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-2016/16

Nessus Manager
Version 6.7

Paris, le 23 novembre 2016

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-2016/16**
Nom du produit **Nessus Manager**
Référence/version du produit **Version 6.7**
Catégorie de produit **Administration et supervision de la sécurité**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Tenable Network Security** **7021 Columbia Gateway Dr. ,** **Suite 500,** **Columbia, MD 21046** **Etats-Unis d'Amérique**
Centre d'évaluation **Synacktiv** **5 rue Sextius Michel,** **75015 Paris,** **France**
Fonctions de sécurité évaluées **Protection des flux entre les utilisateurs et le manager** **Protection des flux entre le manager, les scanners et les agents** **Contrôle d'accès** **Authentification des utilisateurs** **Chiffrement des données** **Signature des mises à jour**
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 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 « *Nessus Manager*, version 6.7 » développé par *TENABLE NETWORK SECURITY*.

Nessus Manager est un composant logiciel d'infrastructure permettant la supervision de la sécurité d'un parc de machines.
Nessus Manager permet la configuration et le pilotage d'un ensemble de *Nessus Scanners* et de *Nessus Agents* ainsi que la gestion et l'agrégation des différentes informations qu'ils produisent.

Les *Nessus Scanner* sont des scanners réseau et de vulnérabilités pouvant communiquer avec un *Nessus Manager* sur un autre réseau ou sous-réseau.
Les *Nessus Agents* sont des programmes installés sur des machines, typiquement d'utilisateurs nomades. Ces *Nessus Agents* se connectent au *Nessus Manager* au démarrage du poste et permettent au *Nessus Manager* d'avoir une visibilité sur la configuration de la machine.

Nessus Manager permet de définir des rôles aux utilisateurs pour effectuer des tâches et gérer des groupes d'utilisateurs, des agents ou des scanners.

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

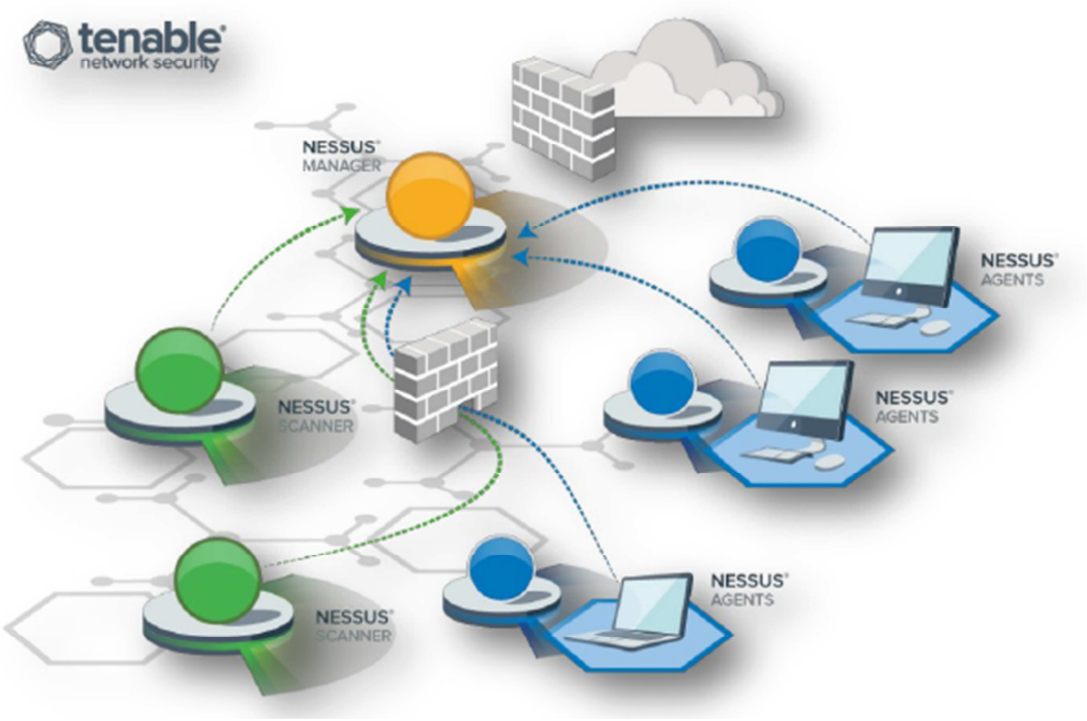

Figure 1 - Architecture de la solution.

