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 IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

WipeDrive v9.1

OCSI/CERT/CCL/08/2018/RC

Versione 1.0

27 marzo 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	27/03/2019

2 Indice

3 Elenco degli acronimi

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 Riferimenti

4.1 Criteri e normative

[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 Documenti tecnici

[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 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su http://www.sogisportal.eu.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA per tutti i componenti di garanzia indicati.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL 2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia indicati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "WipeDrive v9.1", sviluppato dalla società WhiteCanyon Software, Inc.

L'ODV è uno strumento di pulizia per dischi magnetici che cancella permanentemente da un sistema i dati del disco rigido, i sistemi operativi, i file dei programmi e tutti gli altri file di dati. WipeDrive offre inoltre agli utenti la possibilità di eliminare definitivamente tutte le partizioni precedentemente configurate.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL2, con aggiunta di ALC_FLR.2 e ASE_TSS.2, in conformità a quanto indicato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione riassume l'esito della valutazione di sicurezza del prodotto "WipeDrive v9.1" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

I potenziali acquirenti sono quindi tenuti a consultare il presente Rapporto di Certificazione congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	WipeDrive v9.1
Traguardo di Sicurezza	"WipeDrive v9.1" Server Security Target, v1.3, 7 February 2019
Livello di garanzia	EAL2 con aggiunta di ALC_FLR.2 e ASE_TSS.2
Fornitore	WhiteCanyon Software, Inc.
Committente	WhiteCanyon Software, Inc.
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	16 ottobre 2018
Data di fine della valutazione	21 febbraio 2019

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono riassunte le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV è uno strumento di pulizia per dischi magnetici che cancella permanentemente da un sistema i dati del disco rigido, i sistemi operativi, i file dei programmi e tutti gli altri dati dei file. WipeDrive offre inoltre agli utenti la possibilità di eliminare definitivamente tutte le partizioni precedentemente configurate. L'ODV fornisce 20 funzioni di pulizia del disco. Tutte le funzioni di cancellazione sovrascrivono la memoria del disco o utilizzano comandi di cancellazione speciali nativi per le unità, per garantire che non rimangano dati residui.

Una volta completato il processo di cancellazione, viene creato un registro di controllo che consente di verificare che le informazioni contenute nel disco rigido siano state effettivamente cancellate.

L'ODV:

- è basato su un sistema operativo Linux avviato da un LiveCD, EXE o PXE Server, che risiede nella memoria durante l'esecuzione;
- è uno strumento di protezione e cancellazione dei dati che cancella permanentemente i dati dai dispositivi ATA, SCSI, USB, eMMC e NVMe-block. Questo include unità disco tradizionali e SSD;
- consente agli utenti di creare un registro di controllo per acquisire le verifiche del successo o del fallimento degli eventi di cancellazione del disco rigido;
- ha la capacità di cancellare completamente i sistemi operativi, i file di programma e tutti i dati dei file;
- utilizza le interfacce utente per consentire agli amministratori di vedere graficamente l'andamento degli eventi di analisi, scansione e cancellazione;
- consente agli amministratori di visualizzare i dati del settore.

7.3.1 Architettura dell'ODV

Per una descrizione maggiormente dettagliata dell'ODV, consultare il capitolo 2 del [TDS]. Di seguito sono riassunti alcuni aspetti ritenuti rilevanti (vedi Figura 1).

Gli unici utenti dell'ODV sono indicati come amministratori, i quali possono eseguire comandi per cancellare le unità utilizzando modelli di cancellazione definibili dall'amministratore stesso. La verifica del successo o del fallimento dell'evento di cancellazione viene inviata all'interfaccia che l'utente sta utilizzando. Inoltre, i dati del log di controllo raccolti dall'evento di cancellazione sono memorizzati in/su un dispositivo di archiviazione dei registri, che può essere: unità flash/pen drive, server FTP, database SQL, directory di condivisione di Windows o altri supporti.

