National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

WhiteCanyon Inc. WipeDrive 6.1

Report Number: CCEVS-VR-VID10395-2010
Version 1.0
December 14, 2010

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Table of Contents

1 Executive Summary

This Security Target (ST) defines the Information Technology (IT) security requirements for WipeDrive 6.1. WipeDrive is a disk sanitizing tool that permanently erases all data from hard drives and other data storage devices. This includes but is not exclusive to: HPA partitions, DCO partitions, remapped sectors, operating systems, programs, and user files. This data is permanently destroyed as to make any type of forensic data recovery impossible.

The TOE primarily provides data destruction in accordance with US DoD 5220.22-M. WipeDrive complies with all of the following disk wipe standards:

- US DoD 5220.22-M
- Standard single pass overwrite
- US Army AR380-19
- US Air Force System Security Instruction 5020
- US Navy Staff Office Publication P-5329-26
- US National Computer Security Center TG-025
- Australian Defense Signals Directorate ACSI-33 (X0-PD)
- Australian Defense Signals Directorate ACSI-33 (X1-P-PD)
- Canadian RCMP TSSIT OPS-II Standard Wipe
- CIS GOST P50739-95
- GB HMG Infosec Standard #5 Baseline
- GB HMG Infosec Standard #5 Enhanced
- German VSITR

Upon completion of data sanitization an audit log is created detailing the wipe process. This includes the drive serial number, date of sanitization, pattern used, and protections removed. This audit log certifies compliance with the needed regulatory requirement(s). All wipe functions overwrite disk storage 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.

WipeDrive has been tested to conform to the wipe standards identified within this Validation Report and the Security Target, which resulted in the verification that all of the requirements defined within these standards have been met.

Administrators access the TUI or 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.

The only users of the TOE are referred to as administrators. Administrators, whether through the GUI or TUI, 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 UI 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, MySQL database, or other media storage device.

2 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product	WhiteCanyon Inc. WipeDrive 6.1
Sponsor & Developer	WhiteCanyon Inc., Orem, UT
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	January 2011
CC	*Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Interpretations	None.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Evaluation Class	EAL4 Augmented ALC_FLR.2 and ASE_TSS.2
Description	The TOE is the WipeDrive Live CD, which is a security software product developed by WhiteCanyon, Inc. as a Sensitive Data Protection tool.
Disclaimer	The information contained in this Validation Report is not an endorsement of the WipeDrive product by any agency of the U.S. Government, and no warranty of the product is either expressed or implied.
PP	None.
Evaluation Personnel	Justin Fisher John Schroeder Jeremy Sestok Andrea Wright Emmanuel Apau Seyithan Ayhan Amit Sharma
Validation Body	NIAP CCEVS

2.1 Threats to Security

Table 2 summarizes the threats that the evaluated product addresses.

Table 2 – Threats

An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
A malicious user or process failure may cause the TOE to fail to record or improperly record audit data, thus masking a user's action.
Any person with access to a target environmental resource can access residual data, either due to a wipe operation being incomplete or a completed wipe operation being insufficient.
An unauthorized user can obtain the physical medium which contains the TOE and can use it to perform a wipe operation against an environmental resource which there has been no authorization to wipe.

3 Identification

The product being evaluated is WhiteCanyon Inc. WipeDrive 6.1.

4 Security Policy

4.1 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 of failure) is stored in the Log Storage component. The resulting output of a wipe operation is displayed in an easily interpretable manner. Other events that are recorded include the start-up and shutdown of the audit functions and various parameters related to the TOE's probe, scan, and subsequent erasure of targets on a drive. 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.

4.2 Security Management

The only users of the TOE are referred to as administrators. Administrators 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 storage (in the Log Storage component), 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; and
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 can be operated via two user interfaces – a TUI or GUI. The TUI runs on the same host as the WipeDrive application (back-end). It is used primarily for systems that do not have framebuffer support – which is typical on many architectures other than x86. The GUI is also run on the same host as the back-end. This will be the default interface for x86 machines where a framebuffer can be accessed.

4.3 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 while the probe operation is run each time a device is discovered. Administrators, whether via the GUI or TUI, can execute commands 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.

4.4 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.

