



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

Agence nationale de la sécurité
des systèmes d'information

Rapport de certification ANSSI-CSPN-2021/04

Blanco Drive Eraser Version 6.12.0

Paris, le 18 février 2021

Le directeur général de l'Agence nationale de la
sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]



AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CSPN-2021/04
Nom du produit	Blancco Drive Eraser
Référence/version du produit	Version 6.12.0
Catégorie de produit	Effacement de données
Critère d'évaluation et version	CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)
Commanditaire	BLANCCO TECHNOLOGY GROUP IP OY Länsikatu 15 FIN-80110 Joensuu, Finlande
Développeur	BLANCCO TECHNOLOGY GROUP IP OY Länsikatu 15 FIN-80110 Joensuu, Finlande
Centre d'évaluation	AMOSSYS 11 rue Maurice Fabre 35000 Rennes, France
Fonctions de sécurité évaluées	Détection de disque et des partitions Effacement sécurisé Vérification de l'effacement Génération de rapport Gestion des clés
Fonctions de sécurité non évaluées	Néant
Restriction(s) d'usage	Non

PREFACE

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit évalué.....	6
1.2.1	Catégorie du produit	6
1.2.2	Identification du produit	7
1.2.3	Fonctions de sécurité.....	7
1.2.4	Configuration évaluée	7
2	L'évaluation.....	8
2.1	Référentiels d'évaluation.....	8
2.2	Charge de travail prévue et durée de l'évaluation.....	8
2.3	Travaux d'évaluation	8
2.3.1	Installation du produit.....	8
2.3.2	Analyse de la documentation.....	8
2.3.3	Revue du code source (facultative).....	8
2.3.4	Analyse de la conformité des fonctions de sécurité	9
2.3.5	Analyse de la résistance des mécanismes des fonctions de sécurité	9
2.3.6	Analyse des vulnérabilités (conception, construction, etc.)	9
2.3.7	Analyse de la facilité d'emploi	9
2.4	Analyse de la résistance des mécanismes cryptographiques	9
2.5	Analyse du générateur d'aléas.....	9
3	La certification	10
3.1	Conclusion.....	10
3.2	Recommandations et restrictions d'usage.....	10
ANNEXE A.	Références documentaires du produit évalué	11
ANNEXE B.	Références à la certification.....	12

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Blancco Drive Eraser, Version 6.12.0 » développé par BLANCCO TECHNOLOGY GROUP IP OY.

La fonction principale de la TOE est d'effectuer une détection de matériel sur un ordinateur hôte, d'afficher une liste des périphériques de stockage disponibles à l'utilisateur puis d'effacer les périphériques cibles sélectionnés selon une norme d'effacement choisie. Les périphériques peuvent être des disques durs classiques dits *hard disk drive* (HDD) ou *solid-state drive* (SSD).

Une fois l'effacement effectué un rapport est fourni à l'utilisateur explicitant les informations détaillées sur le matériel connecté et le processus d'effacement, y compris des informations sur le temps, des détails sur les zones cachées, les secteurs *remappés* et une liste de tous les problèmes rencontrés pendant l'effacement.

Le produit est distribué sous forme d'image ISO. L'outil *Drive Eraser Configuration Tool* (DECT) de *BLANCCO TECHNOLOGY GROUP IP OY* est utilisé pour configurer cette image ISO. Une fois l'image déployée sur une clé USB, elle est utilisée pour démarrer l'ordinateur hôte dont on veut effacer le disque.

1.2 Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 Catégorie du produit

<input type="checkbox"/>	1	détection d'intrusions
<input type="checkbox"/>	2	anti-virus, protection contre les codes malicieux
<input type="checkbox"/>	3	pare-feu
<input checked="" type="checkbox"/>	4	effacement de données
<input type="checkbox"/>	5	administration et supervision de la sécurité
<input type="checkbox"/>	6	identification, authentification et contrôle d'accès
<input type="checkbox"/>	7	communication sécurisée
<input type="checkbox"/>	8	messagerie sécurisée
<input type="checkbox"/>	9	stockage sécurisé
<input type="checkbox"/>	10	environnement d'exécution sécurisé
<input type="checkbox"/>	11	terminal de réception numérique (<i>Set top box</i> , STB)
<input type="checkbox"/>	12	matériel et logiciel embarqué
<input type="checkbox"/>	13	automate programmable industriel
<input type="checkbox"/>	99	autre

1.2.2 Identification du produit

Produits	
Nom du produit	Blancco Drive Eraser
Numéro de la version évaluée	Version 6.12.0

Une fois le logiciel démarré, le numéro de version apparaît en haut à gauche de l'écran.

