CSPN Security target

Product Blancco Drive Eraser version 6.12.0

Category « Data Erasure »

Reference: CSPN-ST-Blancco Drive Eraser 6-3.04

Date: 08/10/2020

Internal reference: BLA006

Copyright AMOSSYS

Siège : Immeuble Le Ouessant • Bâtiment B • 11 rue Maurice Fabre • 35000 Rennes • France • **www.amossys.fr**
SIRET : 493 348 890 00051 • **NAF** : 6202 A • RCS Rennes B 493 348 890 • SAS au capital de 38.000 Euros

EVOLUTION OF THE DOCUMENT

Version	Date	Description	Author(s)
1.00	10/02/2017	Document creation	Benjamin DUFOUR Antoine COUTANT (AMOSSYS)
1.01	11/05/2017	Update following ANSSI comments	Antoine COUTANT (AMOSSYS)
2.00	19/03/2019	Update regarding cryptographic mechanisms evolution	Kelly RESCHE (AMOSSYS) Bernard LE GARGEAN (Blancco)
2.01	16/05/2019	Update following ANSSI remarks	Alexandre DELOUP (AMOSSYS)
3.00	12/03/2020	Update regarding the new report digital signature	Bernard LE GARGEAN (Blancco) Kelly RESCHE (AMOSSYS)
3.01	02/04/2020	Update following ANSSI remarks	Bernard LE GARGEAN (Blancco)
3.02	12/05/2020	Update following ANSSI and AMOSSYS remarks on the evaluation platform	Bernard LE GARGEAN (Blancco)
3.03	26/06/2020	Update the evaluation platform to explicitly include SSD evaluation	Cédric MURDICA (AMOSSYS)
3.04	08/10/2020	Update regarding the users considered for the evaluation	Marion VOGT (AMOSSYS)

This document is validated by Blancco Technology Group IP Oy.

SUMMARY

GLOSSARY

Acronyms	Definitions
ATA	Advanced Technology Attachment
BIOS	Basic Input/Output System
BDE	Blancco Drive Eraser
BMC	Blancco Management Console
CD	Compact Disc
DCO	Device Configuration Overlays
DECT	Blancco Drive Eraser Configuration Tool
DHCP	Dynamic Host Configuration Protocol
eMMC	embedded Multi-Media Controller
GB	GigaByte
GUI	Graphical User Interface
HPA	Host Protected Areas
MGF	Mask Generation Function
NIC	Network Interface Card
PSS	Probabilistic Signature Scheme
PXE	Preboot eXecution Environment
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RPD	Report Per Drive
RSA	Rivest Shamir Adleman
SAS	Serial Attached SCSI
SATA	Serial ATA
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SSD	Solid State Drive
SSH	Secure SHell
SSL	Secure Sockets Layer
SVGA	Super Video Graphics Array
TOE	Target Of Evaluation
USB	Universal Serial Bus
VESA	Video Electronics Standards Association
XML	eXtensible Markup Language

Table 1 - Glossary

1. INTRODUCTION

1.1. SUBJECT OF THE DOCUMENT

This document has been written for the CSPN[1] certification scheme promoted by the ANSSI[2] (French authority) for the product "Blancco Drive Eraser 6.12.0" developed by **Blancco Technology Group IP Oy**.

The TOE[3] considered is Blancco Drive Eraser including DECT use.

This document is subject to technical and quality controls from **AMOSSYS,** and the validation by **Blancco Technology Group IP Oy**. Updates of this document are done by the **AMOSSYS** project team.

1.2. PRODUCT IDENTIFICATION

Éditeur	**Blancco Technology Group IP Oy** Länsikatu 15 FIN-80110 Joensuu FINLAND
Lien vers l'organisation	https://www.blancco.com
Nom commercial du produit	Blancco Drive Eraser
Numéro de la version évaluée	6.12.0
Catégorie du produit	Data erasure

1.3. REFERENCES

For the writing of this security target, the following documents were used:

- Blancco Drive Eraser: User Manual for version 6.12.0,
- Blancco Drive Eraser 6: technical document describing the cryptographic mechanisms available in Blancco Drive Eraser.