5 Assumptions

5.1 Personnel Assumptions

Table 3 – Personnel Assumptions

One or more authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.
Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.

5.2 Physical Assumptions

Table 4 – Physical Assumptions

The TOE will be loaded onto the same physical machine as the target resource so that commands are not exposed over the network.

The physical medium which contains the TOE will be located in a secure location and physical custody is maintained by one or more authorized administrators.

5.3 Logical Assumptions

Table 5 – Logical Assumptions

Administrators of the Operational Environment exercise due diligence to acquire updated versions of the TOE and patch the Operational Environment (e.g., OS and database) so they are not susceptible to attacks resulting in malfunction of the TOE or associated audit data.

6 Clarification of Scope

The TOE includes all the code that enforces the policies identified (see Section 4).

The evaluated configuration of the TOE includes the WhiteCanyon Inc. WipeDrive 6.1 product that is a live CD executable run within a computing environment.

The Network GUI feature is not included in the scope of the evaluation.

MediaWiper is a separately licensed product that also resides on the Live CD, but is not enabled without the additional license. The features of MediaWiper have not been included in the scope of the evaluation.

6.1 System Requirements

The following hardware and software requirements are required for the TOE and environment for TOE functionality to operate properly:

TOE:

- WipeDrive 6.1: A 150 MB Linux-based disc based on the Gentoo meta-distribution which is configured to start WipeDrive upon booting up. Also contained on the disc is a Windows executable file that takes initial input parameter, modifies the boot loader in order to add a Gentoo RAM disc, then reboots the system into the disc where the program is run.

Environment:
WipeDrive Target Machine:

- CPU – 156 MHz
- RAM – 64 MB
- VGA or higher video support
- ATA- or SCSI-block 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 MySQL to optionally be used to store logs of erasure events in lieu of the log storage file if desired.

7 Architectural Information

The TOE’s boundary has been defined in Figure 1.

