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-2020/44

TSCAP

Référence cpe:/a:sopra_steria_group:tscap, version 1.1.0.115

Paris, le 23 décembre 2020

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 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-CSPN-2020/44**
Nom du produit **TSCAP**
Référence/version du produit **Référence cpe:/a:sopra_steria_group:tscap, version 1.1.0.115**
Catégorie de produit **Administration et supervision de la sécurité**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **SOPRA STERIA** Parc de la Conterie 2 12 rue Léo Lagrange CS 30611 35131 Chartres de Bretagne
Développeur **SOPRA STERIA** Parc de la Conterie 2 12 rue Léo Lagrange CS 30611 35131 Chartres de Bretagne
Centre d'évaluation **SYNACKTIV** 5 boulevard Montmartre 75002 Paris, France
Fonctions de sécurité évaluées Chiffrement des communications réseau Signature du rapport produit par TSCAP avec la clé auditeur Vérification de la signature du contenu SCAP passé en entrée - Vérification des entrées XML malformées
Fonctions de sécurité non évaluées Sans objet
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 7
1.2.1 Catégorie du produit 7
1.2.2 Identification du produit 8
1.2.3 Fonctions de sécurité 8
1.2.4 Configuration évaluée 8
2 L'évaluation 9
2.1 Référentiels d'évaluation 9
2.2 Charge de travail prévue et durée de l'évaluation 9
2.3 Travaux d'évaluation 9
2.3.1 Installation du produit 9
2.3.2 Analyse de la documentation 9
2.3.3 Revue du code source (facultative) 9
2.3.4 Analyse de la conformité des fonctions de sécurité 10
2.3.5 Analyse de la résistance des mécanismes des fonctions de sécurité 10
2.3.6 Analyse des vulnérabilités (conception, construction, etc.) 10
2.3.7 Analyse de la facilité d'emploi 10
2.4 Analyse de la résistance des mécanismes cryptographiques 10
2.5 Analyse du générateur d'aléas 11
3 La certification 12
3.1 Conclusion 12
3.2 Recommandations et restrictions d'usage 12
ANNEXE A. Références documentaires du produit évalué 13
ANNEXE B. Références à la certification 14

1 Le produit

1.1 Présentation du produit

Le produit évalué est « TSCAP, Référence cpe:/a:sopra_steria_group:tscap, version 1.1.0.115 » développé par SOPRA STERIA.

Ce produit est un outil permettant, à partir d'entrées SCAP (*Security Content Automation Protocol*), d'auditer des systèmes et de produire des rapports aux formats XML et HTML. Ces rapports donnent un état de conformité du système audité à la politique de sécurité en vigueur.

Les résultats SCAP sont issus d'un calcul entre le résultat attendu de l'état du système, défini par l'auditeur, et l'état réel du système, donné par le système via des sondes de collecte. L'environnement d'utilisation du produit est illustré dans la figure ci-dessous.

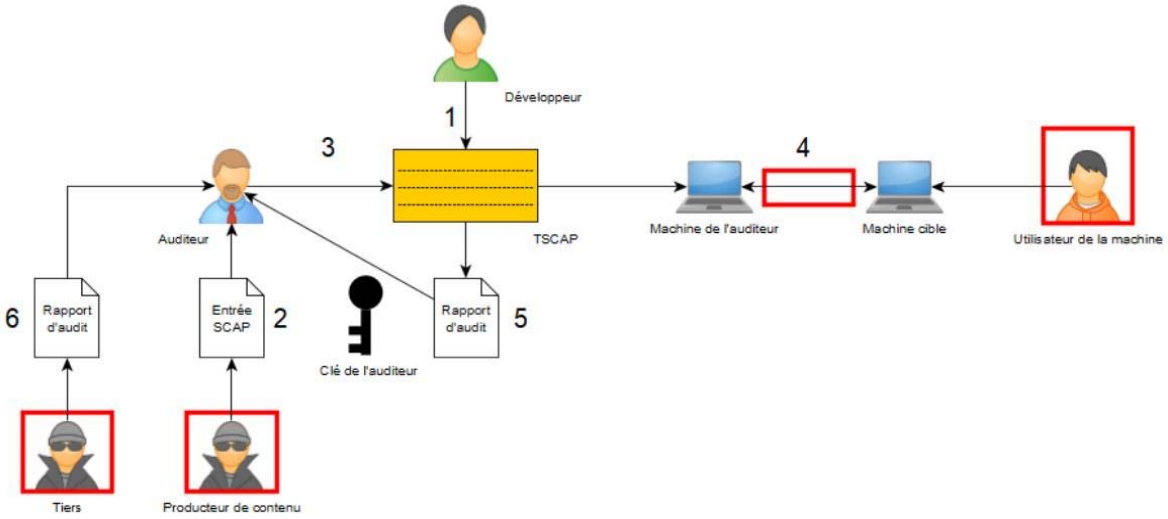

Figure 1 – Environnement de fonctionnement du produit.

La figure ci-dessous explicite l'architecture du produit.

