



**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-2024/06

NEXIUM SafeCore Version 2.1.1

Paris, le 14 Juin 2024

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

Emmanuel NAEGELEN

[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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CSPN-2024/06
Nom du produit	NEXIUM SafeCore
Référence/version du produit	Version 2.1.1
Catégorie de produit	Matériel et logiciel embarqué
Critère d'évaluation et version	CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)
Commanditaire	THALES SIX GTS France 4 avenue des Louvresses 92622 Gennevilliers, France
Développeur	THALES SIX GTS France 4 avenue des Louvresses 92622 Gennevilliers, France
Centre d'évaluation	THALES / CNES 290, allée du Lac 31670 Labège, France
Fonctions de sécurité évaluées	Génération de clefs Contrôle d'accès Isolation cryptographique Effacement sécurisé Journalisation Démarrage sécurisé Isolation des flux de données
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 cyber.gouv.fr.

TABLE DES MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit évalué.....	6
1.2.1	Catégorie du produit.....	6
1.2.2	Identification du produit.....	6
1.2.3	Fonctions de sécurité.....	7
1.2.4	Configuration évaluée.....	7
2	L'évaluation.....	8
2.1	Référentiels d'évaluation.....	8
2.2	Travaux d'évaluation.....	8
2.2.1	Installation du produit.....	8
2.2.2	Analyse de la documentation.....	8
2.2.3	Revue du code source (facultative).....	9
2.2.4	Analyse de la conformité des fonctions de sécurité.....	9
2.2.5	Analyse de la résistance des mécanismes des fonctions de sécurité.....	9
2.2.6	Analyse des vulnérabilités (conception, construction, etc.).....	9
2.2.7	Analyse de la facilité d'emploi.....	9
2.3	Analyse de la résistance des mécanismes cryptographiques.....	10
2.4	Analyse du générateur d'aléa.....	10
3	La certification.....	11
3.1	Conclusion.....	11
3.2	Recommandations et restrictions d'usage.....	11
ANNEXE A.	Références documentaires du produit évalué.....	12
ANNEXE B.	Références liées à la certification.....	13

1 Le produit

1.1 Présentation du produit

Le produit évalué est « NEXIUM SafeCore, Version 2.1.1 » développé par THALES SIX GTS France.

Ce produit est une infrastructure de virtualisation (hyperviseur) sécurisée orientée réseau. Il permet l'exécution simultanée et sécurisée de plusieurs machines virtuelles hébergeant des fonctionnalités réseau ou applicatifs ou système d'exploitation sur un matériel x86. Il fournit une isolation logique forte, à la fois entre les différentes machines virtuelles et entre les machines virtuelles et le matériel.

Le périmètre évalué couvre le logiciel de virtualisation NEXIUM SafeCore. Les autres composants du système, comme les machines virtuelles et l'équipement matériel ne sont pas dans le périmètre d'évaluation. NEXIUM SafeCore est conçu pour être intégré dans le système d'information de l'utilisateur final.

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

<input type="checkbox"/>	1	détection d'intrusions
<input type="checkbox"/>	2	anti-virus, protection contre les codes malicieux
<input type="checkbox"/>	3	pare-feu
<input type="checkbox"/>	4	effacement de données
<input type="checkbox"/>	5	administration et supervision de la sécurité
<input type="checkbox"/>	6	identification, authentification et contrôle d'accès
<input type="checkbox"/>	7	communication sécurisée
<input type="checkbox"/>	8	messagerie sécurisée
<input type="checkbox"/>	9	stockage sécurisé
<input type="checkbox"/>	10	environnement d'exécution sécurisé
<input type="checkbox"/>	11	terminal de réception numérique (Set top box, STB)
<input checked="" type="checkbox"/>	12	matériel et logiciel embarqué
<input type="checkbox"/>	13	automate programmable industriel
<input type="checkbox"/>	99	autre

1.2.2 Identification du produit

Produit	
Nom du produit	NEXIUM SafeCore
Numéro de la version évaluée	Version 2.1.1

La version certifiée du produit peut être identifiée en se connectant au SafeCore avec un des comptes utilisateurs autorisés, et en exécutant les commandes `system-info` et `system-api-version`.

1.2.3 Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- la génération de clefs, en utilisant une source d'entropie physique ;
- le contrôle d'accès, via un mécanisme d'authentification ;
- l'isolation cryptographique : protection en confidentialité et en intégrité des clefs utilisées pour la protection des données ;
- l'effacement sécurisé, de toutes les clefs générées et des mots de passes sauvegardés ;
- la journalisation : stockage et protection en intégrité des événements de sécurité ;
- le démarrage sécurisé : contrôle de l'intégrité de la chaîne de démarrage, et de l'intégrité et de l'authenticité du logiciel ;
- l'isolation des flux internes de données : cloisonnement des machines virtuelles.

1.2.4 Configuration évaluée

Le SafeCore a pour plateforme matérielle cible les équipements type Intel x86_64 banalisés. Il est basé sur un noyau Linux 5.10.0-23-amd64 de la distribution Debian 5.10.179-1. Les mécanismes de virtualisation sont assurés par KVM/QEMU.

La plateforme de test est constituée des éléments décrits dans la cible de sécurité [CDS] section 3.4.1.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

2.2 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].

2.2.1 Installation du produit

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

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

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

Le produit est livré sur un ordinateur hôte, prêt à être opéré, sans aucune procédure d'installation.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 Analyse de la documentation

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 Revue du code source (facultative)

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit ainsi que des scripts d'installation et d'administration du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 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.

2.2.6 Analyse des vulnérabilités (conception, construction, etc.)

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitable pour le niveau d'attaquant considéré dans le contexte défini par la cible de sécurité [CDS].

2.2.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitable pour le niveau d'attaquant considéré.

2.2.7 Analyse de la facilité d'emploi

2.2.7.1 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.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.2.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit ne comporte pas de générateur d'aléa entrant dans le périmètre d'évaluation.

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 « NEXIUM SafeCore, Version 2.1.1 » 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], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- La version courante du produit SafeCore ne doit pas être intégrée sur une plateforme cible contenant des composants dont les drivers présentent des vulnérabilités.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : <ul style="list-style-type: none">- CIBLE DE SÉCURITÉ CSPN <i>SECURITY TARGET</i> - NEXIUM SAFECORE 3, révision D, 30 octobre 2023
[RTE]	Rapport technique d'évaluation : <ul style="list-style-type: none">- Rapport d'évaluation CSPN – NEXIUM3, référence NEXIUM3_CSPN_1.2, version 1.2, 6 mai 2024
[GUIDES]	Guide d'utilisation, d'administration et d'installation du produit : <ul style="list-style-type: none">- Manuel utilisateur du logiciel (SUM) SAFECORE, référence 0026-F0057 69357905-108-v001 ;- Manuel utilisateur du logiciel (SUM) SAFEINSTALLER outil de déploiement d'un SAFECORE, référence 69357909-108-v001.

ANNEXE B. Références liées 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, version 5.0, 12 janvier 2023. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0, 6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.