Gli amministratori accedono alla GUI per eseguire il file eseguibile per l'applicazione WipeDrive. Una volta eseguita l'applicazione WipeDrive, la cache memorizza i dati sui dispositivi scansionati e analizzati per visualizzare i dati agli utenti. La scansione e l'analisi vengono entrambi eseguiti durante l'inizializzazione dell'ODV. L'applicazione WipeDrive esegue un'operazione di scansione per individuare i dispositivi collegati. Per ogni dispositivo rilevato, viene eseguita un'operazione di analisi per elencare le informazioni sul dispositivo.

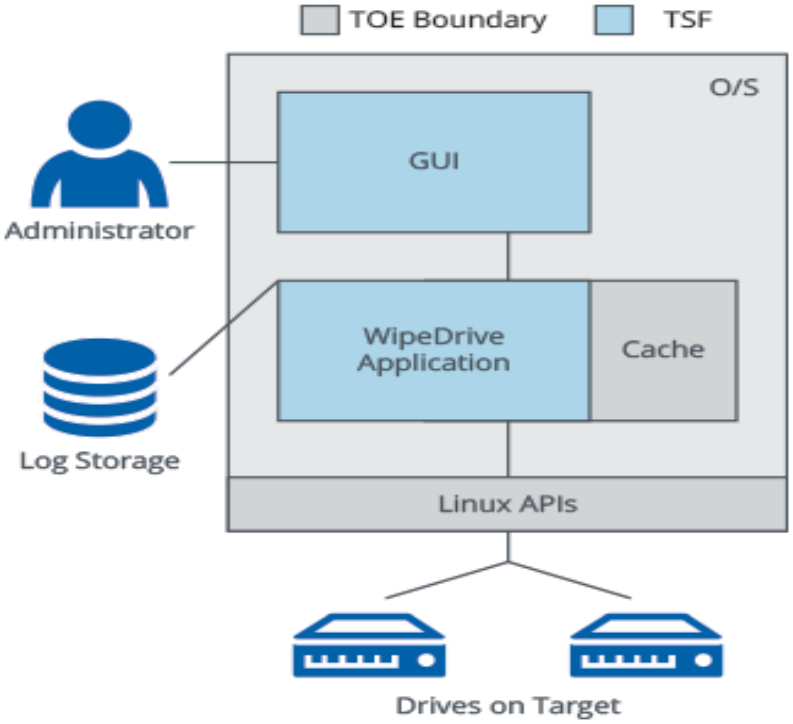

Figura 1 – Confini dell'ODV

7.3.1.1 WipeDrive application

L'applicazione WipeDrive funge da singolo file eseguibile principalmente responsabile di:

- scansione del sistema per dispositivi che possono essere oggetto di cancellazione;
- analisi dei dispositivi rilevati per le funzionalità;
- cancellazione dei dispositivi ed esecuzione di operazioni correlate (come la rimozione di ATA, HPA, aree DCO o impostazioni di indirizzo massimo accessibile);
- invio messaggi sull'avanzamento degli eventi o sui risultati per la consultazione da parte dell'interfaccia utente;
- registrazione dopo che è stata completata la cancellazione del supporto.

Solo una singola applicazione WipeDrive potrà essere eseguita su un singolo host in qualsiasi momento.

7.3.1.2 User Interfaces

L'interfaccia utente funge da interfaccia fisica in cui i controlli vengono utilizzati per gestire una o più istanze dell'applicazione WipeDrive, ciascuna su un host distinto. Le interfacce incluse nella configurazione valutata sono:

- GUI – Un'interfaccia utente grafica che viene eseguita sullo stesso host dell'applicazione WipeDrive. Questa sarà l'interfaccia di default per macchine x86 a cui è possibile accedere tramite *frame buffer*.

7.3.1.3 Linux APIs

Le API di Linux forniscono un'interfaccia logica tra l'applicazione e le unità di destinazione. Ad esempio, quando l'ODV esegue la scansione di un disco, si affida a Linux per raccogliere alcuni dati. Questa è una funzione integrata del sistema operativo.

