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-24

Prove-IT
Version 4.0-4

Paris, le 24 décembre 2018

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-2018/24**
Nom du produit **Prove-IT**
Référence/version du produit **Version 4.0-4**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **RUBYCAT-Labs** **1137 Avenue des Champs Blancs** **35510 Cesson-Sévigné**
Développeur **RUBYCAT-Labs** **1137 Avenue des Champs Blancs** **35510 Cesson-Sévigné**
Centre d'évaluation **Amossys** **11 rue Maurice Fabre** **35000 Rennes, France**
Fonctions de sécurité évaluées **Communications sécurisées** **Authentification** **Contrôle d'accès** **Traçabilité**
Fonction(s) de sécurité non évaluées **Néant**
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 « Prove-IT, version 4.0-4 », développé par *RUBYCAT-LABS*.

Prove-IT est une *appliance* logicielle qui vise à renforcer le contrôle des accès à un système d'information, ainsi qu'à apporter une traçabilité des accès en proposant des pistes d'audit.

Le produit se positionne en coupure des accès internes et externes du SI. Il se place sur le réseau interne pour assurer sa fonction de portail d'accès centralisé aux ressources. La solution ne nécessite pas l'installation d'agents sur les serveurs cibles ni sur les clients.

Le produit s'articule autour de différents modules ci-dessous :

- gestion accès SSH utilisateurs avec les sous-modules intégrés :
  - contrôle d'accès,
  - traçabilité,
  - filtrage ;
- gestion accès RDP utilisateurs avec les sous-modules intégrés :
  - contrôle d'accès,
  - traçabilité,
  - filtrage ;
- administration et audit ;
- accès administration maintenance ;
- gestion identités secondaires ;
- gestion base de données et stockage.

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

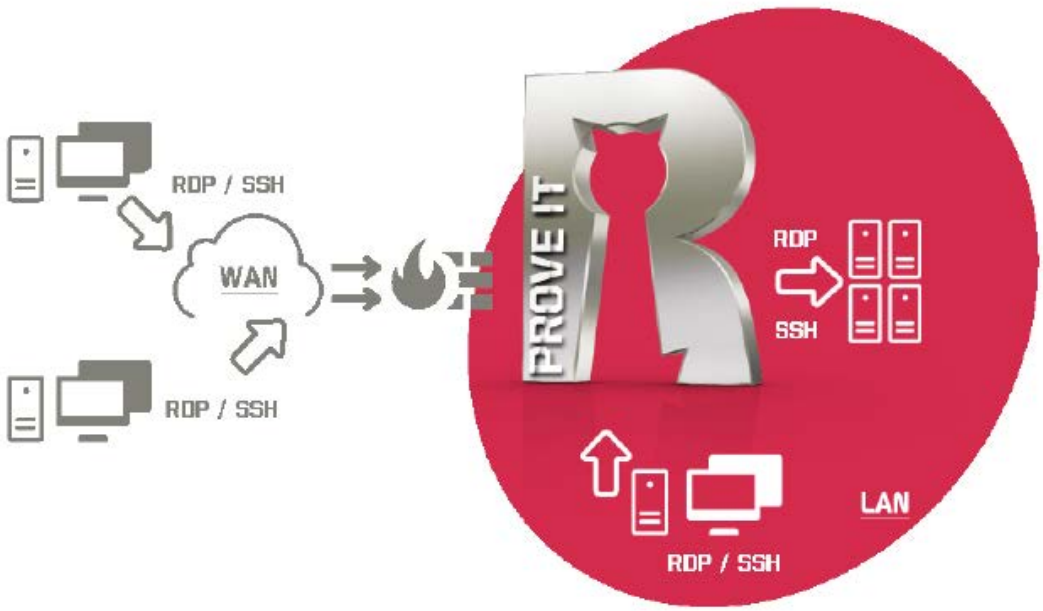

Figure 1 - Architecture Produit.

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

Nom du produit	Prove-IT
Numéro de la version évaluée	4.0-4

La version certifiée du produit peut être identifiée de deux manières :

- depuis la ligne de commande du serveur *ProveIT* (# dpkg –l | grep proveit) ;
- depuis le menu « Système > Informations > Informations » de l'interface web d'administration du produit.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- les communications sécurisées ;
- l'authentification ;
- le contrôle d'accès ;
- la traçabilité.

1.2.4. Configuration évaluée

La configuration évaluée contient :

- les modules de contrôle d'accès et de traçabilité des flux utilisateurs uniquement sur le protocole RDP ;
- le module administration et audit (via l'interface web).

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

Le produit est livré sous la forme d'une image ISO qui peut être déployée sur un environnement virtualisé *ESXi*.
Pour l'installation, l'utilisateur doit suivre la procédure d'installation [GUIDES] fournie par le développeur. Le prérequis de la configuration de la machine virtuelle est défini dans [REQUIREMENTS], également fournis par le développeur.
L'installation du système ne propose à l'administrateur que des choix de configuration personnelle (langue du système, clavier, etc.) qui n'impactent pas la sécurité du produit.

2.3.1.3. Durée de l'installation

L'installation du produit et sa première configuration durent à peu près une heure.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

La documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit. En outre, les choix de configuration par défaut du produit sont sûrs et robustes, afin d'assurer un bon niveau de sécurité.

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue du code source et estime que le code est clairement organisé et que chaque interface est bien commentée.

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 dans le contexte d'utilisation prévu et pour le niveau d'attaquant considéré.

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. 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.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Aucune recommandation particulière n'est formulée par l'évaluateur. Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

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

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

2.3.8.4. 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. Celle-ci n'a pas identifié de vulnérabilité exploitable

2.5. Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé. Il en ressort que le produit utilise le générateur d'aléa du noyau *Linux* (/dev/urandom). Aucune vulnérabilité exploitable n'a été identifiée.

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 « Prove-IT, version 4.0-4 » 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. 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 énoncées dans le présent rapport (voir 2.3.8.2).

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN* Référence : CSPN-ST-PROVE IT-1.02 ; Version : *1.02* ; Date : *26 juillet 2018*
[RTE]	*Rapport Technique d'Evaluation CSPN* Référence : CSPN-RTE-ProveIT2-1.00 ; Version : 1.0 ; Date : *8 octobre 2018*
[ANA-CRY]	*Expertise des mécanismes cryptographiques* Référence : CSPN-CRY-ProveIT2-1.00 ; Version : 1.0 ; Date : *15 octobre 2018*
[SPEC-CRY]	*Spécifications de mécanismes cryptographiques de la solution PROVE IT version 4.0-4* Version : 1.03 ; Date : *1 août 2018*
[GUIDES]	Guide d'utilisation du produit : *Guide de l'utilisateur PROVE IT version 4.0-4* Guide d'administration du produit : *Guide d'administration PROVE-IT version 4.0-4* Guide d'installation du produit : *Guide d'installation PROVE IT version 4.0-4*
[REQUIREMENTS]	*Fiche de pré-requis PROVE IT*

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, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. 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.