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
☐ 14 – autre

1.2.2. Identification du produit

Nom du produit	Nessus Manager
Numéro de la version évaluée	6.7

La version certifiée du produit peut être identifiée à partir de l'interface Web de Nessus Manager, tel qu'illustré sur la Figure 2.

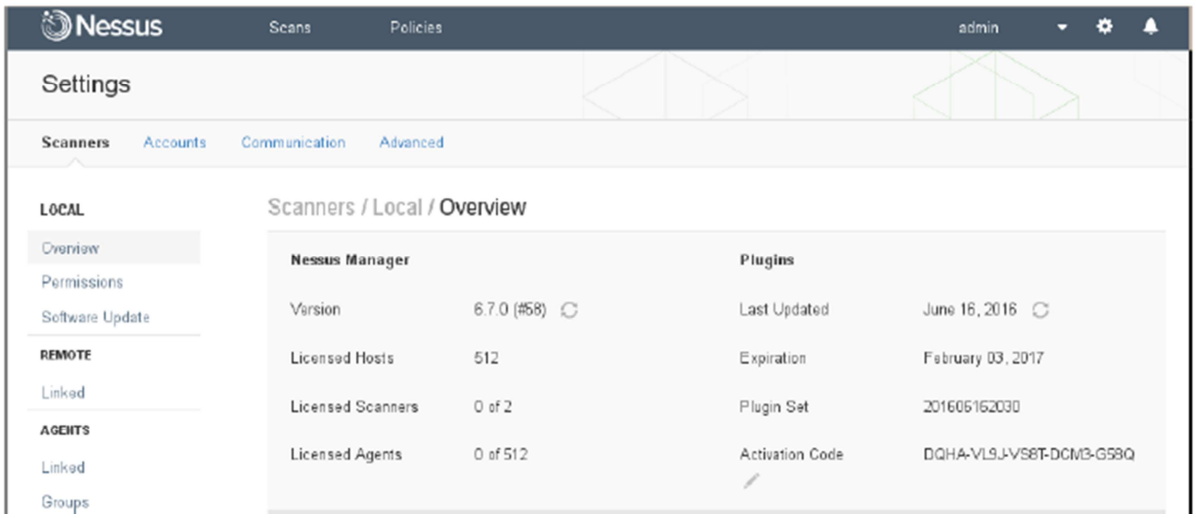

Figure 2 - Identification de la version

Cette version a été installée par l'évaluateur à partir du paquet Nessus-6.7.0-es6.x86_64.rpm. Après installation la version peut être affichée en lançant la commande suivante :

```
# /opt/nessus/sbin/nessusd -v
nessusd (Nessus) 6.7.0 [build M20058] for Linux
Copyright (C) 1998 - 2016 Tenable Network Security, Inc
```

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- la protection des flux entre les utilisateurs et le manager : l'ensemble des flux entre le manager et les utilisateurs sont protégés en intégrité, confidentialité et authenticité à l'aide du protocole TLS ;
- la protection des flux entre le manager et les scanners et les agents : l'ensemble des flux entre le manager et les scanners et les agents sont protégés en intégrité, confidentialité et authenticité à l'aide du protocole TLS 1.0 associé aux suites de chiffrement AES128-SHA et AES256-SHA. Le serveur est authentifié à l'aide de son certificat. Les scanners et agents sont authentifiés à l'aide d'un jeton d'authentification de 256 bits, propre à chaque scanner ou agent et envoyé dans les en-têtes des requêtes http ;
- le contrôle d'accès : *Nessus Manager* permet de contrôler l'accès à ses différentes fonctions au moyen de rôles alloués aux utilisateurs ;
- l'authentification des utilisateurs : *Nessus Manager* authentifie les utilisateurs à l'aide de leur mot de passe ou d'un certificat ;
- le chiffrement des données : l'ensemble des données manipulées par *Nessus Manager* (les politiques, les scans et les configurations) sont stockées ou exportées dans des bases de données SQLite, chiffrées à l'aide du module SQLite SEE paramétré de façon à utiliser l'algorithme AES-128 en mode OFB ;
- la signature des mises à jour : les mises à jour sont signées à l'aide de RSASSA PKCS#1 v1.5 et d'une clé RSA de 4096 bits. Seul le développeur a accès à la clé privée de ce bi-clé.

