Cible de Sécurité CSPN

Nessus Manager version 6.7

- PUBLIC -

Version 1.0

Identification du document

Caractéristiques

Objet	Cible de Sécurité CSPN - Nessus Manager version 6.7
Nombre de pages	15
Diffusion	PUBLIC

Historique

Version	Date	État
1.0	30/05/2016	Première version

Table des matières

1. Introduction

1.1. Identification du produit

Organisation éditrice	Tenable Network Security
Lien vers l'organisation	https://www.tenable.com/
Nom commercial du produit	Nessus Manager
Numéro de la version évaluée	6.7
Catégorie de produit	Administration et supervision de la sécurité

2. Argumentaire (description) du produit

2.1. Description générale du produit

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.

2.1.1. Nessus Scanner

Les *Nessus Scanner* sont des scanners réseau et de vulnérabilités. Ils interagissent avec une liste donnée d'adresses (IPv4 ou IPv6) dans le but de :

- identifier les services et machines actifs sur le réseau ;
- rechercher des vulnérabilités connues dans les services identifiés ;
- vérifier la conformité de la configuration des systèmes à une politique donnée ;
- détecter la présence de logiciels malveillants ;
- trouver des vulnérabilités dans les applications web ;
- signaler la présence d'informations sensibles sur les systèmes.

Afin de permettre au scanner l'accès à certaines informations ou fonctionnalités, il est possible de configurer le scanner pour qu'il utilise des comptes et des mots de passes sur les systèmes à auditer. Ces comptes peuvent être privilégiés.

Dans la suite de ce document, nous utiliserons le mot *scan* pour désigner l'exécution d'un *Nessus Scanner* sur une ou plusieurs adresses.

2.1.2. Nessus Agents

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. C'est le *Nessus Manager* qui pilote les agents qui peuvent eux-mêmes être utilisés pour :

- récupérer des informations sur la machine :
  - La liste des mises à jour appliquées, des utilisateurs présents, des programmes installés, des programmes lancés au démarrage, des périphériques USB insérés, etc. ;
- vérifier la conformité de la configuration de la machine à une politique de sécurité donnée ;
- détecter la présence de logiciels malveillants sur la machine.

2.1.3. Nessus Plugins

Les *Nessus Plugins* sont des modules permettant la détection d'une vulnérabilité ou la collecte d'une information donnée. Concrètement, les *Nessus Plugins* sont des programmes codés à l'aide du langage *Nessus Attack Scripting Language* (NASL). Ces *Nessus Plugins* sont exécutés par les *Nessus Scanner* et *Nessus Agents*.

2.1.4. Nessus Manager

Nessus Manager permet de gérer un ensemble de *Nessus Scanners* et de *Nessus Agents*. Cette gestion s'effectue à plusieurs niveaux : utilisateurs, politiques, scans et mises à jour.

Gestion des utilisateurs

Il existe quatre rôles d'utilisateurs dans *Nessus Manager* :

- *Read Only* : les utilisateurs ne peuvent que lire les résultats des scans auxquels ils ont accès.
- *Standard* : les utilisateurs peuvent, en plus des actions précédentes, lancer des scans, créer des politiques de scans, planifier des scans et générer des rapports de scans.
- *Administrator* : les utilisateurs peuvent, en plus des actions précédentes, gérer les différents groupes d'utilisateurs, utilisateurs, scanners et agents.
- *System Administrato*r : rôle le plus privilégié, les utilisateurs peuvent configurer l'intégralité du système.

En plus de ces quatre rôles, il est possible de définir des groupes d'utilisateurs. Ces groupes permettent d'attribuer et de révoquer des droits à un ensemble d'utilisateurs en même temps.

Des droits peuvent être affectés aux différents utilisateurs ou groupes :

- Sur les différents scanners et les politiques :
  - *No Access* : aucun accès ;
  - *Can Use* : l'utilisateur ou le groupe peut voir et utiliser le scanner ou la politique mais il ne peut pas le configurer ;
  - *Can Manage* : l'utilisateur ou le groupe peut voir, utiliser et modifier la configuration du scanner ou la politique.
- Sur les scans :
  - *No Access* : aucun accès ;
  - *Can View* : l'utilisateur ou le groupe peut voir les résultats du scan ;
  - *Can Control* : l'utilisateur ou le groupe peut, en plus des actions précédentes, lancer le scan, le stopper ou le mettre en pause ;
  - *Can Configure* : l'utilisateur ou le groupe peut, en plus des actions précédentes, modifier la configuration du scan (périodicité, politique etc.).
- Sur les différents groupes d'agents :
  - *No Access* : aucun accès ;
  - *Can Use* : l'utilisateur ou le groupe peut interagir avec les agents.