[1] *Certification de Sécurité de Premier Niveau*
[2] *Agence nationale de la sécurité des systèmes d'information*
[3] *Target Of Evaluation*

2. PRODUCT DESCRIPTION

2.1. GENERAL DESCRIPTION

The TOE (Blancco Drive Eraser) is a solution for end of life management of computer assets and has been designed and implemented for x86-64 architecture. Typical use cases of this product are (for a hard disk) reassignment or end of use.

The main function of the TOE is to perform hardware detection on a host computer, to display a list of available storage device(s) to the user, and to erase the selected target devices according to a chosen erasure standard (user can set their own default using the configuration tool and, by default, the vanilla image uses HMG Infosec 5, Lower Standard). The software also prepares a report that can be generated before or after the erasure process. This report contains the detailed information about the attached hardware and the erasure process, including timing information, details about hidden areas, remapped sectors and a list of any problems encountered during the erasure. The software can erase simultaneously several disks while displaying its interface and reports to the user.

Erased hard disks can be reused. Blancco Drive Eraser has no effect on the mechanics of the hard disk.

Blancco Drive Eraser is distributed as a disc image file (.ISO) and can be used with two other products developed by **Blancco Technology Group IP Oy** (Java tools):

- DECT which is used to configure the Drive Eraser ISO image to best fit the user's needs. This tool can generate a pair of keys used to sign a custom digital signature in the report,
- BMC which is used to store and manage erasure reports. It also verifies the digital signature of the report. It can also be used to remotely control Drive Eraser.

The use of DECT is permitted only to a dedicated responsible person who belongs to the organisation of the final client (organisational measure mandatory). DECT is used on a local machine (*i.e.* no network involved) and can change the configuration of the TOE by modifying the ISO image and saving these modifications by overwriting the existing ISO file or saving as a new ISO under a different name. The ISO can be deployed on a suitable medium such as a USB stick/CD or via a PXE server.

On the other hand, the use of BMC is not mandatory for the erasure process. It is mainly used as a report repository but does provide a security enforcing functionality via the digital signature verification which ensures the authenticity of the report.

The TOE is Blancco Drive Eraser including DECT use.

2.2. PRINCIPLE OF OPERATION

It is assumed that before using the TOE to erase all the data of a hard disk, the user has saved the useful data he needs on an external support.

The TOE is distributed as a disc image file (.ISO) from which a bootable CD or USB stick can be made. It can also be booted from a dedicated network using PXE (natively supported) which is an environment to boot computers using a network interface. The TOE is both OS and platform agnostic, meaning that it works independently of the operating system installed in the host computer, the data storage device filesystem or capacity, or the hardware manufacturer.

Remote erasure requires a network access connected to the computer. It can be done using PXE, or the computer can boot from a live-CD/USB, and then be controlled by a remote administrator.

The TOE can be booted from distribution media or, in certain cases, installed on a dedicated hardware eraser appliance. When booted directly from the ISO image, the software will be run

completely in RAM without installation. Erasure reports are either saved to external USB memory stick or sent to BMC using a network connection (outside evaluation perimeter).

The user then boots its computer on the TOE bootable media. Once booted, the TOE opens its main interface (a browser-based GUI written in HTML5/CSS3/JavaScript with CoffeeScript). This interface allows the user to:

- configure the TOE (language & keyboard layout, operation settings, network (wired & wireless) and management console configuration),
- do hardware tests on the main components of the machines (disabled by default, needs to be enabled via DECT),
- choose disks to erase and configure the erasure:
    - choosing the mode among manual, semi-automatic or automatic. This needs to be pre-configured using DECT,
    - choosing the erasure type among 25 standards,
    - configuring the percentage of verification after erasure,
    - selecting erasing options among erasing the remapped sectors, failing the erasure if the erasure of remapped sectors is not supported, removing the hidden areas, enforcing the TOE SSD method on SSDs, preserving the recovery partition, showing the drive partitions to select the ones to erase,
    - running a diagnostic of the disk (SMART test) before the erasure starts,
    - formatting the disk (ntfs, fat32) after the erasure is completed.
- control the erasure (starting, pausing, resuming and cancelling),
- display the report and save it (sending it to the BMC or saving it locally on a USB stick in XML or PDF formats).

