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-2020/42

Huawei AR Series Service Router

Référence AR6120, Version V300R019C00SPC007T

Paris, le 15 décembre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti 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-CSPN-2020/42**
Nom du produit **Huawei AR Series Service Router**
Référence/version du produit **Référence AR6120, Version V300R019C00SPC007T**
Catégorie de produit **Communication sécurisée**
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
Développeur **HUAWEI TECHNOLOGIES CO., Ltd.** Administration Building, Huawei Base, Bantian Longgang District, Shenzhen 518129, China
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées Listes de contrôle d'accès Authentification de l'utilisateur Contrôle d'accès Audit Sécurité des communications
Fonctions de sécurité non évaluées Néant
Restriction(s) d'usage Oui (cf. §3.2)

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 « Huawei AR Series Service Router, Référence AR6120, Version V300R019C00SPC007T » développé par HUAWEI TECHNOLOGIES CO., Ltd.

Les routeurs « Huawei AR Series Routers » sont des équipements réseau informatique assurant le routage des paquets. Au cœur du routeur se trouve le logiciel VRP (*Versatile Routing Platform*) déployé sur MPU (*Main Processing Unit*), le logiciel de gestion et d'exécution de la fonctionnalité de mise en réseau du routeur. Il offre également des fonctionnalités de sécurité étendues. Pour des raison de performance, VRP est supporté par la *Concurrence Accelerate Platform* (CAP).

Le routeur AR6120 gère les trafics L2 et L3. Tout le trafic L3 qui passe par le MPU, passe d'abord par le logiciel CAP.

L'architecture matériel du routeur AR6120 contient les éléments suivants :
- un processeur Hisilicon1213 ;
- une mémoire de 512MB ;
- deux types différents de stockage flash : 2MB de stockage pour le bootrom et 512MB de stockage pour les paquets logiciels ;
- deux fentes SIC ;
- une interface 8FE+2GE ;
- *Forwarding Performance* : 450K PPS.

L'architecture logiciel se compose du logiciel VRP, du logiciel CAP et du système d'exploitation sous-jacent.

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	Huawei AR Series Service Router
Numéro de la version évaluée	Référence AR6120, Version V300R019C00SPC007T

La version certifiée du produit peut être identifiée de la manière suivante :

- la référence du routeur est indiquée sur le boîtier ;
- la version du *firmware* est récupérée par l'utilisateur en utilisant la commande « *display version* » sur un terminal après avoir été authentifié via ssh au moins comme utilisateur niveau 1.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- les listes de contrôle d'accès : pour empêcher le trafic du réseau indésirable, le produit utilise des listes de contrôle d'accès pour filtrer le trafic destiné à la TOE et pour empêcher la surcharge de trafic interne et l'interruption de service ;
- l'authentification de l'utilisateur : pour pouvoir exécuter des commandes l'utilisateur doit s'authentifier en utilisant un identifiant et un mot de passe ;
- le contrôle d'accès : pour empêcher tout accès non autorisé, le produit gère les privilèges des utilisateurs par niveau d'accès ;
- l'audit : la TOE journalise tout type d'évènement lié à la sécurité et le traite en fonction de la configuration de l'utilisateur ;
- la sécurisation des communications : la TOE renforce la sécurité des communications en utilisant le protocole SSH2.0.

1.2.4 *Configuration évaluée*

La configuration évaluée, qui constitue également la plateforme de test, correspond à un routeur « Huawei AR Series Service Router » sur lequel l'évaluateur a appliqué les configurations décrites dans les guides d'administration et d'utilisation [GUIDES].

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

Le produit est livré fonctionnel avec le *firmware* préinstallé. L'utilisateur final devra le connecter sur un port *Ethernet*, s'authentifier comme administrateur et configurer les interfaces réseaux.

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 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. 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

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.

2.3.7 *Analyse de la facilité d'emploi*

2.3.7.1 Cas où la sécurité est remise en cause

Les risques identifiés lors de l'évaluation entraînent des restrictions d'usage pour l'utilisateur (voir chapitre 3.2).

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 celles-ci 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 du TRNG, la TOE utilise la puce Hisilicon1213 développée par HUAWEI, hors du périmètre de l'évaluation (voir [RTE]).

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 « Huawei AR Series Service Router, Référence AR6120, Version V300R019C00SPC007T » 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], et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations et restrictions suivantes :

- suivre les recommandations du guide « *Security Hardening And Maintenance Guide* » [GUIDES] ;
- utiliser la configuration obligatoire pour les privilèges utilisateur décrite dans « *Security Hardening And Maintenance Guide* » [GUIDES], section 1.4.7.

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 AR6120 Router – CSPN Security Target* Version : 1.8 ; Date : 10 août 2020.
[RTE]	*CSPN Evaluation Technical report – EIRENE2 - Huawei AR6120* Référence : OPPIDA/CESTI/EIRENE2/RTE/1.1 ; Version : 1.1 ; Date : 14 octobre 2020.
[GUIDES]	*Security Hardening And Maintenance Guide* Version : 1.0 ; Date : 26 juillet 2020. *Test Guide* Référence : *AR6120V V300R019C00SPC007T Test Guide.* *Configuration Guide* Référence : *AR6100 Series Configuration.*

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.