7.3.1.4 Third Party Programs

Con il sistema operativo Linux sono opzionalmente inclusi vari programmi che forniscono funzionalità utilizzate da WipeDrive.

7.3.2 Caratteristiche di Sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nei cap. 4 e 5 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il cap. 9 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

- **Security Audit**. L'ODV genera e acquisisce i dati di audit utilizzati per fornire un'ulteriore verifica della presenza di un evento di cancellazione. I registri di controllo contenenti i dati di verifica (che denotano un esito positivo o negativo) sono memorizzati internamente all'applicazione WipeDrive. L'output risultante di un'operazione di cancellazione viene visualizzato in modo facilmente interpretabile. Tutte le operazioni di controllo possono essere associate all'amministratore che ha eseguito quell'evento. L'ODV salva gli eventi di controllo in un formato leggibile dall'utente al di fuori dell'ODV ma non è responsabile di facilitare la visualizzazione dei record di controllo ad eccezione di una revisione dei risultati di cancellazione immediatamente dopo un'operazione di cancellazione.

- **Security Management**. Gli unici utenti dell'ODV sono indicati come amministratori, i quali mantengono l'accesso fisico all'applicazione WipeDrive e, di conseguenza, possiedono diverse capacità di gestione. Gli amministratori possono specificare il percorso per l'archiviazione di controllo, specificare il formato in cui questi dati vengono archiviati, creare, eseguire, visualizzare o eliminare un modello di cancellazione definibile dall'amministratore, analizzare dispositivi, visualizzare dati di settore, e ottenere informazioni sul dispositivo per tutti i dispositivi precedentemente sottoposti a scansione. L'ODV è equipaggiato per funzionare tramite varie interfacce messe a disposizione degli amministratori. Gli amministratori dell'ODV utilizzano queste interfacce per eseguire le funzioni di gestione sopra elencate. Gli scopi principali di queste interfacce sono:

    1. consentire ai comandi definiti dall'ODV di essere richiamati nell'applicazione WipeDrive allegata;

    2. visualizzare visivamente lo stato dell'applicazione WipeDrive allegata interpretando le risposte e le notifiche ricevute;

    3. creare registri di controllo in base alle preferenze dell'utente. I registri possono essere memorizzati su qualsiasi tipo di supporto che l'utente desidera (ad esempio una pen drive o un server FTP).

L'ODV viene gestito principalmente tramite l'interfaccia GUI. La GUI viene eseguita anche sullo stesso host dell'applicazione WipeDrive. Questa sarà l'interfaccia di default per macchine x86 a cui è possibile accedere tramite *frame buffer*.

- **Disk Erasure**. L'ODV è in grado di eseguire tre operazioni distinte di pulizia dei dischi: scansione dei dispositivi, analisi dei dispositivi e cancellazione dei dispositivi. La scansione e l'analisi vengono eseguite entrambe durante l'inizializzazione dell'ODV. Gli amministratori possono eseguire comandi tramite la GUI per cancellare le unità. Il comando *wipe* applica il modello di cancellazione definibile dall'amministratore a ciascuna istanza del disco selezionata, ed esegue le operazioni di sovrascrittura direttamente sul disco.

- **User Data Protection**. L'ODV prevede la cancellazione delle informazioni residue. Questa cancellazione viene avviata alle interfacce utente e richiede la comunicazione con il repository di informazioni (disco). Nessuna informazione residua risiederà nella RAM dopo un evento di cancellazione.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita ai clienti insieme al prodotto. La documentazione indicata contiene tutte le informazioni richieste per l'installazione, l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Tutti i Requisiti Funzionali (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si

raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS CCLab Software Laboratory.

L'attività di valutazione è terminata in data 21 febbraio 2019 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV], che è stato approvato dall'Organismo di Certificazione il 13 marzo 2019. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS CCLAB Software Laboratory e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "WipeDrive v9.1" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL2, con aggiunta di ALC_FLR.2 e ASE_TSS.2, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL2, con aggiunta di ALC_FLR.2 e ASE_TSS.2.