2.3. DESCRIPTION OF DEPENDENCIES

The TOE has no dependency; it is distributed as a disc image file (.ISO).

The TOE uses third-party components to facilitate the operations of the erasure application, as follows:

Components	Descriptions
boost	For the C++ programming language that provide support for tasks and structures.
bzip2	File compression program.
curl	For transferring data with URL syntax.
freetype2	Library to render fonts.
gcc-libs	The GNU Compiler Collection.
glibc	The GNU C Library.
libpng	Library for reading and writing PNGs.
libssh2	Client-side C library implementing the SSH2 protocol.
libxml2	XML C parser and toolkit developed for the Gnome project.
libxml++	C++ wrapper for the libxml XML parser library.
libxslt	XML language to define transformation for XML.

Components	Descriptions
lightfirefox-48.0-1	Light version of Firefox, web browser for displaying the GUI. Uses full screen kiosk mode for total control of user experience. Both mouse and keyboard control with shortcuts are supported. With compatible hardware it is also possible to use with touch screen.
openssl	Toolkit implementing the Secure Sockets Layer.
xerces-c	Validating XML parser written in a portable subset of C++.
X.org	An open source implementation of the X Window System. Detects available hardware and sets display mode, keyboard layout and pointing device accordingly.
xz	General-purpose data compression software.
gettext.js	JavaScrypt library handle gettext translation messages.
base64.js	JavaScript code used to encore/decode data using base64.
jquery	JavaScript library designed to simplify HTML DOM tree traversal and manipulation.
jquery-ui	Set of user interface interactions, effects, widgets, and themes built on top of the jQuery JavScript Library.
kidomi.js	A JSON-to-DOM templating library.
xmlbuilder-js	An XML builder for node.js similar to java-xmlbuilder.
querystring.js	JavaScript library for manipulating the Query String.
mCustomScrollbar	Highly customizable custom scrollbar jQuery plugin.
jquery.mousewheel.js	A jQuery plugin that adds cross-browser mouse wheel support with delta normalization.
jquery.multiselect.js	Enhances an ordinary multiple select control into elegant drop-down list of checkboxes.
jquery.mask.js	A jQuery Plugin to make mask on form fields and HTML elements.
node-minify	Allows you to compress JavaScript, CSS and HTML files.
jquery.highlight.js	JavaScript text highlighting jQuery plugin.

Table 2 - Components used by the erasure application

2.4. DESCRIPTION OF THE TECHNICAL OPERATING ENVIRONMENT

The TOE works on x86-64 architectures. It is required that the targeted computer can boot with a USB stick, a CD or a PXE.

The TOE works independently from the operating system of the erased systems. Blancco Drive Eraser uses Arch Linux as its base Operating System.

Arch Linux is an independently developed, general purpose GNU/Linux distribution which focuses on simplicity and minimalism. The kernel sources are downloaded from the kernel.org repository, while the kernel has **Blancco Technology Group IP Oy** customized configuration and patches for the hardware drivers to add required functionality.

Minimum system requirements for Blancco Drive Eraser are as follows:

- x86-64 architecture machine,

- 1 GB of RAM (2 GB of RAM for PXE-booting),
- CD-drive or CD-compatible drive for CD-booting,
- USB-port for USB-booting and/or exporting/saving reports locally,
- SVGA display and VESA-compatible video card for graphical user interface,
- Ethernet NIC, DHCP Server running on local network (for BMC and PXE use).

The PXE server supports Debian 8, Ubuntu 18.04 LTS and Windows Server 2016.

