Australian Government
Australian Signals Directorate

Australian Cyber Security Centre

Australasian Information Security Evaluation Program

Certification Report

Blancco Drive Eraser v6.9.1

Version 1.0, 03 June 2020

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of Blancco Drive Eraser version 6.9.1 against Common Criteria EAL2.

The Target of Evaluation (TOE) is Blancco Drive Eraser version 6.9.1. The TOE is a software product that securely erases hard disk drives and solid state drives in accordance with recognised standards, as well as generating reports on erasure activities.

This report concludes that the TOE has complied with the Common Criteria (CC) evaluation assurance level EAL2 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP).

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program. The evaluation was performed by Teron Labs and was completed on 24 May 2020.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that:

- the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- users review their operational environment and ensure security objectives for the operational environment can be met
- users configure and operate the TOE according to the vendor’s supplementary guidance
- users configure the adjustable erasure verification level at 100% rather than use the quicker default value of 1%, noting that the verification value should be set at a level commensurate with the importance of the completeness of the data erasure
- users make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- users check and understand all drive erasure reports
- users verify the integrity of the TOE software prior to use by comparing the SHA256 hash of the downloaded software against the hash value provided by Blancco as part of the purchase process.

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [7] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is Blancco Drive Eraser v6.9.1.

Description	Version
Evaluation scheme	Australasian Information Security Evaluation Program
TOE	Blancco Drive Eraser
Software version	v6.9.1
Security Target	*Blancco Drive Eraser v6.9.1 Security Target v6.0 dated 22 May 2020*
Evaluation Technical Report	*Evaluation Technical Report 1.0 dated 24 May 2020* Document reference EFT-T008-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Conformant and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	EAL 2
Developer	Blancco Technology Group Länsikatu 15 FIN-80110 Joensuu, Finland

Evaluation facility

Teron Labs Pty Ltd
Unit 3, 10 Geils Court
Deakin ACT 2600
Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is Blancco Drive Eraser version 6.9.1.

Blancco Drive Eraser is software that is used to securely erase information from various persistent store technologies including traditional hard disk drives (HDDs) and newer solid state drives (SSDs). The software is delivered as an .iso file that can be used to boot a computer connected to the data drives requiring erasure. The software runs in RAM using information from the .iso file to analyse the attached data drive(s), erase the information on the data drive(s) and check the erasure activities for success or failure.

There are many algorithms for erasing data drive information. Blancco Drive Eraser supports proprietary and standard algorithms that can be selected as required by the user. As well as the data drive erasure functionality the TOE takes steps to ensure correct functioning on the hardware it happens to be running on. Another important function performed by the TOE is the generation of reports that are protected from tampering – thus providing a valuable record of data drive erasure activities performed by the user.

TOE Functionality

The TOE functionality that was evaluated is described in section 2.4.2 of the Security Target [7].

TOE physical boundary

The TOE physical boundary is described in section 2.4.1 of the Security Target [7].

TOE Architecture

Blancco Drive Eraser can be run in different configurations depending on the scale of use and the licencing arrangements between the user and Blancco. In this case the TOE software is executed on a computer system supplied by the user that is connected to the data drives.

Various ways that the TOE can be used include:

- local – with the user interface provided by a screen and keyboard connected to the computer the TOE is running on
- remote – in this case the TOE software is configured so the user interface is provided by the Blancco Management Console (BMC) running on a different computer.

Various ways to use the TOE which is licenced from Blancco include:

- through the Blancco Management Console (BMC)
- through a connected HASP (security dongle)
- through a TOE configured to use BIOS time settings.

Clarification of scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [7].

Non-evaluated functionality and services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [4] for policy relating to using an evaluated product in an unevaluated configuration. New Zealand Government users should consult the *New Zealand Information Security Manual* [5].

Security

The TOE Security Policy is a set of rules that defines how information within the TOE is managed and protected. The Security Target [7] contains a summary of the evaluated functionality.

Usage

Evaluated configuration

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as described in the Common Criteria Guidance Supplement [6]. Selecting these settings will increase confidence in the data erasure process with the trade-off that the erasure might take longer.

Important settings include:

- **Erase remapped sectors** and the related **Fail erasure if not supported** are both set to **on**
- **Remove hidden areas** is set to **on**
- **Enforce Blancco SSD method on SSDs** is set to **on**
- **Preserve recovery partition** is set to **off**
- **Execute self-tests on Drives** is set to **extended** and the related **Fail Erasure if Unsuccessful** is set to **on**.