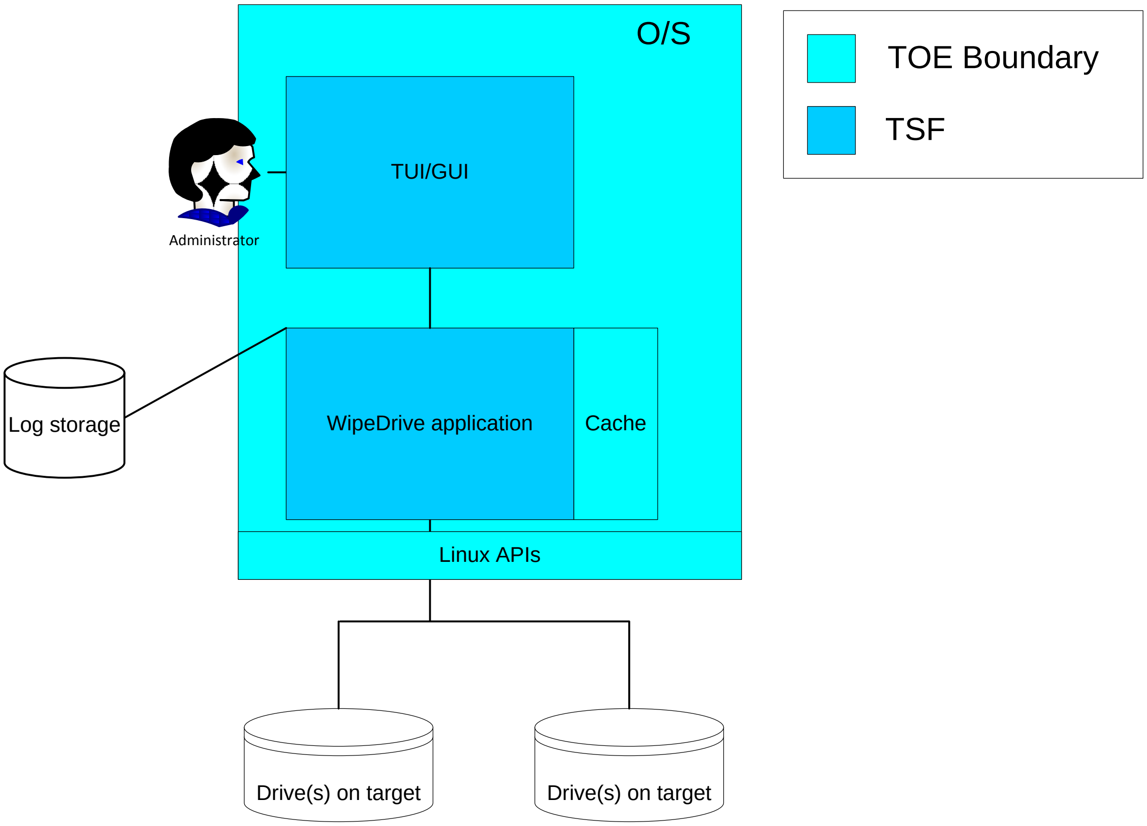

Figure 1 – TOE Boundary for WhiteCanyon Inc. WipeDrive 6.1

7.1 TOE Components

7.1.1 WipeDrive Application

The WipeDrive application serves as a single executable file that is 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 or DCO areas)
- producing progress event messages for consumption by a UI for display to the user
- producing result messages for consumption by a UI and/or logging facilities

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

7.1.2 User Interfaces (UI)

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

- TUI – A text-based UI, run on the same host as the back-end. It is used primarily for systems that do not have framebuffer support – which is typical on many architectures other than x86.
- GUI – A graphical UI that is run on the same host as the back-end. This will be the default interface for x86 machines where a framebuffer can be accessed.

7.1.3 Cache

The cache stores data about scanned and probed devices in order to display that information to users. The cache component is also responsible for the auditing of data that is collected. The audit data received from the WipeDrive application is stored in the cache, which sends a copy of the same data back to both the Log Storage component and interface the user is currently using.

7.1.4 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 the data. This is a built-in function of the Operating System.

8 TOE Acquisition

The NIAP-certified WipeDrive product is acquired via normal sales channels, and physical delivery of the TOE is coordinated with the end customer by WhiteCanyon Inc.

These documents were evaluated to satisfy assurance requirements:

- WipeDrive Enterprise User Guide Software Version 6.1
- WhiteCanyon WipeDrive 6.1 Security Target v1.0

No other documents were provided within the TOE delivery and the evaluation team was able to complete the evaluation using the documents listed above.

9 IT Product Testing

The test team's test approach is to test the security mechanisms of WipeDrive by exercising the external interfaces to the TOE and viewing the TOE behavior either remotely, or on the platform. Each TOE external interface is described in the appropriate design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design (TDS), Functional Specification (FSP), Low Level Design documents (LLDs), and the vendor's test plans were used to demonstrate test coverage of all *appropriate* EAL4 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that were determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

EAL4 requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

The evaluation team created a test plan that contained a sample of the vendor functional test suite, and supplemental functional testing of the vendors' tests. Booz Allen also performed vulnerability assessment and penetration testing.

9.1 TEST METHODOLOGY

9.1.1 Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The Evaluation Team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.
The team tested the following areas:

- Eavesdropping on Communications
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network. This test was specialized for the following interfaces:
  - FTP logging
  - Email logging
- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- Vulnerability Scanner (Nessus)

This test used the Nessus Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE. The scanner probes a wide range of vulnerabilities that includes but is not limited to the following:

Backdoors
CGI abuses
Denial of Service
Finger abuses
Firewalls
FTP
Gain a shell remotely
Gain root remotely
General
Miscellaneous
Netware
NIS
Port scanners
Remote file access
RPC
Settings
SMTP Problems
SNMP
Untested
Useless services

- Host Protected Area (HPA) and Device Configuration Overlay (DCO)
  This test creates a disk that contains preconfigured data as well as a DCO hidden area with an HPA hidden area included inside it. The product should be able to detect and remove data included inside of DCO and HPA sections. If not, then it could be possible to hide data within these sections.
- ATA Security
  This test attempts to wipe a drive that has been preconfigured with an ATA security password. WipeDrive may not be able to effectively wipe the drive, but it should be able to present an appropriate error to the user. ATA security may be a mechanism by which a malicious user could create a device that cannot be wiped by WipeDrive.
- Faulty Sectors
  This test attempts to create a device that has been marked with faulty sectors and feed it into WhiteCanyon for wiping. WhiteCanyon should be able to successfully erase all data surrounding the faulty sectors and should flag them as faulty appropriately.