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

Classi e componenti di garanzia		Verdetto
Flaw reporting procedures	ALC_FLR.2	Positivo
Test	**Classe ATE**	Positivo
Evidence of coverage	ATE_COV.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Vulnerability analysis	AVA_VAN.2	Positivo

Tabella 1 – Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "WipeDrive v9.1" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 5.1.1 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di sicurezza organizzative e le ipotesi descritte nel TDS.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata; in particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto include una serie di raccomandazioni relative alla consegna, all'inizializzazione e all'utilizzo sicuro del prodotto, secondo le indicazioni contenute nella documentazione operativa fornita insieme all'ODV ([DEL], [BLD], [OPE], [LOG]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per i potenziali acquirenti del prodotto.

9.1 Consegna

Ci sono tre modi in cui un ODV WipeDrive v9.1 può essere consegnato: elettronicamente dal sito Web sicuro del Fornitore (www.whitecanyon.com), tramite CD/DVD, o sia elettronicamente che tramite CD/DVD.

Verificare l'autenticità e l'integrità varia leggermente con ciascuno di questi metodi.

Quando il cliente scarica il prodotto dal sito Web, vedrà anche l'hash MD5 per quel prodotto. Il cliente può confrontare l'hash MD5 sul sito Web con quello della versione scaricata per confermare l'autenticità e l'integrità.

Se il cliente richiede la consegna tramite CD/DVD, il CD/DVD viene creato per il cliente utilizzando un disco con il nome del prodotto e la versione principale stampata su di esso. Il prodotto viene quindi consegnato direttamente a un comune corriere per la consegna al sito del cliente.

Maggiori dettagli su tali procedure sono riportati nel documento "WhiteCanyon Product Delivery Process" [DEL].

9.2 Installazione, inizializzazione ed utilizzo sicuro dell'ODV

L'installazione dell'ODV si compone di due fasi.

1. Preparazione e costruzione del WipeDrive. Il progetto WipeDrive contiene uno script shell di Linux che viene utilizzato per costruire WipeDrive, le sue librerie di supporto e compilare i file di traduzione. Tutte le attività di preparazione sono riportate nel documento:
    - WhiteCanyon Building WipeDrive [BLD]
2. L'installazione e la configurazione dell'ODV devono essere eseguite seguendo le istruzioni nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente, in particolare in:
    - WipeDrive Enterprise User Guide [OPE]
    - WipeDrive Enterprise Logging Manual [LOG]

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "WipeDrive v9.1", sviluppato dalla società WhiteCanyon Software, Inc.

L'ODV è identificato nel Traguardo di Sicurezza [TDS] con il numero di versione 9.1. Il nome e il numero di versione identificano univocamente l'ODV e l'insieme dei suoi componenti, costituenti la configurazione valutata dell'ODV, verificata dai Valutatori all'atto dell'effettuazione dei test e a cui si applicano i risultati della valutazione stessa.

Per maggiori dettagli, consultare anche il cap. 2 del [TDS].

10.1 Ambiente operativo dell'ODV

In Tabella 2 sono riportati sinteticamente i requisiti minimi dell'ambiente operativo dell'ODV per consentirne la corretta operatività.

Per maggiori dettagli, consultare anche il par. 2.5.1 del [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

Tabella 2 – Componenti dell'ambiente operativo dell'ODV

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL2, con aggiunta di ALC_FLR.2 e ASE_TSS.2, tali attività prevedono tre passi successivi:

- valutazione in termini di copertura dei test eseguiti dal Fornitore;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

Per l'esecuzione dei test è stato predisposto un apposito ambiente di test presso la sede dell'LVS con il supporto del Committente/Fornitore, che ha fornito le risorse necessarie.

L'installazione dell'ambiente di test è avvenuta seguendo le istruzioni contenute nella documentazione di supporto ([BLD], [OPE], [LOG]), come indicato in Appendice A – Indicazioni per l'uso sicuro del prodotto. Dopo la configurazione dell'ODV i valutatori hanno verificato che l'ODV è stato installato correttamente e tutti i servizi previsti funzionavano correttamente.

