Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 3/19

(Certification No.)

Prodotto: WipeDrive v9.1

(Product)

Sviluppato da: WhiteCanyon Software Inc.

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2+

(ALC_FLR.2, ASE_TSS.2)

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 27 marzo 2019

Common Criteria

SOGIS

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

WipeDrive v9.1

OCSI/CERT/CCL/08/2018/RC

Version 1.0

27 March 2019

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	27/03/2019

2 Table of contents

1 Document revisions 5
2 Table of contents 6
3 Acronyms 8
4 References 10
4.1 Criteria and regulations 10
4.2 Technical documents 11
5 Recognition of the certificate 12
5.1 European Recognition of CC Certificates (SOGIS-MRA) 12
5.2 International Recognition of CC Certificates (CCRA) 12
6 Statement of Certification 13
7 Summary of the evaluation 14
7.1 Introduction 14
7.2 Executive summary 14
7.3 Evaluated product 14
7.3.1 TOE Architecture 15
7.3.2 TOE security features 17
7.4 Documentation 18
7.5 Protection Profile conformance claims 18
7.6 Functional and assurance requirements 18
7.7 Evaluation conduct 18
7.8 General considerations about the certification validity 19
8 Evaluation outcome 20
8.1 Evaluation results 20
8.2 Recommendations 21
9 Annex A – Guidelines for the secure usage of the product 22
9.1 TOE Delivery 22
9.2 Installation, initialization and secure usage of the TOE 22
10 Annex B – Evaluated configuration 23
10.1 TOE operational environment 23
11 Annex C – Test activity 24

11.1 Test configuration 24
11.2 Functional tests performed by the developer 24
11.2.1 Test coverage 24
11.2.2 Test results 24
11.3 Functional and independent tests performed by the evaluators 24
11.4 Vulnerability analysis and penetration tests 25

3 Acronyms

API Application Programming Interface

ATA Advanced Technology Attachment

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

DCO Device Configuration Overlay

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

eMMC embedded Multi Media Card

EXE Windows Executable

FTP File Transfer Protocol

GUI Graphical User Interface

HPA Host Protected Area

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza

NIS Nota Informativa dello Schema

NVMe Non-Volatile Memory Express

OCSI Organismo di Certificazione della Sicurezza Informatica

PP Protection Profile

PXE Preboot eXecution Environment

RFV Rapporto Finale di Valutazione (Evaluation Technical Report)

SAR Security Assurance Requirement

SCSI Small Computer System Interface

SFR Security Functional Requirement

SQL Structured Query Language

SSD	Solid State Device
TDS	Traguardo di Sicurezza (Security Target)
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
USB	Universal Serial Bus

4 References

4.1 Criteria and regulations

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[BLD] WhiteCanyon Building WipeDrive, v1.10, 12 February 2019

[DEL] WhiteCanyon Product Delivery Process, v2, 12 February 2019

[LOG] WipeDrive Enterprise Logging Manual, v1.1, 15 January 2019

[OPE] WipeDrive Enterprise User Guide, v1.3, 7 February 2019

[RFV] “WipeDrive v9.1” Evaluation Technical Report, v1, 21 February 2019

[TDS] “WipeDrive v9.1” Security Target, v1.3, 7 February 2019

5 Recognition of the certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on http://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

5.2 International Recognition of CC Certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL 2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA for all assurance components selected.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “WipeDrive v9.1”, developed by WhiteCanyon Software, Inc.

The TOE is a Disk Sanitizing tool that permanently erases hard drive data, operating systems, program files, and all other file data from a system. WipeDrive also provides users with the ability to permanently delete all partitions previously configured.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [TDS]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL2, augmented with ALC_FLR.2 and ASE_TSS.2, according to the information provided in the Security Target [TDS] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “WipeDrive v9.1” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [TDS], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	WipeDrive v9.1
Security Target	“WipeDrive v9.1” Server Security Target, v1.3, 7 February 2019
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.2 and ASE_TSS.2
Developer	WhiteCanyon Software, Inc.
Sponsor	WhiteCanyon Software, Inc.
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	16 October 2018
Evaluation ending date	21 February 2019

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [TDS] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of TOE; for a detailed description, please refer to the Security Target [TDS].

The TOE is a Disk Sanitizing tool that permanently erases hard drive data, operating systems, program files, and all other file data from a system. WipeDrive also provides users with the ability to permanently delete all partitions previously configured. The TOE provides 20 disk wipe functions. All wipe functions overwrite disk storage, or use special erasure commands native to the drives, to ensure no residual data remains. After the

sanitization process has been completed, an audit log is created which compiles verifications that the information contained on the hard drive was in fact erased.

