Certification Report

Invincea FreeSpace™ v4.0 and Invincea Management Server v2.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-296-CR
Version: 1.0
Date: 30 April 2015
Pagination: i to iii, 1 to 10

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, applies 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, 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, 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.

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 CSC Security Testing/Certification Laboratories.

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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 30 April 2015, 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 trademark:

- Invincea FreeSpace is a trademark of Invincea, Inc.

TABLE OF CONTENTS

Executive Summary

Invincea FreeSpace™ v4.0 and Invincea Management Server v2.0 (hereafter referred to as Invincea FreeSpace), from Invincea, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that Invincea FreeSpace™ meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

Invincea FreeSpace is an anti-malware and threat intelligence solution that provides a secure container for users to run web browsers and document applications within. The secure container keeps malware from executing or installing on the host machine. Malware is detected by Invincea's behavior-based threat detection. Upon detection, the secure container is destroyed and a clean container is recreated to ensure the end user machine is not compromised. Invincea FreeSpace client integrates with the Invincea Management Server which manages client configuration and collects any threats that were detected on an end user's machine.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 30 April 2015 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 Invincea FreeSpace, and the security functional/assurance 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.

Communications Security Establishment, as the CCS Certification Body, declares that the Invincea FreeSpace 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 EAL 2+ evaluation is Invincea FreeSpace™ v4.0 and Invincea Management Server v2.0 (hereafter referred to as Invincea FreeSpace), from Invincea, Inc..

2 TOE Description

The TOE is comprised of the following two components:

- Invincea FreeSpace. Invincea FreeSpace is a software application that is installed on end user machines which provides a secure container for users to run web browsers and document applications within. The secure container protects users from malicious attacks that may come from a website or an infected document.

- Invincea Management Server. The Invincea Management Server is a virtual appliance used to manage client configuration, view logs and collect information on threats detected on an end user's machine.

3 Security Policy

Invincea FreeSpace implements a role-based access control policy to control administrative access to the system. In addition, Invincea FreeSpace implements policies pertaining to the following security functional classes:

- *Security Audit*
- *Cryptographic Support*
- *User Data Protection*
- *Identification and Authentication*
- *Security Management*
- *Protection of the TSF*
- *TOE Access*
- *Trusted Path*

The following cryptographic module was evaluated to the FIPS 140-2 standard:

Cryptographic Module	Certificate
Red Hat Enterprise Linux OpenSSL (openssl 1.0.0-20.el6 and dracut-fips 004-248.el6_3.1)	1758

4 Security Target

The ST associated with this Certification Report is identified below:

Invincea FreeSpace™ v4.0 and Invincea Management Server v2.0 Security Target, Version 1.9, 21 April 2015

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.

Invincea FreeSpace is:

a. EAL 2 augmented, containing all security assurance requirements listed, as well as the following:

   ALC_FLR.1 - Basic Flaw Remediation

b. 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:

   FDP_SVC.1 - Secure Virtual Container

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

6 Assumptions and Clarification of Scope

Consumers of Invincea FreeSpace™ 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- *Administrators of the TOE are trusted and follow guidance.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The Invincea Management Server is deployed in a physically secure environment on a trusted network.*
- *It is assumed that there is no pre-existing compromise of the host.*
- *Microsoft Windows provides cryptographic services to Invincea FreeSpace.*

6.3 Clarification of Scope

Cryptographic operations are relevant to the Invincea Management Server only. The FIPS validation is vendor affirmed and the cryptographic module has been ported in accordance with FIPS IG G.5.

The Invincea FreeSpace client platform makes use of the Microsoft CryptoAPI provided by the environment.

7 Evaluated Configuration

The evaluated configuration for Invincea FreeSpace is as follows:

- *Invincea FreeSpace Client version 4.0 running on Microsoft Windows 7 (32 and 64-bit) and Microsoft Windows 8.1 (32 and 64-bit); and*
- *The Invincea Management Server version 2.0 installed on VMware Workstation 10.*

The publication entitled Invincea FreeSpace™ v4.0 / Invincea Management Service v2.0 Common Criteria Addendum describes the procedures necessary to install and operate Invincea FreeSpace in its evaluated configuration.

8 Documentation

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

a. Invincea FreeSpace™ Administrator's Guide 4.0;

b. Invincea FreeSpace™ User Guide v4.0;

c. Invincea Management Server – Installation and Configuration Guide v2.0; and

d. Invincea FreeSpace™ v4.0 / Invincea Management Service v2.0 Common Criteria Addendum.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Invincea FreeSpace, including the following areas:

Development: The evaluators analyzed the Invincea FreeSpace 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 Invincea FreeSpace 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 Invincea FreeSpace 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 Invincea FreeSpace configuration management system and associated documentation was performed. The evaluators found that the Invincea FreeSpace configuration items were clearly marked.

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

The evaluators reviewed the flaw remediation procedures used by developer for the Invincea FreeSpace. 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.

10 ITS Product Testing

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

10.1 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[1].

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.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

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 test goals:

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

b. OpenSSL Equivalency: The objective of this test goal is to confirm the version of OpenSSL used by the TOE.

10.3 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. Infected Document Hiding: The objective of this test goal is to generate various combinations of "infected" files, masking their contents and attempt to save the infected files in the Windows file system.

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

10.4 Conduct of Testing

Invincea FreeSpace was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information

[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.

Technology Security Evaluation and Test 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.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that Invincea FreeSpace behaves as specified in its ST and functional specification.

11 Results of the Evaluation

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

12 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
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
TOE	Target of Evaluation
TSF	TOE Security Function

13 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. Invincea FreeSpace™ v4.0 and Invincea Management Server v2.0 Security Target, Version 1.9, 21 April 2015

e. Evaluation Technical Report Invincea FreeSpace™ v4.0 and Invincea Management Server v2.0, Version 1.2, 30 April 2015.