2.5. EVALUATION PERIMETER

2.5.1. Perimeter

This evaluation targets the main functionality of erasure for Blancco Drive Eraser product with the use of DECT tool, with an ISO image booted locally (PXE is out of scope). For reminder, BMC is not included in the evaluation perimeter.

2.5.2. Evaluation platform

The evaluation platform is composed of pre-installed computers (x86-64) and the TOE is used on both the CD and USB stick media (PXE is out of scope). Therefore, network interfaces are not enabled. Some examples of evaluation platforms (considered for this evaluation) are listed below:

- A laptop or desktop or server installed with a Windows operating system (NTFS or FAT32 file system),
- A laptop or desktop or server installed with a Linux operating system (EXT4 or XFS file system).

It is assumed that reports are saved to an external USB memory stick and not sent to BMC.

Blancco Drive Eraser supports various storage technologies. This evaluation particularly focuses on the traditional Hard Disk Drive (HDD) and newer Solid State Drive (SSD). Consequently, the evaluation platform must consider both HDD and SSD to test the TOE for such storage technologies.

The following figure illustrates the setup of the evaluation platform:

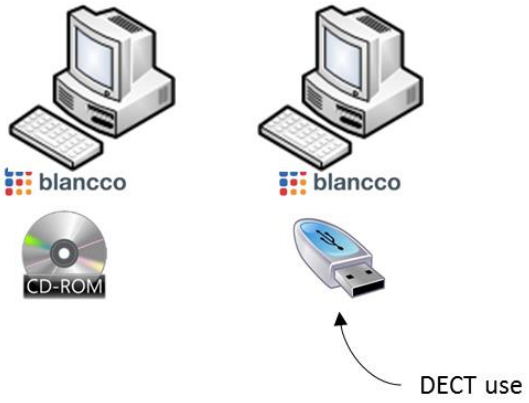

Figure 1 - Evaluation platform

3.SECURITY PERIMETER

3.1. USERS

Three users are considered for this evaluation:

- The one able to trigger a security erasure on a targeted computer,
- The one able to use DECT tool to modify the BDE image:
    - DECT must be used to generate and embed (or to simply embed) a custom private key into the image, this key is used to sign a custom digital signature in the report. DECT can also be used to modify the configuration of the ISO image (predefine the image settings like changing the default erasure standard),
    - Once modified, this ISO can be delivered via any means possible i.e. USB or CD (PXE is out of scope).

Note that there is another user, which is not considered, as BMC is out of scope:

- The one able to use BMC:
    - This user must import the custom public key into the BMC, this key is used to validate the custom digital signature of the report,
    - This user can also check the validity of the reports imported into the BMC,
    - In practice, this user can be the same as the user that configures the BDE image.

3.2. SENSITIVE ASSETS

An asset is a piece of data (or a function) assessed to be of value for the TOE. Its value is estimated according to security criteria (also called security needs): availability, integrity, confidentiality, authenticity.

There is nothing to prevent an unauthorized person to reconfigure the image of the TOE by using DECT (this tool is available to anyone in theory). Therefore, no sensitive asset (like TOE configuration for example) with DECT use is considered.

Similarly, no sensitive assets with PXE use is identified.

The sensitive assets protected by the TOE are as follows:

- **D1.DISK_IDENTIFICATION**

  Detected information about hard disk for defining required low-level actions for the erasure process.

  Security needs: integrity.

- **D2.USER_DATA**

  The data stored on the disk and to be erased.

  Security needs: confidentiality.

- **D3.REPORTS**

  The reports produced by the TOE before or after an erasure.

  Security needs: integrity, authenticity.

- **D4.KEYS**

  The keys used to sign/verify reports; generated by the DECT or externally. The private key is imported into the BDE image, the public key into BMC.

  Security needs: integrity, confidentiality.

3.3. ASSUMPTIONS

An assumption is a statement on the context of use of the TOE or on the TOE environment.

The assumptions are:

- **A1.TOE_USAGE**

  The TOE shall be used on computers in good working order and clean from any threat or malicious modification. In particular, the computers are safe from any hardware implants and they use the genuine and unmodified firmware (for the CD-ROM, HDD and BIOS).