The TOE:

- is a Linux based OS booted from either a LiveCD, EXE, or PXE Server, which resides in memory whilst running;
- is a data protection and erasure tool that permanently wipes data from ATA, SCSI, USB, eMMC and NVMe-block devices. This includes traditional platter drives as well as SSDs;
- allows users to create an audit log to capture verifications of the success or failure of hard drive erasure events;
- has the ability to wholly erase Operating Systems, program files, and all file data;
- utilizes user interfaces to allow administrators to graphically see the progress of probing, scanning, and erasure events;
- enables administrators to view sector data.

7.3.1 TOE Architecture

For a detailed description of the TOE, please refer to sect. 2 “TOE Description” of the Security Target [TDS]. The most significant aspects are summarized below (see Figure 1).

The only users of the TOE are referred to as administrators, who can execute commands to wipe drives by using the administrator definable wipe patterns. Verification of the success or failure of the wipe event is sent to the interface the user is currently using. Also, the audit log data collected from the wipe event is stored in/on a log storage device, which can be a portable flash/thumb drive, FTP server, SQL database, Windows Share directory, or other media storage device.

Administrators access the GUI in order to run the executable file for the WipeDrive application. Once the WipeDrive application has been executed, the cache stores data about scanned and probed devices in order to display the data to users. Scanning and probing are both performed during the initialization of the TOE. The WipeDrive application performs a scanning operation to discover attached devices. For each device that is discovered, a probe operation is run to enumerate device information.

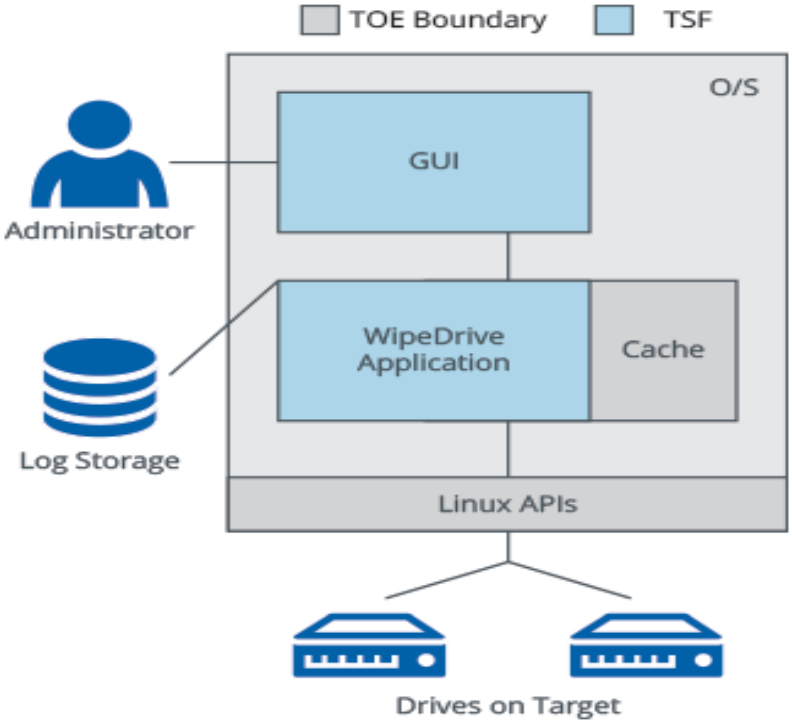

Figure 1 – TOE Boundaries

7.3.1.1 WipeDrive application

The WipeDrive application serves as a single executable file primarily responsible for:

- scanning the system for devices that can be erasure targets;
- probing the discovered devices for capabilities;
- erasing the devices, and performing related operations (such as removing ATA, HPA, DCO areas, or Accessible Max Address settings);
- producing progress event messages or result messages for consumption by user interface;
- performs logging after the erasure of the media has completed.

Only a single WipeDrive application will be able to run on any single host at any one time.

7.3.1.2 User Interfaces

The user interface serves as the physical interfaces where controls are used to operate one or more instances of the WipeDrive application, each on a distinct host. The interfaces that are included in the evaluated configuration are:

- GUI – A graphical user interface that is run on the same host as the WipeDrive application. This will be the default interface for x86 machines that framebuffer can be accessed.

7.3.1.3 Linux APIs

Linux APIs provide a logical interface between the application and the target drive(s). For example, when the TOE scans a disk, it relies on Linux to gather some of the data. This is a built-in function of the Operating System.

7.3.1.4 Third Party Programs

Optionally included with the Linux operating system are various programs that provide functionality utilized by WipeDrive.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sect. 4 and 5 of the Security Target [TDS].

For a detailed description of the TOE Security Functions, consult sect. 9 of the Security Target [TDS]. The most significant aspects are summarized below.