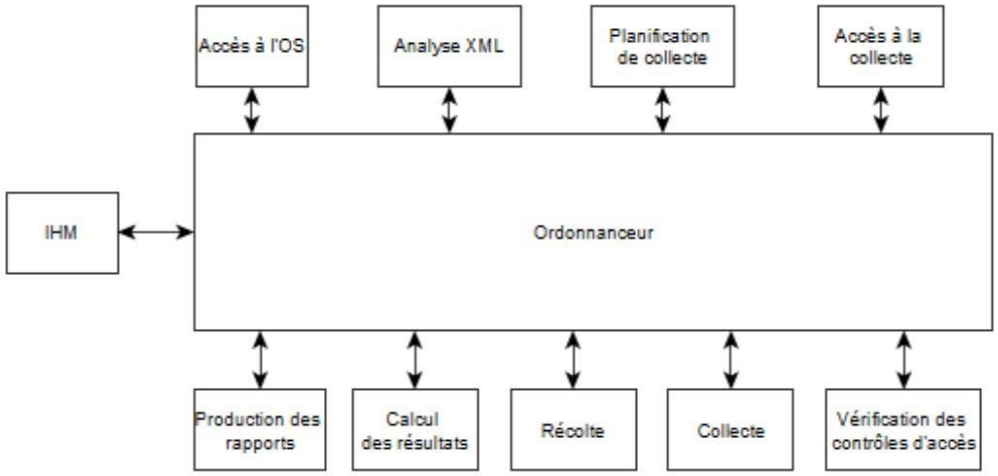

Figure 2 - Architecture Produit.

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*

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

1.2.2 *Identification du produit*

Produit	
Nom du produit	TSCAP
Numéro de la version évaluée	Référence cpe:/a:sopra_steria_group:tscap, version 1.1.0.115

La version certifiée du produit peut être identifiée de plusieurs manières :
- lancement de l'exécutable avec l'option appropriée : .\TSCAP.exe .\tscap_keys.txt – version ;
- affichage des propriétés WINDOWS du binaire.

Le fichier ChangeLog.pdf spécifie le *hash* SHA-256 du fichier tscap_keys.txt, permettant de vérifier l'intégrité de la version fournie. Ce fichier contient l'ensemble des *hash* de l'ensemble des exécutables et dépendances de TSCAP. L'utilisateur peut donc effectivement identifier la version de TSCAP, en vérifiant l'intégrité de ce fichier.

Enfin, la version est affichée dans la balise oval :product_version des rapports XML émis par le produit.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :
- chiffrement des communications réseau ;
- signature du rapport produit par TSCAP avec la clé auditeur ;
- vérification de la signature du contenu SCAP passé en entrée ;
- Vérification des entrées XML malformées.

1.2.4 *Configuration évaluée*

La configuration évaluée est composée de deux machines WINDOWS 10, correspondant à la machine auditée et à la machine de l'auditeur, sur laquelle TCSAP est installé. Les installations de WINDOWS sur ces ordinateurs ne sont pas reliées à un domaine *Active Directory*, cas d'usage possible du produit mais non considéré pour la TOE. Le certificat DISCO.pem a été ajouté au magasin de certificats de chaque poste pour permettre la signature de documents et la communication via WinRM. Les deux postes sont placés sur le même réseau Ethernet par l'intermédiaire d'un *switch*.

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.

TSCAP est portable : l'installation du produit à proprement parler correspond à la copie du programme et de ses dépendances dans un dossier sur le système de fichiers. Il n'existe pas d'étape de configuration du produit suite à son installation.

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

Sans objet.

2.3.1.3 Durée de l'installation

Sans objet.

2.3.1.4 Notes et remarques diverses

Sans objet.

2.3.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit [GUIDES] 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 manuellement le code source des parties du produit en lien avec ses fonctions de sécurité. Bien que cette revue ne soit pas exhaustive, l'évaluateur a constaté un respect global des

bonnes pratiques de développement dans le langage C++, ainsi qu'un niveau de documentation du code approprié.

La revue du code 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 inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

2.3.7 *Analyse de la facilité d'emploi*

2.3.7.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.7.2 Avis d'expert sur la facilité d'emploi

Le CESTI signale que certains contenus SCAP, s'ils sont fournis dans une archive ZIP, ne sont pas correctement interprétés, de sorte que la vérification de leur intégrité échoue. Cela ne cause pas de problème de sécurité particulier et s'apparente plustôt à un *bug* fonctionnel dans la mesure où ces contenus seront correctement interprétés si fournis par un autre moyen.

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

Le produit s'appuie sur les mécanismes cryptographiques du système d'exploitation sous-jacent (WINDOWS). La documentation de ces fonctions n'est pas complète et leur code source n'est pas disponible – il n'est donc pas possible d'en faire une analyse complète au sens de la méthodologie CSPN.

2.5 Analyse du générateur d'aléas

Le produit s'appuie sur un générateur aléatoire du système d'exploitation sous-jacent (WINDOWS). La documentation de cette fonction n'est pas complète et son code source n'est pas disponible – il n'est donc pas possible d'en faire une analyse complète au sens de la méthodologie CSPN.

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 « TSCAP, version Référence cpe:/a:sopra_steria_group:tscap, version 1.1.0.115 » 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.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], en particulier du respect des conditions de déploiement prévues dans la cible de sécurité [CDS]. Les utilisateurs doivent se conformer aux [GUIDES] fournis.

ANNEXE A. Références documentaires du produit évalué

[CDS]	*Cible de sécurité DISCO* Référence : DISCO_cible de sécurité ; Version : 1.05 ; Date : 23 octobre 2020.
[RTE]	Rapport d'audit sécurité CSPN DISCO Référence : 010.3/SYNACKTIV/DR ; Version : 2.0 ; Date : 27 novembre 2020.
[GUIDES]	DISCO Manuel utilisateur Référence : sans ; Version : 1.0 ; Date : 20 octobre 2020.

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]	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. 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. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. Documents disponibles sur www.ssi.gouv.fr.