- **A2.COMPETENT_USERS**

  Persons using the TOE are trusted, trained, and competent; they follow the application guidance documentation.

- **A3.REPORTS**

  Users must read the TOE reports to confirm the completeness of the erasure. It is assumed that reports are not sent to the BMC but exported from the software via an external USB stick. Only the reports that include a custom digital signature are considered in the evaluation perimeter.

- **A4.DECT_USERS**

  It is assumed that the use of DECT tool is allowed only to a dedicated responsible belonging to the organisation of the final client (organisational measure mandatory).

- **A5.BIOS_SETTINGS**

  BIOS settings of the hardware to be erased are modified in such way that they do not prevent the erasure of storage devices. Moreover, BIOS clock must be set to the correct time and date for reporting purposes.

- **A6.ISO_IMAGE**

  The ISO image and the external devices used to boot the system on the TOE (USB sticks or CDs) are clean and not modified from the original ISO image of the product. Furthermore, the USB sticks are configured and loaded with the ISO image using a specific tool, accordingly to the user manual. It is assumed that the ISO image and the external booting devices are stored in secure locations to ensure their confidentiality and, in case they are reused, their integrity.

- **A7.DISKS**

  The erased hard drives are directly connected to the PC using direct cables (i.e. SATA drives are connected with SATA cables). Docking systems, allowing the connection of a hard drive through a USB port, are not used.

- **A8.KEY_MANAGEMENT**

  The key pair used to create and verify the custom digital signature of the report must be kept in a secure location to ensure its confidentiality and integrity.

3.4. THREATS

A threat consists of an adverse action performed by a threat agent on an asset.

Only one threat agent is considered: an unauthorized individual or program having access before or after disk erasure by the TOE. The TOE can also fail to perform an action.

There is nothing to prevent an unauthorized person to reconfigure the image of the TOE by using DECT.

The threats are as following:

- **T1.ID_MODIFICATION**

  A threat agent succeeds in luring the TOE by indicating bad credentials for hardware detection (done by the operating system).

- **T2.DATA_RECOVERY**

  A threat agent gets data or metadata from a disk that has been previously erased by the TOE.

- **T3.REPORTS_MODIFICATION**

  A threat agent succeeds in modifying reports generated (and exported locally) by the TOE.

- **T4.INCOMPLETE_OVERWRITE**

  The TOE fails to overwrite contents of the storage devices or a specified part of the storage devices has not been overwritten.

- **T5.INCORRECT_REPORTING**

  The TOE fails to report correctly about the result of erasure process and/or the capacity of the storage device.

- **T6.KEY_DISCLOSURE_OR_MODIFICATION**

  A signature private key is improperly disclosed or modified.

3.5. SECURITY FUNCTIONS

The security functions are the technical measures and the mechanisms enforced by the TOE to protect the sensitive assets from the threats.

The security functions of the TOE are:

- **F1.DISK_DETECTION**

  The TOE collects (during bootstrap phase) detected information and uses it for defining required low-level actions for the erasure process. The initial identification happens before any erasure has been started, and it will be performed again after erasure in situations where a drive capacity changes, for example when hidden areas, such as DCO or HPA are removed.

  Disk identification are performed on disks that support the ATA communication, on disks that use the SCSI command protocol. eMMC and NVMe detection is also performed by fetching the name and device identifier.

- **F2.SECURE_ERASURE**

  The TOE performs overwriting with predefined or random data and/or executes firmware-based erasure commands.

