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-2019/08

OpenVPN

Version 2.4.6, utilisé conjointement avec OpenSSL version 1.1.0h

Paris, le 25 juillet 2019

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-2019/08

Nom du produit

OpenVPN

Référence/version du produit

Version 2.4.6

Utilisé conjointement avec OpenSSL 1.1.0h

Catégorie de produit

Communication sécurisée

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

Agence Nationale de la Sécurité des Systèmes d'Information

51 boulevard de La Tour Maubourg

75700 Paris, France

Développeur

OpenVPN Technologies

www.openvpn.net

Centre d'évaluation

Quarkslab

71 avenue des Ternes

75017 Paris, France

Fonctions de sécurité évaluées

Fonction de VPN

Mécanismes d'authentification

Fonctions d'administration

Journalisation locale d'événements

Fonction(s) de sécurité non évaluées

Sans objet

Restriction(s) d'usage

Non

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 CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le « *OPENVPN*, version 2.4.6, utilisé conjointement avec OpenSSL version 1.1.0h » développé par *OPENVPN TECHNOLOGIES*.

Ce produit est une passerelle de réseau privé virtuel (*Virtual Private Network – VPN*) logicielle libre sous licence publique générale GNU (*General Public Licence – GPL*). Il permet d'établir des connexions point à point ou site à site selon des configurations de type route (explicite) ou pont (transparent) en utilisant un protocole qui lui est propre et qui repose largement sur *OPENSSL*.

OPENVPN est disponible sous tous les environnements *nix mais aussi sous *MAC OS X*, *WINDOWS* (2000, *XP*, *VISTA*, 7, 8 et 10), *ANDROID* et *iOS*.

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	OpenVPN
Numéro de la version évaluée	2.4.6
Version d'*OpenSSL* utilisée pour l'évaluation	1.1.0h

Le produit a été testé sur 3 environnements : une distribution *UBUNTU* 18.04, une distribution *DEBIAN* 10 *testing*, ainsi qu'un environnement *WINDOWS* 10.

La version certifiée du produit peut être identifiée en tapant les commandes suivantes :
- Sous *LINUX* : `> openvpn –version`
- Sous *WINDOWS* : `C:\> openvpn.exe –version`.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :
- la fonction de *VPN* : le produit permet d'établir des tunnels *VPN* entre un poste client distant et une passerelle Internet distante ou un réseau privé dans le but d'apporter confidentialité et intégrité du trafic utilisateur au travers d'un réseau non maîtrisé ;
- les mécanismes d'authentification : lors de l'établissement de la fonction de *VPN*, le produit offre la possibilité de configurer différents moyen d'authentification entre serveur et client ;
- les fonctions d'administration : le produit dispose des fonctions permettant de configurer l'ensemble des différentes fonctionnalités ;
- la journalisation locale d'événements : le produit permet de définir une politique de journalisation locale d'événements (au niveau du serveur et au niveau du client) notamment ceux liés à sa sécurité et à son administration.

1.2.4. Configuration évaluée

La configuration évaluée correspond à :

- un serveur *OPENVPN* sous *LINUX* (*DEBIAN* 10 *testing* et *UBUNTU* 18.04), installé depuis les sources disponibles sur le site officiel, en version 2.4.6 ;
- un client *OPENVPN* sous *LINUX* (*DEBIAN* 10 *testing* et *UBUNTU* 18.04), installé à partir du même exécutable utilisé pour le serveur ;
- un client *OPENVPN* sous *WINDOWS* 10 x64, installé depuis l'installateur disponible sur le site officiel, en version 2.4.6

Dans le cadre de l'évaluation, la version d'*OPENSSL* considérée est la 1.1.0h.

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

Sous *LINUX*, le client et le serveur *OPENVPN* partagent la même procédure d'installation, tout en ayant des fichiers de configuration spécifiques.