1.2.4. Configuration évaluée

Les configurations avancées du service *Nessusd* pour le *Nessus Manager* et *Nessus Scanner* ont été laissées par défaut.
Pour la gestion de *Nessus Manager* depuis l'interface web et les besoins de l'évaluation, quatre utilisateurs ont été créés avec les rôles suivants :

- administrateur système ayant les droits les plus privilégiés sur la solution ;
- administrateur ;
- utilisateur « standard » pouvant effectuer des scans ;
- basique ;
- pour le scanner *Nessus* deux utilisateurs avec les différents rôles suivant ont été créés :
    - administrateur ;
    - standard.

La plateforme de test est constituée :

- d'une machine virtuelle embarquant un système CentOS 6 provenant du dépôt officiel CentOS, avec un noyau Linux 2.6.32, hébergant *Nessus Manager* ;
- différentes machines virtuelles situées sur le même réseau que *Nessus Manager* sur lesquelles ont été installées un scanner et des agents.

Par défaut, CentOS est configuré avec un pare-feu *iptables* acceptant uniquement les connexions SSH sur le port TCP 22 et les messages ICMP. Une règle acceptant les connexions en entrée sur le port TCP 8834 pour l'interface Web a donc été ajoutée :

```
$ iptables -I INPUT 1 -m state --state NEW -m tcp -p tcp --dport 8834 -j ACCEPT
```

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, menaces, utilisateurs et 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 1.2.3.

2.3.1.2. Description de l'installation et des non-conformités éventuelles

L'installateur Nessus utilisé pour le manager est le paquet « Nessus-6.7.0-es6.x86_64.rpm ».

Nessus Manager supporte la définition d'une clé maîtresse utilisée pour chiffrer les politiques de scans et les données d'authentifications.
Conformément aux hypothèses de la cible, une clé maîtresse a été définie à l'aide de la commande suivante :

```
/opt/nessus/sbin/nessusd -K
```

Alternativement à l'authentification avec un identifiant et un mot de passe, *Nessus Manager* permet aux utilisateurs de se connecter avec un certificat.
Afin de tester cette fonctionnalité, un certificat client a été généré avec le programme *nessuscli.*

Pour passer d'un mode d'authentification à l'autre, la commande suivante a été utilisée :

```
# nessuscli fix --set force_pubkey_auth=yes/no
```

Un scanner *Nessus* a été installé sur une machine virtuelle dédiée. Tout comme *Nessus Manager*, l'interface Web du scanner est disponible sur le port TCP 8834.
Pour connecter le scanner au manager, le scanner a besoin d'une clé de management qu'il est possible d'obtenir et de renouveler dans l'interface Web. Cette clé est ensuite fournie au scanner en même temps que les informations de connexion.

L'agent *Nessus* est contenu dans un paquet d'installation différent du scanner et du *Nessus Manager*. Le paquet utilisé pour son installation est Nessus-6.7.0-debian6_amd64.deb.
Une fois l'agent *Nessus* installé, le programme /opt/nessus_agent/sbin/nessuscli a été utilisé pour l'associer au *Nessus Manager*.

2.3.1.3. Durée de l'installation

L'installation, consistant en les étapes décrites ci-après, a duré trois heures au total :

- l'installation des machines avec CentOS pour le manager et *Debian* pour le scanner et l'agent ;
- l'installation de *Nessus Manager*, *Nessus Scanner* et *Nessus Agent* ;
- la configuration des utilisateurs et l'association des scanners et agents.

2.3.1.4. Notes et remarques diverses

Aucune procédure d'installation sécurisée spécifique n'est référencée dans le guide d'installation [GUIDE]. *Nessus Manager* a été configuré par l'évaluateur en se référant à la cible de sécurité, et en respectant les bonnes pratiques de sécurité.

2.3.2. Analyse de la documentation

Le guide d'installation décrit correctement les étapes d'installation par défaut. Cependant il n'existe pas de partie dédiée au déploiement d'un environnement Nessus de manière sécurisée. Toutes ces informations sont dispersées dans les différentes étapes et décrites comme optionnelles.
Le renforcement de la sécurité d'un *Nessus Manager* demande de faire preuve de rigueur et d'une bonne connaissance du produit.