L'ambiente di test così realizzato è lo stesso utilizzato dal Fornitore per testare le TSFI.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Copertura dei test

I valutatori hanno esaminato il piano di test presentato dal Fornitore e hanno verificato la completa copertura dei requisiti funzionali (SFR) e delle TSFI descritte nelle specifiche funzionali.

11.2.2 Risultati dei test

I Valutatori hanno eseguito una serie di test, scelti a campione tra quelli descritti nel piano di test presentato dal Fornitore, verificando positivamente il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

Successivamente, i Valutatori hanno progettato dei test indipendenti per la verifica della correttezza delle TSFI.

Non sono stati utilizzati strumenti di test particolari, oltre ai componenti dell'ODV che hanno permesso di sollecitare tutte le TSFI selezionate per i test indipendenti.

Nella progettazione dei test indipendenti, i Valutatori hanno considerato aspetti che nei test del Fornitore erano non presenti o ambigui o inseriti in test più complessi che

interessavano più interfacce contemporaneamente ma con un livello di dettaglio non ritenuto adeguato.

I Valutatori, infine, hanno anche progettato ed eseguito alcuni test in modo indipendente da analoghi test del Fornitore, sulla base della sola documentazione di valutazione.

Tutti i test indipendenti eseguiti dai Valutatori hanno dato esito positivo.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività è stato utilizzato lo stesso ambiente di test già utilizzato per le attività dei test funzionali (cfr. par. 11.1). I Valutatori hanno innanzitutto verificato che le configurazioni di test fossero congruenti con la versione dell'ODV in valutazione, cioè quella indicata nel [TDS], par. 1.2.

In una prima fase, i Valutatori hanno effettuato delle ricerche utilizzando varie fonti di pubblico dominio, quali internet, libri, pubblicazioni specialistiche, atti di conferenze, ecc., al fine di individuare eventuali vulnerabilità note applicabili a tipologie di prodotti simili all'ODV. In questa ricerca è stato considerato anche il sistema operativo Linux, facente parte dell'ambiente operativo, ma comunque necessario al corretto funzionamento dell'ODV. Sono state così individuate alcune vulnerabilità potenziali.

In una seconda fase, i Valutatori hanno esaminato i documenti di valutazione (TDS, specifiche funzionali, progetto dell'ODV, architettura di sicurezza e documentazione operativa) al fine di evidenziare eventuali ulteriori vulnerabilità potenziali dell'ODV. Da questa analisi, i Valutatori hanno effettivamente determinato la presenza di altre vulnerabilità potenziali.

I Valutatori hanno analizzato nel dettaglio le potenziali vulnerabilità individuate nelle due fasi precedenti, per verificare la loro effettiva sfruttabilità nell'ambiente operativo dell'ODV. Quest'analisi ha portato a individuare alcune effettive vulnerabilità potenziali.

I Valutatori hanno quindi progettato dei possibili scenari di attacco, con potenziale di attacco Basic, e dei test di intrusione per verificare la sfruttabilità di tali vulnerabilità potenziali candidate. I test di intrusione sono stati descritti con un dettaglio sufficiente per la loro ripetibilità avvalendosi a tal fine delle schede di test, utilizzate in seguito, opportunamente compilate con i risultati, anche come rapporto dei test stessi. Per l'esecuzione dei test i Valutatori hanno utilizzato lo strumento Kali Linux.

Sulla base dei risultati dei test di intrusione, i Valutatori hanno così concluso che nessuno degli scenari di attacco ipotizzati con potenziale Basic può essere portato a termine con successo nell'ambiente operativo dell'ODV. Pertanto, nessuna delle vulnerabilità potenziali precedentemente individuate può essere effettivamente sfruttata. Sono state invece individuate nel protocollo di registrazione un paio di vulnerabilità residue relative a metodi di trasferimento di rete non sicuri; tali vulnerabilità potrebbero però essere sfruttate solo da attaccanti con potenziale di attacco superiore a Basic.