9.1.2 Vulnerability Results

The testing staff, upon completion of the vulnerability testing process, were able to verify that all tested areas of potential vulnerability contained no actual vulnerabilities. However, administrators tasked with operating the TOE are expected to follow the user guidance provided appropriately to ensure secure operation. Informational notes for the TOE found during testing can be found in the following section, Section 9.1.2.1.

9.1.2.1 Informational Notes

Network Authentication Credentials Disclosed

The authentication credentials for FTP and SMTP servers are transmitted in cleartext as the TOE does not provide any encryption functionality.

Cleaning DCO Sectors Does Not Work In All Environments

Through the functional and independent testing, the functionality of DCO did not work on all testing environments. Through research, the evaluation team was able to determine that any BIOS that performs a DCO freeze lock upon detecting a hard drive will not allow DCO functionality to be performed by any program, including WipeDrive. This means that if a drive was used in the same machine environment through its entire life cycle, it should not have any DCO sectors for WipeDrive to clean. WipeDrive has also been updated to alert users when DCO functionality is blocked by the BIOS upon performing a wipe or a verify function. DCO positive testing was performed on an Intel DG43GT motherboard.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the WhiteCanyon Inc. WipeDrive 6.1 TOE meets the security requirements contained in the Security Target.

The criteria against which the WipeDrive TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the WhiteCanyon Inc. WipeDrive 6.1 TOE is EAL4 augmented with ALC_FLR.2. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed in January 2011. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

11 Validator Comments/Recommendations

11.1 Secure Installation and Configuration Documentation

The “WipeDrive Enterprise User Guide Software Version 6.1” document defines the recommendations and secure usage directions for the TOE as derived from testing.

11.2 Additional Validator Comments

Additional validator comments are already captured above in the “Clarification of Scope” (6) and “Informational Notes” (9.1.2.1) sections.

12 Security Target

The security target for this product’s evaluation is WhiteCanyon WipeDrive 6.1 Security Target, Version 0.4, September 24 2010.

13 List of Acronyms

Acronym	Definition
ATA	Advanced Technology Attachment
BIOS	Basic Input/Output System
DCO	Device Configuration Overlay
DHCP	Dynamic Host Configuration Protocol
GNU	*Recursive acronym for GNU’s Not Unix*

HPA	Host Protected Area
JSON	JavaScript Object Notation
LBA	Logical Block Addressing
OS	Operating System
PXE	Preboot eXecution Environment
RPC	Remote Procedure Call Protocol
SCSI	Small Computer System Interface
UI	User Interface

14 Terminology

Terminology	Definition
Administrator	Any user of the TOE who maintains physical possession of the WipeDrive application
Administrator Definable Wipe Pattern	A concatenation of static primitives that is not persistent between boots.
ATA HPA	ATA Host Protected Area Refers to as a hidden protected area that is a section of a hard drive that is not normally visible to an Operating System
Kernel	The central component for most Operating Systems (in this case, UNIX) that is primarily responsible for starting and stopping programs, handling the file system, as well as other low level tasks most programs share.
LAB28/LBA48	A common scheme used for specifying the location of blocks of data stored on computer storage devices, generally secondary storage systems such as hard disks. LBA48, in particular, refers to a logical block address that is 28- or 48-bits wide, resulting in a disk size limit.
LiveCD	A Linux-based compact disc based on the Gentoo meta-distribution which is configured to start WipeDrive upon booting up.
Log/Logging	Synonymous with audit/auditing
Preboot eXecution Environment (PXE)	An environment to boot computers using a network interface independently of available data storage devices (e.g. hard disks) or installed Operating Systems.
White Canyon	Vendor
WipeDrive	Product

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 3.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 3.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 3.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.
5. WhiteCanyon WipeDrive 6.1 Security Target, Version 1.0, January 25 2011.
6. Evaluation Technical Report for a Target of Evaluation “WhiteCanyon WipeDrive 6.1” Evaluation Technical Report, Version 1.0, 14 December 2010.