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue du code source et estime que le code est lisible et bien organisé.
La maintenabilité du code est assurée par sa modularité et l'utilisation de fonctions clairement définies.

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

Le composant *Nessus Manager* est, par défaut, lancé avec l'identité *root*. Ceci expose le système hôte dans le cas où une vulnérabilité venait à être exploitée sur le composant.
La version évaluée du produit permet toutefois de réduire le niveau de privilèges de *Nessus Manager* en le configurant tel que décrit dans le guide utilisateur (voir [GUIDES]).
Il est fortement recommandé d'utiliser cette option de configuration afin de réduire les risques induits sur le système hébergeant *Nessus Manager*.

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

Lors de l'édition d'un paramètre de configuration, il est nécessaire de valider deux fois la modification effectuée ; une première fois via la boîte de dialogue ouverte (bouton « *save* »), puis dans le menu en haut de page (nouveau bouton « *save* »).
En effet, la première validation n'entraîne pas l'application des nouveaux paramètres, ainsi un administrateur non habitué ou inattentif pourrait modifier un paramètre de sécurité mais ne pas l'appliquer.

2.3.8.2. Recommandations pour une utilisation sûre du produit

L'évaluateur recommande de n'utiliser *Nessus Manager* qu'en mode « orchestrateur », afin d'isoler correctement la partie contrôle de la partie tests. Seuls les scanners devraient exécuter les plugins.
En outre, les recommandations suivantes sont formulées :

- utiliser une clé maîtresse pour assurer un niveau de confidentialité en cas de compromission du système de fichiers ;
- restreindre les permissions sur le répertoire `/opt/nessus` en retirant les droits pour *others ;*
- filtrer l'accès réseau au port TCP 8344 en autorisant uniquement les utilisateurs *Nessus Manager* ainsi que les agents et scanners à accéder au service ;
- bloquer le trafic réseau de *Nessus Manager* en autorisant uniquement les connexions sortantes vers un relais HTTP pour la mise à jour du produit ;
- installer uniquement des plugins NASL (compilés ou non-compilés) provenant d'une source de confiance ;
- auditer régulièrement les droits d'accès configurés pour les utilisateurs *Nessus Manager* ;
- régénérer la clé d'enrôlement avant et après tout enrôlement de scanner ou d'agent ;
- enrôler les agents et scanners dans un environnement de confiance. Utiliser une liaison réseau sécurisée entre les agents, les scanners et le *Nessus Manager* pendant l'enrôlement.

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

De manière générale, le produit s'utilise simplement ; l'administrateur doit toutefois être vigilant et effectuer la configuration conformément aux bonnes pratiques de sécurité et en suivant les recommandations formulées dans ce rapport.

2.3.8.4. Notes et remarques diverses

Sans objet.

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. Certains algorithmes utilisés ne sont pas conformes au RGS, toutefois aucune vulnérabilité exploitable n'a été identifiée.

2.5. Analyse du générateur d'aléas

Les différentes sources d'aléas ont été étudiées dans le cadre de cette évaluation ; les mêmes conclusions que celles énoncées au chapitre 2.4 s'appliquent.

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 « Nessus Manager, version 6.7 » 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 Nessus Manager version 6.7* Version : *1.0* ; Date : 30 mai 2016.
[RTE]	*Rapport technique d'évaluation CSPN Nessus Manager v6.7* Référence : *CSPN-NESSUS-MANAGER-01* ; Version : 1.0 ; Date : 18 juillet 2016.
[GUIDES]	*Nessus 6.4 Installation and Configuration Guide* Référence : *http://static.tenable.com/documentation/nessus_6.4_installation_guide.pdf ;* Version : 5 ; Date : *4 novembre 2015 ;* Nessus 6.7 User Guide Référence : *https://docs.tenable.com/nessus/6_7/Content/PDF/Nessus_User_Manual.pdf ;* Version : 6 ; Date : *Juin 2016 ;* *Nessus 6.4 Command Line Reference* Référence : *http://static.tenable.com/documentation/nessus_6.4_command_line_reference.pdf ;* Version : 2 ; Date : *7 juillet 2015.*

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 (CSPN) 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/
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.