- **Security Audit**. The TOE generates and captures audit data which is used to provide further verification that an erasure event has occurred. Audit logs containing verification data (either denoting a success or failure) are stored internally to the WipeDrive application. The resulting output of a wipe operation is displayed in an easily interpretable manner. All audit operations can be associated with the administrator who performed that event. The TOE saves the audit events in a user-readable format outside of the TOE but is not responsible for facilitating the viewing of audit records except for a review of wipe results immediately following a wipe operation.

- **Security Management**. The only users of the TOE are referred to as Administrators. They are the individuals who maintain physical access to the WipeDrive application, and, as a result, possess several management capabilities. Administrators are able to specify the location for audit, specify the format in which this data is stored, create, run, view, or delete an administrator definable wipe pattern, scan for devices, view sector data, and get device info for all devices previously scanned. The TOE is equipped to operate via various interfaces which are made available to administrators. The administrators of the TOE utilize these interfaces to perform the management functions listed above. The primary purposes of these interfaces are to:

    1. Allow commands defined by the TOE to be invoked on the attached WipeDrive application;

    2. Visually display the status of the attached WipeDrive application by interpreting the responses and notifications received;

    3. Create audit logs according to the user's preferences. The logs can be stored on any form of media that the user desires (e.g. a thumb drive or on an FTP server).

The TOE is primarily operated via the GUI interface. The GUI is also run on the same host as the WipeDrive application. This will be the default interface for x86 machines that framebuffer can be accessed.

- **Disk Erasure**. The TOE is able to perform three distinct operations under the guise of Disk Erasure – scanning of devices, probing of devices, and the erasure of the devices. Scanning and probing are both performed during the initialization of the TOE. Administrators can execute commands via the GUI to wipe drives. The wipe command applies the administrator definable wipe pattern to each selected disk instance, which performs the overwrite operations directly on the disk.

- **User Data Protection**. The TOE provides for the erasure of residual information. This erasure is initiated at the user-facing interfaces and requires communication with the information repository (disk). No residual information will reside in the RAM subsequent to a wipe event.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customers together with the product. The guidance documentation contains all the information for secure installation, initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [TDS].

Customers should also follow the recommendations for the secure use of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [TDS] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All Security Functional Requirements (SFR) have been selected from CC Part 2 [CC2].

Please refer to the Security Target [TDS] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [TDS]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in

accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory.

The evaluation was completed on 21 February 2019 with the issuance by LVS of the Evaluation Technical Report [RFV], which was approved by the Certification Body on 13 March 2019. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [TDS], with reference to the operating environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [RFV] issued by the LVS CCLAB Software Laboratory and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "WipeDrive v9.1" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL2, augmented with ALC_FLR.2 and ASE_TSS.2, with respect to the security features described in the Security Target [TDS] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL2, augmented with ALC_FLR.2 and ASE_TSS.2.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification with architectural design summary	ASE_TSS.2	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Security-enforcing functional specification	ADV_FSP.2	Pass
Basic design	ADV_TDS.1	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Use of a CM system	ALC_CMC.2	Pass
Parts of the TOE CM coverage	ALC_CMS.2	Pass
Delivery procedures	ALC_DEL.1	Pass

Assurance classes and components		Verdict
Flaw reporting procedures	ALC_FLR.2	Pass
Test	**Class ATE**	Pass
Evidence of coverage	ATE_COV.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 – Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product "WipeDrive v9.1" are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [TDS].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 5.1.1 of the Security Target [TDS]. It is assumed that, in the operating environment of the TOE, all the assumptions and the organizational security policies described in the Security Target are respected.

This Certification Report is valid for the TOE in the evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([DEL], [BLD], [OPE], [LOG]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE Delivery

There are three ways that a TOE WipeDrive v9.1 can be delivered: either electronically from developer secure website (www.whitecanyon.com), via CD/DVD, or both electronically and via CD/DVD.

Verifying authenticity and integrity varies slightly with each of these methods.

When the customer downloads the product from the web site, he will also see the MD5 hash for that product. The customer can compare the MD5 hash on the website to his download to confirm authenticity and integrity.

If the customer requests delivery by CD/DVD, the CD/DVD is created for the customer using a disk that has the product name and major version printed on it. The product is then delivered directly to a common carrier for delivery to the customer's site.

More detail on such a procedure are contained in "WhiteCanyon Product Delivery Process" [DEL].

9.2 Installation, initialization and secure usage of the TOE

TOE installation consists of two steps.

