PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2021/28

Guardian sur NSG-M

Version 21.3.0

Paris, le 30 novembre 2021

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

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-2021/28**
Nom du produit **Guardian sur NSG-M**
Référence/version du produit **Version 21.3.0**
Catégorie de produit **Administration et supervision de la sécurité**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire NOZOMI NETWORKS, INC. Via Maria Ghioldi-Schweizer 2 6850 Mendrisio Suisse
Développeur NOZOMI NETWORKS, INC. Via Maria Ghioldi-Schweizer 2 6850 Mendrisio Suisse
Centre d'évaluation AMOSSYS 11 rue Maurice Fabre, 35000 Rennes
Fonctions de sécurité évaluées **Communications sécurisées sur les interfaces d'administration** **Authentification sur les interfaces d'administration** **Mise à jour sécurisée** **Journalisation** **Stockage de secrets sécurisé** **Confidentialité et intégrité de la configuration** **Gestion des entrées malformées** **Alarmes**
Fonctions de sécurité non évaluées **Sans objet**
Restriction(s) d'usage **Oui (cf. §3.2)**

PREFACE

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 MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est le composant Guardian sur NSG-M, Version 21.3.0, développé par NOZOMI NETWORKS, INC.

Ce produit est le composant principal de la solution *Nozomi Networks Solution*, dédiée à la gestion de la sécurité des réseaux et à la détection d'intrusion. La solution complète est composée des éléments suivants :

- « Guardian », l'entité principale, en charge du traitement des données ;
- « *Remote Collector* », un composant optionnel qui collecte des données pour « Guardian »;
- « *Central Management Console* », une interface optionnelle unifiée pour les architectures mettant en œuvre plusieurs « Guardian » ;
- « *Threat Intelligence* », un service optionnel visant à améliorer la détection de maliciels et d'anomalies ;
- « *Smart Polling* », une fonctionnalité optionnelle visant à améliorer l'extraction de données.

La cible de cette évaluation est le composant « Guardian ». Ce composant analyse le trafic réseau en temps-réel et reporte les anomalies détectées. Le trafic est obtenu via capture passive ; à cette capture peuvent s'ajouter les données obtenues via les « *Remote Collector* » optionnels. Aucun « *Remote connector* » n'a été déployé dans le cadre de cette évaluation.

Une interface graphique est accessible via un navigateur *web*, et permet d'afficher l'état général du réseau, les processus, alarmes, rapports et vulnérabilités détectés par le « Guardian ». L'accès à cette interface est contrôlable via un *Active Directory*, et de l'intégrer à un SSO via le protocole SAML.

Le « Guardian » peut être déployé sur différentes appliances physiques, dans une machine virtuelle ou encore dans un conteneur. Cette évaluation CSPN a uniquement considéré un « Guardian » déployé sur une appliance physique NSG-M.

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*

Produit	
Nom du produit	Guardian sur NSG-M
Numéro de la version évaluée	Version 21.3.0

La version certifiée du produit peut être affichée depuis l'interface *web*, lors d'une connexion SSH et dans le fichier `/etc/n2os_version` comme visible ci-dessous:

1.2.3 *Fonctions de sécurité*

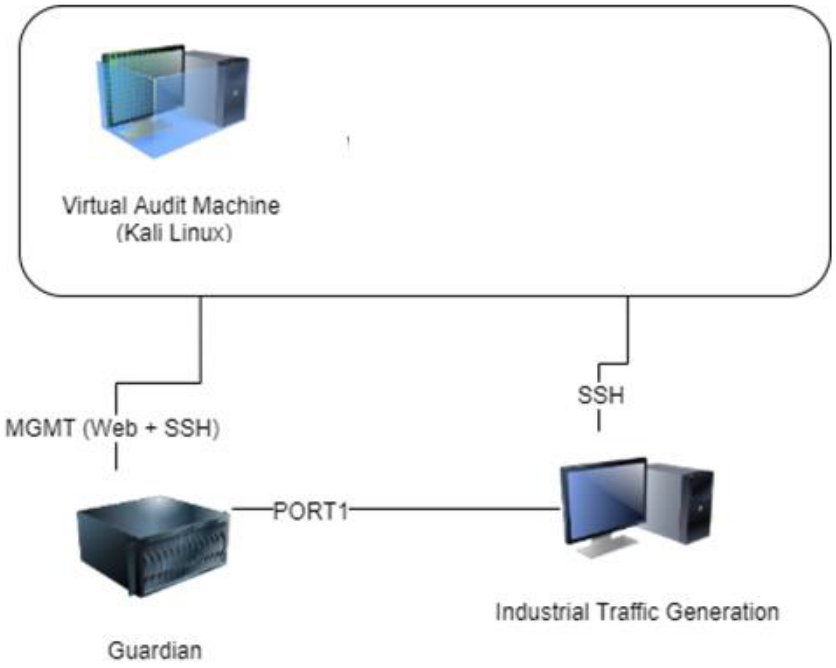
Les fonctions de sécurité évaluées du produit sont :

- les communications sécurisées sur les interfaces d'administration ;
- l'authentification sur les interfaces d'administration ;
- la mise à jour sécurisée ;
- la journalisation ;
- le stockage de secrets sécurisé ;
- la confidentialité et intégrité de la configuration ;
- la gestion des entrées malformées ;
- les alarmes.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond à un déploiement sur appliance NSG-M.