Erasure algorithms in scope include:

- Blancco SSD Erasure
- CESG CPA – Higher Level
- DoD 5220.22-M
- DoD 5220.22-M ECE
- NIST 800-88 Clear
- NIST 800-88 Purge
- HMG Infosec Standard 5, Higher Standard
- HMG Infosec Standard 5, Lower Standard.

Secure delivery

Software delivery procedures

The TOE can be delivered to the user via download from the Blancco web site or via physical delivery on media such as DVD-ROM.

- When downloaded from the web Blancco provides a SHA256 hash that allows the user to verify the download.
- When physically delivered the packaging and tamper-evident seal should be carefully examined by the user.

Installation of the TOE

The Common Criteria Guidance Supplement [6] contains all relevant information for the secure configuration of the TOE. It is important that the user understands the implications of policies concerning NIST 800-88 Clear fallback and the possible interference of RAID systems on data drive erasure.

Version verification

The version of Blancco Drive Eraser being run can be verified from the top left area of the GUI screen. In the evaluated configuration this will be v6.9.1.

Documentation and guidance

The general user documentation for Blanco Drive Erase v6.9.1 and the Common Criteria Guidance Supplement included in the scope of the TOE are available on-line from a link provided by Blancco after purchase. These documents are *Blancco Drive Eraser User Manual for Version 6.9.1 (ref: 06022020)* and *Blancco Drive Eraser v6.9.1 Common Criteria Guidance Supplement v4.0* [6].

All Common Criteria guidance material is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [4]. The *New Zealand Information Security Manual* is available at https://www.gcsb.govt.nz/ [5].

Secure usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

- The TOE user is not negligent or hostile. The TOE is used in accordance with the enterprise security policies.
- The hardware that runs the TOE is trustworthy and functioning as expected.
- The Drive Eraser Configuration Tool (DECT) software used to configure the TOE is authentic.
- The Blancco Management Console (BMC) software used to manage the TOE remotely (when applicable) is authentic.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

Evaluation procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3* [1, 2].

Testing methodology was drawn from *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5* [3].

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program [10].

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* were also upheld [9].

Functional testing

To gain confidence that the developer testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining the test coverage, test plans and procedures, and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

These developer tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All Security Functional Requirements listed in the Security Target were exercised during testing.

Penetration testing

A vulnerability analysis of the TOE was conducted in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

The developer performed a vulnerability analysis of the TOE in order to identify any obvious security vulnerability in the product, and if identified, to show that the security vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible security vulnerabilities in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

- time taken to identify and exploit (elapsed time)
- specialist technical expertise required (specialist expertise)
- knowledge of the TOE design and operation (knowledge of the TOE)
- window of opportunity
- IT hardware/software or other equipment required for the exploitation.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

EAL2 provides assurance by a full security target and an analysis of the Security Functional Requirements (SFRs) in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE Security Functionality (TSF), evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

Certification result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [7] and **has met** the requirements of Common Criteria EAL2.

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [8], the Australasian Certification Authority **certifies** the evaluation of Blancco Drive Eraser v6.9.1 performed by the Australasian Information Security Evaluation Facility, Teron Labs.

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual* [4] and New Zealand Government users should consult the *New Zealand Information Security Manual* [5].

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australasian Certification Authority also recommends:

- that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- users review their operational environment and ensure security objectives for the operational environment can be met

- users configure and operate the TOE according to the vendor’s supplementary guidance
- users configure the adjustable erasure verification level at 100% rather than use the quicker default value of 1%, noting that the verification value should be set at a level commensurate with the importance of the completeness of the data erasure
- users make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- users check and understand all drive erasure reports
- users verify the integrity of the TOE software prior to use by comparing the SHA256 hash of the downloaded software against the hash value provided by Blancco as part of the purchase process.

Annex A – References and abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*

2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*

3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*

4. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism

5. *New Zealand Information Security Manual:* https://www.nzism.gcsb.govt.nz/ism-document/

6. Guidance documentation:

   - *Blancco Drive Eraser User Manual for Version 6.9.1 (Ref: 06022020) – Link available from the developer*
   - *Blancco Drive Eraser v6.9.1 Common Criteria Guidance Supplement v4.0 – Link available from the developer*

7. *Blancco Drive Eraser v6.9.1 Security Target v6.0 dated 22 May 2020*

8. Evaluation Technical Report - *EFT-T008 ETR 1.0 dated 24 May 2020*

9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2-July-2014*

10. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf

Abbreviations

AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CCRA	Common Criteria Recognition Arrangement
DVD	Digital optical disc storage format
HASP	Hardware Against Software Piracy (security dongle)
TOE	Target of Evaluation
USB	Universal Serial Bus
.iso	File extension for binary image file that can be written to DVD disc or USB drive