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-2021/07

Solution d'authentification utilisateur pour RTOS

Version 207.6

Paris, le 9 avril 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2021/07

Nom du produit

Solution d'authentification utilisateur pour RTOS

Référence/version du produit

Version 207.6

Catégorie de produit

Identification, authentification et contrôle d'accès

Critère d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

HUAWEI TECHNOLOGIES FRANCE
18 quai du Point du Jour
92100 Boulogne-Billancourt, France

Développeurs

HUAWEI TECHNOLOGIES FRANCE
18 quai du Point du Jour
92100 Boulogne-Billancourt, France

HUAWEI CENTRAL SOFTWARE
Building Q27, No. 156 Beiqing Rd.
Shi-Chuang-Ke-Ji-Shi-Fan-Yuan, Hai-Dian District
Beijing 100095, P. R. China

Centre d'évaluation

THALES / CNES
290, allée du Lac
31670 Labège, France

Fonctions de sécurité évaluées

Identification et authentification de l'utilisateur
Canal de communication de confiance
Séparation des utilisateurs et des données de configuration

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

1.1 Présentation du produit

Le produit évalué est la « Solution d'authentification utilisateur pour RTOS, Version 207.6 » développée par HUAWEI TECHNOLOGIES FRANCE.

Il peut fournir des services à plusieurs utilisateurs, locaux ou distants, en même temps. Après une connexion réussie, les utilisateurs ont accès à un environnement générique leur permettant de lancer des applications utilisateur, d'exécuter des commandes utilisateur au niveau du *shell*, de créer et d'accéder à des fichiers. Il fournit des mécanismes adéquats pour séparer les utilisateurs et protéger leurs données. En outre, les commandes privilégiées sont réservées aux utilisateurs administrateurs.

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	Solution d'authentification utilisateur pour RTOS
Numéro de la version évaluée	Version 207.6

La version certifiée du produit peut être identifiée en tapant sur un terminal la commande `cat /etc/RTOS-Release`.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'identification et l'authentification de l'utilisateur ;
- le canal de communication de confiance ;
- la séparation des utilisateurs et des données de configuration.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond au système d'exploitation RTOS fonctionnant sur une carte de dispositif matériel Hi1213 SoC de HISILICON.

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

Pour procéder à l'installation du produit, l'évaluateur a suivi le guide d'installation [GUIDES]. Il a estimé que ce guide est bien documenté et contient de nombreuses captures d'écran décrivant étape par étape toutes les opérations à effectuer lors de la première installation du produit.

2.3.1.3 Durée de l'installation

L'installation dure quelques heures.

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 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'intégralité du produit. L'analyse a été effectuée manuellement.

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

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré dans le contexte défini par la cible de sécurité [CDS].

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

Il n'a pas été découvert de vulnérabilité propre au produit qui puisse remettre en cause la sécurité du produit.

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

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

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 a identifié des non-conformités au RGS (voir [RGS]) mais ces dernières n'engendrent pas de vulnérabilités exploitables pour le niveau d'attaquant visé.

2.5 Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé. Il en ressort que pour la génération d'aléa le produit utilise le DRNG de la librairie OpenSSL.

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 « Solution d'authentification utilisateur pour RTOS, Version 207.6 » 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 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]	*Huawei user authentication solution "RTOS"* Référence : HRTOS_ST_1.3 ; Version : 1.3 ; Date : 2 février 2021.
[RTE]	*CSPN Evaluation Technical Report Project: Tulip CSPN* Version : 1.1 ; Date : 23 février 2021. *Analysis of Cryptographic Mechanisms Project: Tulip CSPN* Version : 1.0 ; Date : 21 décembre 2020.
[GUIDES]	*Huawei RTOS 207 Installation Guide* Version : 0.1 ; Date : 11 août 2020. *Huawei RTOS 207.6 User Guide* Version : 1.1 Révision ; Date : 23 février 2021. *Huawei RTOS 207 Hardware Installation Document* Version : 0.1 ; Date : 27 juillet 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.
[RGS]	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.