La plateforme de test est constituée des éléments suivants :



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 B.

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 **Erreur ! Source du renvoi introuvable.**.

2.3.1 *Installation du produit*

2.3.1.1 Particularités de paramétrage de l'environnement et options d'installation

La plateforme évaluée consiste en une appliance physique NGS-M qui a été fournie préinstallée dans le cadre de travaux de pré-audit.

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

Seules quelques actions ont été nécessaires de la part de l'auditeur :

- branchements électriques ;
- connexion de l'interface de gestion à un VLAN d'expérimentation dédié ;
- initialisation de la configuration (adresse IP, DNS) depuis le port série USB à l'avant de l'appliance.

Pour les travaux d'évaluation, une mise à jour a été effectuée suivie d'une restauration usine totale. Puis la partie initialisation a de nouveau dû être réalisée. Ces travaux ont permis de détecter une non-conformité et entraîné une restriction d'usage sur le produit (cf. §3.2).

2.3.1.3 Durée de l'installation

L'installation a duré moins d'une journée.

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'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité. En revanche, certains paramétrages documentés comme optionnels dans les [GUIDES] sont nécessaires au maintien de la sécurité de la solution (voir §3.2)

2.3.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques 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.

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 connues existent sur des briques tierces du produit, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et 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 et dans le contexte défini par la cible de sécurité [CDS].

2.3.7 *Analyse de la facilité d'emploi*

2.3.7.1 Cas où la sécurité est remise en cause

Les risques identifiés lors de l'évaluation entraînent des recommandations et des restrictions d'usage pour l'utilisateur (voir chapitre 3.2).

2.3.7.2 Avis d'expert sur la facilité d'emploi

L'évaluateur estime que la TOE est facilement utilisable. La documentation permet correctement son installation et son utilisation.

2.3.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le **Erreur ! Source du renvoi introuvable.**.

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 **Erreur ! Source du renvoi introuvable.**). Celle-ci n'a pas identifié de non-conformités à [ANSSI-PG-083] entraînant de vulnérabilités exploitables.

2.5 Analyse du générateur d'aléas

Le générateur aléatoire du produit a fait l'objet d'une analyse au titre de cette évaluation CSPN (voir **Erreur ! Source du renvoi introuvable.**). Celle-ci n'a pas identifié de non-conformités à [ANSSI-PG-083] entraînant de vulnérabilités exploitables.

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 Guardian sur NSG-M, Version 21.3.0 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité **Erreur ! Source du renvoi introuvable.** 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 et conditions de déploiement spécifiés dans la cible de sécurité **Erreur ! Source du renvoi introuvable.**, et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations et restrictionsde **Erreur ! Source du renvoi introuvable.**. .

Afin de garantir l'utilisation sécurisée du produit, il est impératif que l'utilisateur mette en œuvre les mesures suivantes :

- contrairement à ce qu'indique la procédure Setup Phase 1 du manuel *USER MANUAL* (voir [GUIDES]), l'invite de commande ne force pas l'utilisateur à changer le mot de passe du compte admin. Il en résulte que la connexion SSH n'est pas sûre par défaut. Il est impératif que l'utilisateur change ce mot de passe après installation, afin de mettre en œuvre un mot de passe spécifique et conforme avec les recommandations [NT-MDP] ;
- la configuration par défaut entraîne l'utilisation d'un certificat TLS autosigné. L'utilisateur doit impérativement suivre les [GUIDES] afin de remplacer ce certificat par un certificat issu d'une IGC et conforme aux recommandations de [NT-TLS] ;
- la configuration par défaut permet la mise en œuvre de mots de passe *web* ne respectant pas [NT-MDP]. L'utilisateur doit impérativement utiliser des mots de passe respectant les recommandations [NT-MDP].

La solution offre des fonctionnalités et procédures documentées pour corriger ces deux points et respecter ainsi l'état de l'art.

ANNEXE A. Références documentaires du produit évalué

[CDS]	*CSPN Security Target - Product Guardian on NSG-M version 21.3.0* Référence : CSPN-ST-Guardian on NSG-M-1.05 ; Version : 1.05 Date : 11/08/2021
[RTE]	Rapport Technique d'Évaluation CSPN - Produit Guardian sur NSG-M - version 21.3.0 Référence : CSPN-RTE-N2OSv21.3.0 ; Version : 2.01 ; Date : 15 octobre 2021.
[GUIDES]	*« USER MANUAL – Nozomi Networks Solution – N2OS »,* Aoüt 2021 N2OS-UserManual-21.3.0.pdf *« SOFTWARE DEVELOPMENT KIT – Nozomi Networks Solution – N2OS »,* Août 2021 N2OS-UserManual-SDK-21.3.0.pdf

ANNEXE B. 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.
[ANSSI-PG-083]	Guide des mécanismes cryptographiques – règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.04 du 1 janvier 2020, voir www.ssi.gouv.fr.
[NT-MDP]	Recommandations de sécurité relatives aux mots de passe, ANSSI, https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/
[NT-TLS]	Note technique « Recommandations de sécurité relatives à TLS », version 1.2 du 26/03/2020 Ref : SDE-NT-35/ANSSI/SDE/NP