L'authentification des utilisateurs peut être faite localement ou à l'aide d'un serveur LDAP, via un certificat ou un mot de passe.

Gestion des politiques et des scans

Des politiques de scans peuvent être créées, exportées et importées depuis le manager. Des scans peuvent être configurés, programmés et lancés depuis le manager sur les différents scanners auxquels il a accès. La possibilité d'effectuer ces

différentes actions est contrôlée par le manager à l'aide des droits des utilisateurs.

L'export et l'import peuvent se faire à l'aide de deux formats : un format XML et une base de donnée au format SQLite chiffrée à l'aide du module SEE, de l'algorithme AES 128 utilisé en mode OFB et à l'aide d'une clé définie par l'utilisateur.

Les scans peuvent aussi être visualisés sous différentes formes (tableau de bord, listes de vulnérabilités, de machines etc.) et comparés entre eux.

Enfin, il est possible de configurer l'envoi automatique d'un e-mail à une liste de personnes lorsqu'un scan se termine.

Gestion des mises à jour

La mise à jour des scanners, plugins et agents est assurée par le manager. Les scanners et agents se connectent au manager au travers d'une communication sécurisée et le manager leur transmet les mises à jours disponibles.

Les mises à jour sont signées à l'aide d'une clé privée à laquelle seul Tenable a accès et à l'aide de l'algorithme RSASSA-PKCS1-v1_5 associé à l'algorithme SHA1 et d'une bi-clé de 4096 bits.

Il est possible de configurer le manager de façon à ce qu'il télécharge et installe les mises à jour de manière automatique.

2.2. Description de la manière d'utiliser le produit

La principale manière d'utiliser Nessus Manager est via une interface web au travers d'une connexion sécurisée à l'aide de HTTPS.

Il est aussi possible, principalement pour des opérations d'administration, d'utiliser une interface en ligne de commande (*nessuscli*).

Enfin, en plus de l'interface web graphique, une API REST (Nessus REST API) est exposée. Cette API expose les mêmes fonctionnalités que l'interface web visuelle et permet d'automatiser certaines tâches.

2.3. Description de l'environnement prévu pour son utilisation

Nessus Manager se déploie sur un serveur dédié. Nessus Manager et l'éventuel serveur LDAP utilisé pour l'authentification des utilisateurs doivent être situés dans une zone de confiance du système d'informations et protégés à un niveau de sécurité équivalent à celui des applications les plus sensibles.

Les scanners sont déployés sur des serveurs dédiés et de confiance, dans des zones potentiellement non de confiance et avec un niveau de sécurité potentiellement inférieur à celui du Nessus Manager.

Les agents sont déployés sur des équipements potentiellement compromis et non de confiance.

2.4. Description des hypothèses sur l'environnement

Nessus Manager doit être installé sur un système sain, correctement mis à jour et suffisamment sécurisé. Les administrateurs systèmes sont considérés comme non hostiles et compétents.

H1. Installation et Initialisation

- Nessus Manager est installé sur un serveur dédié, dans une zone de confiance du système d'information.
- Nessus Manager est administré depuis un poste sain, déployé dans la même zone de confiance du système d'information.

- Les scanners et agents sont installés et configurés sur des équipements sains, non compromis.
- La génération de l'ensemble des clés, bi-clés et certificats associés est effectuée dans un environnement sûr et à l'aide d'un équipement conforme aux règles et recommandations de l'ANSSI dans le RGS.
- Les éléments cryptographiques utilisés par Nessus Manager et configurables sont générés, dimensionnés et utilisés conformément aux règles de l'ANSSI dans le RGS. Ces éléments comportent notamment :
    - la clé maître de Nessus (utilisée pour chiffrer les données sur le disque) ;
    - le certificat utilisé pour l'interface web et l'API REST ;
    - Les mots de passes utilisés pour exporter les scans ;
    - l'ensemble des éléments de l'infrastructure de gestion de clé utilisée pour l'authentification par certificat.
- Seules les suites TLS conformes aux règles et recommandations de l'ANSSI dans le RGS sont autorisées dans la configuration de Nessus Manager.