1.2.3 Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- la détection de disque et des partitions ;
- l'effacement sécurisé ;
- la vérification de l'effacement ;
- la génération de rapport ;
- la gestion des clés.

1.2.4 Configuration évaluée

La plateforme de test est constituée des éléments suivants :

- un *Dell Latitude e6430* avec un SSD *Samsung 850 EVO* d'une capacité de 250 Go ;
- un *Dell Inspiron* avec un HDD *Western Digital 75G33T0* d'une capacité de 500 Go ;
- une clé USB.

Les outils suivants ont été utilisés :

- *Drive Eraser Configuration Tool* en version 2.12.0, permettant la configuration de l'image ISO à copier ensuite sur une clé USB *bootable* ;
- *Enterprise USB Erasure Enablement*, en version 1.2.2, permettant l'écriture de l'image ISO sur la clé USB *bootable* ;

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en ANNEXE B.

2.2 Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1 Installation du produit

2.3.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.3.1.2 Description de l'installation et des non-conformités éventuelles

L'installation de la TOE nécessite l'installation d'un *Java Runtime Environment* pour exécuter le logiciel DECT, écrit en *Java*. Pour l'évaluation le CESTI a pris celui d'Oracle.

2.3.1.3 Durée de l'installation

Néant.

2.3.1.4 Notes et remarques diverses

Sans objet.

2.3.2 Analyse de la documentation

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.3.3 Revue du code source (facultative)

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.3.4 Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.3.5 Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.6 Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1 Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

2.3.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitable dans le contexte défini par la cible de sécurité [CDS] et pour le niveau d'attaquant considéré.

2.3.7 Analyse de la facilité d'emploi

2.3.7.1 Cas où la sécurité est remise en cause

Il est possible, avec un accès physique à la clé USB contenant le logiciel, d'extraire l'ISO en vue de le modifier. Il est donc important de respecter l'hypothèse A4.DECT_USERS de la cible de sécurité [CDS].

Les risques identifiés lors de l'évaluation entraînent des recommandations (voir chapitre 3.2).

2.3.7.2 Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté.

2.3.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.4 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

2.5 Analyse du générateur d'aléas

Le générateur aléatoire mis en œuvre par le produit a fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « Blancco Drive Eraser, Version 6.12.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

ANNEXE A. Références documentaires du produit évalué

[CDS]	<p><i>CSPN Security target</i> <i>Product Blancco Drive Eraser version 6.12.0</i> Référence : CSPN-ST-Blancco Drive Eraser 6-3.04 ; Version : 3.04 ; Date : 8 octobre 2020.</p>
[RTE]	<p><i>CSPN Evaluation Technical Report</i> <i>Product Blancco Drive Eraser - version 6.12.0</i> Référence : CSPN-ETR-Blancco Drive Eraser v6.12.0-DR-1.01 ; Version : 1.01 ; Date : 27 janvier 2021.</p> <p><i>Cryptographic Mechanisms Analysis</i> <i>Product Blancco Drive Eraser - version 6.12.0</i> Référence : CSPN-CRY-Blancco Drive Eraser v6.12.0-DR-1.00 ; Version : 1.0 ; Date : 17 décembre 2020.</p>
[GUIDES]	<p><i>BLANCCO DRIVE ERASER: User Manual for version 6.12.</i></p> <p><i>Blancco website :</i> https://support.blancco.com https://servicedesk.blancco.com</p>

ANNEXE B. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	<p>Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01/2.1 du 13 janvier 2020.</p> <p>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019.</p> <p>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018.</p> <p>Documents disponibles sur www.ssi.gouv.fr.</p>
[RGS]	<p>Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.</p>