  The TOE erases the data of a hard disk by overwriting it and following an erasure standard chosen by the administrator among:

Supported overwriting standards	Overwriting rounds
Air Force System Security Instruction 5020	4
Aperiodic random overwrite	1
Bruce Schneier's Algorithm	7
CESG CPA – Higher Level	3
DoD 5220.22-M	3
DoD 5220.22-M ECE	7
HMG Infosec Standard 5, Higher Standard	3
HMG Infosec Standard 5, Lower Standard	1
National Computer Security Center (NCSC-TG-025)	4
Navy Staff Office Publication (NAVSO P-5239-26)	3
NSA 130-1	3
OPNAVINST 5239.1A	3
Peter Gutmann's Algorithm	35
Random Byte Overwrite (3x)	3
RCMP TSSIT OPS-II	7
U.S. Army AR380-19	3

Table 3 - Supported overwriting standards

The following standards in the TOE use firmware erasure as the entire erasure process or as part of it:

Supported firmware erasure standards	Erasure rounds
Blancco SSD Erasure	3-5 (depending on what the drive supports)
BSI-GS	2
BSI-GSE	3
BSI-2011-VS	2
Cryptographic Erasure	1
NIST 800-88 Clear	1
NIST 800-88 Purge	1
Firmware Based Erasure	1
Extended Firmware Based Erasure	2
TCG Cryptographic Erasure	1

Table 4 - Supported firmware erasure standards

- **F3.VERIFICATION_PROCESS**

  The TOE can perform partial or full verification of erasure (the % amount depends on the erasure standard being used or a user selected value) and will report failure of the erasure, if the verification process encounters unexpected data.

  The value by default for verification is 1% on the vanilla image but the user can configure their own default using DECT.

  If there are any errors during erasure there will be an "ERRORS" text and counter displayed in erasure view of the GUI. The error counter contains total number of errors (write errors occurring during overwriting and read errors occurring during verification).

- **F4.REPORTING**

  The TOE generates (before and after the erasure process) reports that contain two kinds of information: hardware (information detected during start-up detection phase) and erasure (provided after erasure has been performed).

  Each report contains a default digital signature generated by Blancco, but this default digital signature is out of the scope of the Security Target. Instead, each report must contain an additional custom digital signature:

  - The report content is hashed with SHA-256 and signed with an RSA key (2048-bit strong) following the PSS scheme,
  - The key is entirely managed by the customer (creation and storage),
  - The custom digital signature is used to verify that the report hasn't been tampered or corrupted.

  For the TOE, the Report Per Drive (RPD) functionality can be activated to provide a separate report for each erased drive. The RPD mode can be enabled if the TOE is used locally or used in the "Manual" process mode.

- **F5.KEY_MANAGEMENT**

  The custom digital signature uses a private key generated by the user:

  - Either the key pair is generated by DECT and the private key is embedded into the TOE image via DECT,
  - Or the key pair is generated externally and then the private key is embedded into the TOE image via DECT.

  The corresponding public key is imported into BMC and is used to verify the custom digital signature to ensure that the report hasn't been tampered or corrupted.

3.6. COVERAGE

3.6.1. Threats and sensitive assets

The following table traces back the sensitive assets to the threats (letters "V", "I", "C", "A" meaning respectively aVailability, Integrity, Confidentiality, Authenticity):

	D1.DISK_IDENTIFICATION	D2.USER_DATA	D3.REPORTS	D4.KEYS
T1.ID_MODIFICATION	**I**			
T2.DATA_RECOVERY		**C**		
T3.REPORTS_MODIFICATION			**IA**	
T4.INCOMPLETE_OVERWRITE		**C**		
T5.INCORRECT_REPORTING			**I**	
T6.KEY_DISCLOSURE_OR_MODIFICATION				**CI**

Table 5 - Covering of the sensitive assets by the threats

3.6.2. Threats and security functions

The following table traces back the security functions to the threats:

	F1.DISK_DETECTION	F2.SECURE_ERASURE	F3.VERIFICATION_PROCESS	F4.REPORTING	F5.KEY_MANAGEMENT
T1.ID_MODIFICATION	√				
T2.DATA_RECOVERY		√	√		
T3.REPORTS_MODIFICATION				√	
T4.INCOMPLETE_OVERWRITE		√	√		
T5.INCORRECT_REPORTING	√		√		
T6.KEY_DISCLOSURE_OR_MODIFICATION					√

Table 6 - Covering of the threats by the security functions

End of the document