H2. Administrateurs

- Il est supposé que les utilisateurs de Nessus Manager ayant les rôles *System Administrator* ou *Administrator* décrits dans le chapitre sont non hostiles, formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration.

H3. Local

- Les équipements contenant les services de Nessus Manager sont sécurisés et leur accès est restreint aux personnes autorisées qui sont considérées comme non hostiles.

H4. Maîtrise du système

- Le système d'exploitation supportant Nessus Manager est correctement administré et configuré. En particulier, l'accès au système d'exploitation du serveur doit être réservé aux seuls administrateurs systèmes. Seuls les services de Nessus Manager (interface web et API REST) sont exposés sur le réseau et au travers d'une connexion sécurisée par HTTPS.

H5. LDAP

- Le serveur LDAP utilisé pour l'authentification des utilisateurs est considéré comme sain, non hostile et correctement configuré.
- Le serveur LDAP et le Nessus Manager sont situé dans le même réseau de confiance. Cette hypothèse exclut l'interception ou la modification des communications entre le serveur LDAP et le Nessus Manager.

2.5. Description des dépendances

Nessus Manager doit être installé sur l'un des systèmes d'exploitation suivants :

- Unix :
    - Debian 6 et 7 / Kali Linux (i386 ou x86-64)
    - Fedora 20 et 21 (i386 ou x86-64)

- FreeBSD 10 (x86-64)
- Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 ou x86-64)
- Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (i386 ou x86-64) [Server, Desktop, Workstation]
- Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (x86-64) [Server, Desktop, Workstation]
- SUSE 10 (x86-64) ou 11 (i386 ou x86-64)
- Ubuntu 10.04 (9.10 package), 11.10, 12.04, 12.10, 13.04, 13.10 et 14.04 (i386 ou x86-64)

- Mac :
  - Mac OS X 10.8, 10.9 et 10.10 (x86-64)
- Windows :
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Microsoft Server 2012 R2 (x86-64)
  - Windows 7 et 8 (i386 et x86-64)

De plus, Nessus Manager doit être installé sur un système disposant au minimum de 2 Go de mémoire vive (8 Go recommandés), d'un processeur cadencé à 2 GHz (2 cœurs recommandés) et de 30 Go d'espace disque.

Certaines fonctionnalités, en dehors du périmètre de l'évaluation, reposent sur différents logiciels ou matériels non fournis avec le produit :

- Authentification par certificat : nécessite une infrastructure de gestion de clés.
- Authentification à l'aide d'un serveur LDAP : nécessite un serveur LDAP.
- Création de rapports au format PDF : dernière version du produit Oracle Java.
- Envoi d'e-mails automatique à la fin d'un scan : nécessite un serveur SMTP.

2.6. Description des utilisateurs typiques concernés

Les différents types d'utilisateurs et les rôles associés sont décrits dans le chapitre 2.1.4.

2.7. Définition du périmètre de l'évaluation

L'évaluation porte sur les différentes fonctionnalités de Nessus Manager décrites dans le chapitre 2.1 :

- L'authentification des utilisateurs ;
- La gestion des droits d'accès des utilisateurs ;
- Les communications entre les agents ou les scanners et le manager ;

- La génération et le stockage des différents scans ;
- La gestion des agents et des scanners (mise à jour et configuration).

L'interfaçage avec le produit tiers CISCO ISE et le scanner intégré à Nessus Manager sont considérés hors cible. L'évaluation des scanners Nessus pourra faire l'objet d'une certification ultérieure.

3. Description de l'environnement technique dans lequel le produit doit fonctionner

3.1. Matériel compatible ou dédié

Nessus Manager doit être installé sur un système dédié disposant au minimum de 2 Go de mémoire vive (8 Go recommandés), d'un processeur cadencé à 2 GHz (2 cœurs recommandés) et de 30 Go d'espace disque.

3.2. Système d'exploitation retenu

Le système d'exploitation retenu pour l'évaluation est CentOS 6.

