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-CSPN-2020/28

RSPE
Version HiOS 07.0.07

Paris, le 30 juillet 2020

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-CSPN-2020/28

Nom du produit

RSPE

Référence/version du produit

Référence 942084999, Version HiOS 07.0.07

Catégorie de produit

Communication sécurisée

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

Hirschmann Automation and Control GmbH
Stuttgarter Strasse 45 – 51
72654 Neckartenzlingen
Deutschland

Développeur

Hirschmann Automation and Control GmbH
Stuttgarter Strasse 45 – 51
72654 Neckartenzlingen
Deutschland

Centre d'évaluation

Oppida

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

Fonctions de sécurité évaluées

Communication sécurisée
Gestion des accès restreints
Gestion des entrées malformées
Politique de séparation du réseau
Stockage sécurisé des secrets

Fonction(s) de sécurité non évaluées

Néant

Restriction(s) d'usage

Oui (cf. §3.2)

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 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 matières

1. LE PRODUIT 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT EVALUE 7
1.2.1. Catégorie du produit 7
1.2.2. Identification du produit 7
1.2.3. Fonctions de sécurité 7
1.2.4. Configuration évaluée 7

2. L'EVALUATION 8

2.1. REFERENTIELS D'EVALUATION 8
2.2. CHARGE DE TRAVAIL PREVUE ET DUREE DE L'EVALUATION 8
2.3. TRAVAUX D'EVALUATION 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. Accès aux développeurs 9
2.3.8. Analyse de la facilité d'emploi 9
2.4. ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES 9
2.5. ANALYSE DU GENERATEUR D'ALEAS 10

3. LA CERTIFICATION 11

3.1. CONCLUSION 11
3.2. RECOMMANDATIONS ET RESTRICTIONS D'USAGE 11

ANNEXE 1. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 12

ANNEXE 2. REFERENCES A LA CERTIFICATION 13

1. Le produit

1.1. Présentation du produit

Le produit évalué est le « RSPE, version HiOS 07.0.07 » développé par *HIRSCHMANN AUTOMATION AND CONTROL GMBH*.

Le produit RSPE est un commutateur Ethernet industriel. Il a été spécialement conçu pour les réseaux industriels et les environnements difficiles où les commutateurs normaux ne peuvent pas fonctionner correctement en raison de la chaleur, de l'humidité ou de la poussière. Il permet l'interconnexion de différents périphériques ou segments de réseau. Il prend en charge la séparation logique de réseau avec VLAN, ainsi que plusieurs fonctionnalités de sécurité orientées réseau (prévention des dénis de service, filtrage MAC, détection du *spoofing* ARP, etc.).

La figure ci-dessous présente le produit.

Figure 1 – Présentation du 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

Nom du produit	RSPE
Numéro de la version évaluée	HiOS 07.0.07

La version certifiée du produit peut être identifiée dans le menu « *Software* » de l'interface web.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- Communication sécurisée ;
- Gestion des accès restreints ;
- Gestion des entrées malformées ;
- Politique de séparation du réseau ;
- Stockage sécurisé des secrets.

1.2.4. Configuration évaluée

La configuration évaluée, qui constitue également la plateforme de test, correspond à un commutateur Ethernet industriel RSPE 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 2.

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'évaluateur n'a procédé à aucune installation du produit. Le commanditaire a fourni une TOE préinstallée et prête à l'emploi, et a procédé à la mise en route du produit au côté de l'évaluateur.

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'utiliser le produit sans causer de dégradation accidentelle de la sécurité. En particulier, le *Security Configuration Guide for HiOS switches* regroupe les étapes nécessaires pour que la configuration du produit soit conforme aux bonnes pratiques de sécurité.

2.3.3. Revue du code source (facultative)

L'évaluation n'a pas fait l'objet d'une revue de code source.

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 les briques logicielles tierces du produit, mais se sont révélées inexploitables 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

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

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi

2.3.8.1. 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).

2.3.8.2. Avis d'expert sur la facilité d'emploi

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

2.3.8.3. 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][RTE]). Celle-ci a identifié des non-conformités au RGS (voir RGS[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 fait l’objet d’une analyse. Celle-ci a identifié des non-conformités au RGS (voir RGS[RGS]) et des faiblesses qui n'engendrent pas de vulnérabilités exploitables pour le niveau d'attaquant 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.

Ce certificat atteste que le produit « RSPE, version HiOS 07.0.07 » 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.

Afin de garantir l'utilisation sécurisée du produit, il est impératif que l'utilisateur suive toutes les recommandations du *Security Configuration Guide for HiOS switches* [GUIDES]. Notamment, l'utilisateur doit mette en œuvre les mesures suivantes :

- Suivre les recommandations du guide concernant la politique et le renouvellement de mots de passe ;
- Désactiver l'option *System Monitor* ;
- Désactiver le *service shell* via *CLI* ;
- Désactiver le service *HiDiscovery*.

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

Annexe 1. Références documentaires du produit évalué

[CDS]	*RSPE CSPN Security Target* Référence : Security Target-BELDEN ; Version : *1.3* ; Date : *28 mai 2020.*
[RTE]	*Rapport Technique d'Evaluation CSPN - RSPE* Référence : OPPIDA/CESTI/RSPE2/RTE/1.2 ; Version : 1.2 ; Date : *27 mai 2020.*
[GUIDES]	*Guides d'utilisation et d'administration* Référence : ManualCollection_RSPE_HiOS-3S-07000_en ; Référence : IG_RSPM2022_10_0415_en ; Référence : IG_RSPE30323537_10_0415_en ; *Security Configuration Guide for HiOS switches : Minimum security features to secure your netword infrastructure* Référence : Minimum Security Recommendations HiOS-BELDEN ; Version : 1.0 ; Date : *23 janvier 2020.*

Annexe 2. 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.