Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2017/25

Stormshield Endpoint Security

Version 7.2.06 build 29579

Paris, le 7 juin 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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 présupposées 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

Référence du rapport de certification

ANSSI-CC-2017/25

Nom du produit

Stormshield Endpoint Security

Version du produit

Version 7.2.06 build 29579

Conformité à un profil de protection

Application de chiffrement de données à la volée sur mémoire de masse,

PP-CDISK-CCv3.1, v1.4, août 2008

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 3 augmenté

ALC_FLR.3, AVA_VAN.3

Développeur

Stormshield

1, Place Verrazzano,
69009 Lyon, France

Commanditaire

Stormshield

10 rue Marceau,
92130 Issy les Moulineaux, France

Centre d'évaluation

Oppida

4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France

Accords de reconnaissance applicables

CCRA	SOG-IS
Le produit est reconnu au niveau EAL3 augmenté de ALC_FLR.3.	**Le produit est reconnu au niveau EAL3 augmenté de ALC_FLR.3.**

Préface

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 Premier ministre 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 sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. LE PRODUIT 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Services de sécurité 6
1.2.3. Architecture 6
1.2.4. Identification du produit 7
1.2.5. Cycle de vie 7
1.2.6. Configuration évaluée 7

2. L'EVALUATION 8

2.1. REFERENTIELS D'EVALUATION 8
2.2. TRAVAUX D'EVALUATION 8
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 8
2.4. ANALYSE DU GENERATEUR D'ALEAS 8

3. LA CERTIFICATION 9

3.1. CONCLUSION 9
3.2. RESTRICTIONS D'USAGE 9
3.3. RECONNAISSANCE DU CERTIFICAT 9
3.3.1. Reconnaissance européenne (SOG-IS) 9
3.3.2. Reconnaissance internationale critères communs (CCRA) 10

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 11

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 12

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 13

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Stormshield Endpoint Security**,** Version 7.2.06 build 29579 » développé par *STORMSHIELD*, et plus précisément son module fonctionnel de chiffrement de surface, aussi appelé chiffrement de disque avec authentification pré-boot (i.e. avant le démarrage du système d'exploitation).

1.2. Description du produit

1.2.1. Introduction

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

Cette cible de sécurité est conforme au profil de protection [PP-CDISK]. Cette conformité est de type démontrable.

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- le chiffrement initial ;
- l'authentification unique ;
- le recouvrement ;
- la notion d'invité ;
- l'hibernation.

1.2.3. Architecture

Le produit est constitué :

- côté Client :
  - d'un résident BIOS qui gère l'authentification de l'utilisateur et le lancement de Windows ;
  - d'un *driver* Windows qui assure le chiffrement/déchiffrement du disque ;
  - de services, communs à tous les modules fonctionnels de StormShield, qui assurent sous Windows :
    - l'application de la politique de sécurité et l'enregistrement des journaux ;
    - les communications sécurisées avec le serveur (téléchargement de la politique de sécurité, transmission des journaux) ;
    - toutes les fonctions interactives : changement de mot de passe, consultation locale des journaux, etc,

- coté Serveur :
    - des modules qui fournissent les clés de chiffrements et les mots de passe de recouvrement, et qui en assurent le stockage sécurisé dans la base de données ;
- du logiciel installé sur un CD de recouvrement.

Le périmètre physique est constitué des éléments logiciels correspondant aux modules logiques de la TOE.
Les éléments suivants sont hors évaluation :

- le BIOS et le système d'exploitation Microsoft Windows ;
- la base de données dans laquelle sont stockés les secrets ;
- la Console d'administration.

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est la version 7.2.06 build 29579. Le guide [GUIDE] présente au chapitre 3.1.2 une méthode de vérification de l'authenticité du logiciel avant de l'installer.

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement et la livraison du produit sont réalisés sur le site de *STORMSHIELD* ;
- l'installation, l'administration et l'utilisation du produit correspondent au déploiement du produit par le client, tel que décrit au chapitre 1.3.3 de la cible de sécurité [ST].

Le produit a été développé sur le site suivant :

STORMSHIELD

1, Place Verrazzano,
69 009 Lyon, France

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le rôle « administrateur » et comme utilisateur du produit les rôles « utilisateur » et « invité ». Ces rôles sont introduits au chapitre 1.3.2.3 de la cible de sécurité [ST].

1.2.6. Configuration évaluée

Le certificat porte sur la configuration décrite au chapitre 1.4.2 de la cible de sécurité.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 14 avril 2017, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations décrites au chapitre 1 du guide [GUIDE] doivent être suivies.
Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [EXP-CRY]. Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit a fait l'objet d'une analyse. Comme requis dans le référentiel [REF], il comporte un retraitement de nature cryptographique.

Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

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. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « Stormshield Endpoint Security, Version 7.2.06 build 29579 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

3.2. Restrictions d'usage

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

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans le guide fourni [GUIDE], notamment les recommandations au chapitre 1 de ce guide.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, la Pologne, le Royaume-Uni et la Suède.

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs.
Pour les évaluations enregistrées avant septembre 2014, la reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR lorsque les dépendances CC sont satisfaites.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, le Qatar, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**3**	Functional specification with complete summary
	ADV_IMP				**1**	1	**2**	2		
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**2**	Architectural design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**3**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**3**	Implementation representation CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3		
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**1**	Testing: basic design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Stormshield Endpoint Security – Cible de sécurité EAL3+ - version 1.9, 11 avril 2017.
[RTE]	Rapport technique d'évaluation, OPPIDA/CESTI/KIBO/RTE/2.0, 10 avril 2017.
[ANA-CRY]	Rapport de cotation des mécanismes cryptographiques – Stormshield, OPPIDA/CESTI/KIBO/CRYPTO/1.0, 6 mars 2015.
[EXP-CRY]	Expertise de l'implémentation des mécanismes cryptographiques, OPPIDA/CESTI/KIBO/Expertise_Crypto/2.0, 22 mars 2017.
[CONF]	Liste des sources de la version V7.2 patch-6 build 29579, KIBO/DEV/ListeFichiersSource, SES V7.2 patch-6.
[GUIDE]	Stormshield Endpoint Security, Guide d'administration, ses-fr-guide_d_administration-v7.2, mars 2017.
[PP-CDISK]	Profil de protection "Application de chiffrement de données à la volée sur mémoire de masse", réf PP-CDISK-CCv3.1, version 1.4, août 2008. *Certifié le 1 octobre 2008 sous la référence DCSSI-PP-2008/04.*

Annexe 3. Références liées 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.	
[CER/P/01]	Procédure ANSSI-CC-CER-P-01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; - Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; - Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, mai 2000.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[REF]	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.