1. Preparation and building WipeDrive. The WipeDrive project contains a Linux shell script that is used to build WipeDrive, its supporting libraries and compile the translation files. All the preparation works can be found in the document:
    - WhiteCanyon Building WipeDrive [BLD]
2. TOE installation and configuration should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer, and in particular in:
    - WipeDrive Enterprise User Guide [OPE]
    - WipeDrive Enterprise Logging Manual [LOG]

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “WipeDrive v9.1”, developed by WhiteCanyon Software, Inc.

The TOE is identified in the Security Target [TDS] with the version number 9.1. The name and version number uniquely identify the TOE and the set of its subsystems, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

For more details, please refer to sect. 2 of the Security Target [TDS].

10.1 TOE operational environment

In Table 2 are summarized the minimal requirements of the operational environment of the TOE to allow its correct working.

For more details, please refer to sect. 2.5.1 of the Security Target [TDS].

Component	Requirement
Supported Operating Systems	Windows Mac PC running Linux UNIX
System Requirements	CPU – 1 GHz RAM – 1 GB SVGA or higher video support
Target Device(s)	ATA, SCSI, USB, eMMC, SD, and NVMeblock device that has been identified as a candidate for erasure
Log Storage	Location in which the audit data is stored and is located separately from the TOE. The data can be stored on any form of file storage medium
External Server	A physical server that can utilize FTP or SQL to optionally be used to store logs of erasure events in lieu of the log storage file if desired

Table 2 – TOE operational environment components

11 Annex C – Test activity

This annex describes the task of both the evaluators and the developer in testing activities. For the assurance level EAL2, augmented with ALC_FLR.2 and ASE_TSS.2, such activities include the following three steps:

- evaluation of the tests performed by the developer in terms of coverage;
- execution of independent functional tests by the evaluators;
- execution of penetration tests by the evaluators.

11.1 Test configuration

For the execution of these activities a test environment has been arranged at the LVS site with the support of the developer, which provided the necessary resources.

The installation of the test environment was in accordance with the guidance documentation ([BLD], [OPE], [LOG]), as indicated in Annex A – Guidelines for the secure usage of the product.

After configuration of the TOE the evaluators checked the status and found that the TOE was installed properly, and the needed services were running.

The test environment is the same as the developer used for testing the TSFI.

11.2 Functional tests performed by the developer

11.2.1 Test coverage

The evaluators have examined the test plan presented by the developer and verified the complete coverage of the functional requirements SFR and the TSFIs described in the functional specification.

11.2.2 Test results

The evaluators executed a series of tests, a sample chosen from those described in the test plan presented by the developer, positively verifying the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the evaluators

Therefore, the evaluators have designed independent testing to verify the correctness of the TSFI.

They did not use testing tools in addition to the specific components of the TOE that allowed to check all TSFI selected for independent testing.

In the design of independent tests, the evaluators have considered aspects that in the developer test plan were not present, or ambiguous, or inserted in more complex tests, which covered a mix of interfaces but with a level of detail not adequate.

The evaluators also designed and executed some tests independently from similar tests of the developer, based only on the evaluation documentation.

All independent tests performed by evaluators generated positive results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities the same test environment already used for the activities of the functional tests has been used (see sect. 11.1)

The evaluators have first verified that the test configurations were consistent with the version of the TOE under evaluation, that is indicated in the [TDS], sect. 1.2.

In a first phase, the evaluators have conducted researches using various sources in the public domain, such as Internet, books, publications, conference proceedings, etc., in order to identify known vulnerabilities applicable to types of products similar to the TOE. In this research the Linux operating system has been also considered, part of the operational environment, but needed for the correct operation of the TOE. Some potential vulnerabilities have thus been identified.

In a second step, the evaluators examined the evaluation documentation (Security Target, functional specification, TOE design, security architecture and operational documentation) to identify any additional potential vulnerabilities of the TOE. From this analysis, the evaluators have actually determined the presence of other potential vulnerabilities.

The evaluators have analysed in detail the potential vulnerabilities identified in the two previous steps, to ensure their effective exploitability in the TOE operating environment. This analysis led to identify some actual potential vulnerabilities.

Therefore, the evaluators have designed some possible attack scenarios, with Basic attack potential, and penetration tests to verify the exploitability of the potential candidate vulnerabilities. The penetration tests have been described with sufficient detail for their repeatability using for this purpose test sheets, also used, appropriately compiled with the results, as the report of the tests themselves. The evaluator used the Kali Linux tool for executing the tests.

On the basis of the penetration tests, the evaluators concluded that no attack scenario with potential Basic can be completed successfully in the operating environment of the TOE. Therefore, none of the previously identified potential vulnerabilities can be exploited effectively. However, they have identified a couple of residual logging protocol vulnerabilities related to non secure network transfer methods, i.e. vulnerabilities that could be exploited only by an attacker with attack potential beyond Basic.