Pour la distribution *DEBIAN* 10 *testing*, l'installation a été effectuée en utilisant le package *OPENVPN* 2.4.6 et le package *OPENSSL* en version 1.1.0h comme précisé dans la [CDS]. Les commandes utilisées pour l'installation sont les suivantes :

```
dpkg –i openssl_1. 1.0h-4_amd64.deb
dpkg -i libssl1.1_1.1.0h-4_amd64.deb
dpkg -i libssl-dev_1.1.0h-4_amd64.deb
apt install openvpn.
```

La distribution *UBUNTU* 18.04 ne propose pas un package à jour de la version 2.4.6 d'*OPENVPN* mais il est possible d'en construire un à partir des sources du package *OPENVPN* disponibles pour la distribution *DEBIAN Unstable*. Pour cela, *UBUNTU* nécessite les dépendances suivantes : `libssl-dev`, `liblz4-dev`, `liblzo2-dev` et `libpam0g-dev`. Ensuite, il faut récupérer les fichiers `openvpn_2.4.6.orig.tar.xz`, `openvpn_2.4.6-1.debian.tar.xz` et `openvpn_2.4.6-1.dsc` disponibles depuis la page web d'*OPENVPN*. Une fois ces fichiers décompressés dans les bons répertoires, afin de respecter la structure des sources d'un package *DEBIAN*, la construction du package est réalisée avec la commande : `dpkg-buildpackage -uc –us`. Finalement l'installation du package est effectuée au niveau du système : `dpkg -i openvpn_2.4.6-1_amd64.deb.`

Sous *WINDOWS* 10, le client *OPENVPN* est installé depuis l'installateur en version *I602* disponible sur le site officiel. La version de la librairie *OPENSSL* associée à cette installation est `1.1.0h figure-openssl_version_windows`.

Les options de configuration minimale (serveur et client) retenues ainsi que les options proscrites sont détaillées dans la [CDS] (voir section 8).

2.3.1.3. Durée de l'installation

L'installation du produit est immédiate.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

La documentation du produit *OPENVPN* ne concerne que son intégration par des développeurs/administrateurs. Elle est principalement disponible dans le wiki officiel du projet [GUIDES]. Elle est jugée trop succincte par l'évaluateur (voir chapitre 2.3.8.2).

Le code source du produit est documenté selon les conventions de l'outil *DOXYGEN*. Cependant, le protocole et le fonctionnement d'*OPENVPN* ne sont pas détaillés pour le moment. Il manque une documentation à l'intention des développeurs/administrateurs présentant le fonctionnement du produit et l'organisation du code source.

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.

L'évaluateur estime que les développeurs du projet ont suivi de bonnes pratiques de sécurité. Par contre, le code source manque de lisibilité et sa compréhension est difficile.

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 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.

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

La sécurité du produit est remise en cause si les développeurs/administrateurs ne se conforment pas aux guides fournis, ne protègent pas les fichiers de clés privées contre des accès non autorisés et si les configurations proposées par la cible de sécurité [CDS] ne sont pas respectées.

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

L'évaluateur a jugé que les différentes étapes qui amènent à l'exécution correcte d'un serveur et d'un client *OPENVPN* ne sont pas suffisamment bien décrites dans la documentation du produit.

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]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé et son analyse n'a pas identifié de vulnérabilité exploitable.

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 « *OPENVPN*, version 2.4.6, utilisé conjointement avec OpenSSL version 1.1.0h » 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]. Les conditions de déploiement prévues dans la cible de sécurité [CDS] (section 8) doivent être respectées, les utilisateurs doivent se conformer aux [GUIDES] fournis et les fichiers de clés privées doivent être protégés contre des accès non autorisés.

Aucune recommandation particulière n'est formulée par l'évaluateur.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN OpenVPN 2.4.6* Référence : 18-02-403-LIV ; Version : *1.3* ; Date : *03 août 2019.*
[RTE]	*Évaluation CSPN - OpenVPN* Référence : 18-08-458-REP ; Version : 1.2 ; Date : *05 juillet 2019.*
[GUIDES]	*https://openvpn.net/community-resources/how-to/* *https://community.openvpn.net/openvpn* *https://openvpn.net/community-resources/#documentation*

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-01/2.0 du 6 septembre 2018. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 19 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.