4. Description des biens sensibles que le produit doit protéger

Les biens sensibles que Nessus Manager doit protéger sont les suivants :

- les données d'authentification des utilisateurs: le nom et le mot de passe des utilisateurs, les clés d'accès aux API REST.
- les configurations des scans : les adresses IP scannées, les mots de passe utilisés pour les scans authentifiés, la liste des plugins utilisés etc.
- les résultats des scans : quand ils sont affichés, transmis, traités (via l'utilisation des filtres par exemple) et stockés.
- l'accès aux scanners ou aux agents : les clés cryptographiques permettant de les contrôler ou de les configurer.
- les mises à jour des plugins, agents et scanners.

5. Description des menaces

5.1. Agents menaçants

Les agents menaçants sont les suivants :

- les utilisateurs malveillants disposant d'un accès limité à Nessus Manager ;
- les attaquants extérieurs, capable d'intercepter et de modifier les flux de communications entre le Nessus Manager et les scanners ou les agents ;
- les attaquants disposant d'un accès privilégié à un équipement sur lequel serait installé un scanner ou un agent configuré pour communiquer avec le Nessus Manager.

Les administrateurs (utilisateurs disposant des rôles *System Administrator* et *Administrator*) ne sont pas considérés comme des attaquants potentiels.

5.2. Menaces

Les menaces identifiées sont les suivantes :

M1 : Usurpation de l'identité d'un utilisateur

Un attaquant parvient à usurper l'identité d'un utilisateur et abuse des rôles attribués à cet utilisateur.

M2 : Usurpation de l'identité d'un scanner ou d'un agent

Un attaquant parvient à usurper l'identité d'un scanner ou d'un agent et récupère des informations sensibles (comme la configuration d'un scan) ou injecte des données erronées dans le manager.

M3 : Usurpation de l'identité du manager

Un attaquant parvient à usurper l'identité du manager et récupère des informations sensibles (comme le résultat d'un scan) ou essaie de contrôler le scanner.

M4 : Récupération d'information sur le réseau

Un attaquant intercepte les communications entre le manager et un scanner, un agent ou un utilisateur et récupère des informations sensibles (configuration ou résultats de scans).

M5 : Modification d'informations sur le réseau

Un attaquant injecte des données dans les communications entre le manager et un scanner, un agent ou un utilisateur et modifie les données échangées afin de prendre le contrôle de l'agent ou du scanner (en modifiant la configuration ou la mise à jour envoyée par le manager par exemple) ou modifie les résultats remontés par le scanner ou l'agent.

M6 : Élévation de privilèges horizontale

Un utilisateur autorisé du manager parvient à accéder à des données pour lesquels il n'a pas de rôles associés le permettant.

M7 : Élévation de privilèges verticale

Un utilisateur autorisé du manager parvient à utiliser des fonctions d'administration sans avoir de rôle d'administration.

M8 : Utilisation illégitime de l'interface web

Un utilisateur légitime du manager parvient à utiliser des fonctions sensibles exposées par l'interface web sans être authentifié.

M9 : Utilisation illégitime de l'API REST

Un utilisateur légitime du manager parvient à utiliser des fonctions sensibles de l'API REST sans être authentifié.

M10 : Compromission du serveur

Un attaquant ou un utilisateur parvient à exécuter des commandes sur le serveur hébergeant le manager.

6. Description des fonctions de sécurité du produit

F1 : 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.

Par hypothèse, les suites autorisées doivent être conformes aux règles de l'ANSSI dans le RGS.

F2 : 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 suite 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 entêtes des requêtes HTTP.

F3 : contrôle d'accès

Nessus Manager permet de contrôler l'accès à différentes fonctions (détaillées dans le chapitre 2.1.4) au moyen de rôles alloués aux utilisateurs.

F4 : authentification des utilisateurs

Les utilisateurs sont authentifiés à l'aide de leur mot de passe ou d'un certificat. Dans le cas de l'utilisation d'un mot de passe, celui-ci peut être vérifié à l'aide d'un condensat généré à l'aide de l'algorithme MD5 et d'un sel de 16 octets et stocké dans un fichier sur le disque du Nessus Manager ou à l'aide d'un serveur LDAP.

F5 : 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 SEE paramétré de façon à utiliser l'algorithme AES-128 en mode OFB.

Dans le cas des données exportées, la clé de chiffrement est fournie par l'utilisateur. Dans le cas des données stockées sur le Nessus Manager, la clé de chiffrement est générée à l'installation de Nessus Manager et est stockée dans une base de donnée SQLite qui peut être chiffrée à l'aide d'un mot de passe fournit par l'administrateur au démarrage de Nessus Manager.