the TOE; and

d. Attempting to use the administrator privileges to directly access the TOE database, operating system, or Apache server settings.

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

11.4 Conduct of Testing

Trend Micro DDI v3.2 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place onsite at the vendors development facility. 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, providing assurance that Trend Micro DDI v3.2 behaves as specified in its ST and functional specification.

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

The evaluation team's test activities demonstrate that the claims in the ST are met. However, it is important to note that changing the default administrative account is not enforced by the TOE.

Additionally, during testing the evaluators found the TOE's ability to on-demand capture and export network traffic sent to a specific data port an especially useful troubleshooting feature. To access this feature navigate to Appliance IP Setting and look under Network Interface Ports section.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IDS	Intrusion Detection System
IT	Information Technology
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation

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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Trend Micro Deep Discovery Inspector 3.2 Security Target (EAL2+) v2.0, v2.2, 20 January 2014.

e. Evaluation Technical Report Deep Discovery Inspector v3.2, v1.0, 31 December 2013.