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-2021/19

KAKOMA

KAKOMA-10G-0M1 (REV 01), version du logiciel Java code software version S6.4.100

Paris, le 21 juillet 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2021/19**
Nom du produit **KAKOMA**
Référence/version du produit **KAKOMA-10G-0M1 (REV 01), version du logiciel Java code software version S6.4.100**
Catégorie de produit **Matériel et logiciel embarqué**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **CAILABS** 38 boulevard Albert 1er 35200 Rennes, France
Développeur **CAILABS** 38 boulevard Albert 1er 35200 Rennes, France
Centre d'évaluation **CEA - LETI** 17 rue des martyrs 38054 Grenoble Cedex 9, France
Fonctions de sécurité évaluées **Fonction d'obfuscation (camouflage) des données dans la fibre** **Fonction de détection d'intrusion sur la fibre**
Fonctions de sécurité non évaluées **Néant**
Restriction(s) d'usage **Non**

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 l'équipement « KAKOMA, KAKOMA-10G-0M1 (REV 01), version du logiciel Java code software version S6.4.100 » développé par CAILABS.

Ce produit est un équipement actif de réseau local (LAN) destiné à sécuriser une transmission haut débit sur une fibre optique multimode (MMF) contre une attaque physique d'espionnage sur la fibre. Les cas d'usage typiques sont la sécurisation d'une fibre déployée sur une base militaire, sur un site industriel ou dans un immeuble de bureaux partagé entre plusieurs entreprises.

Le produit remplit trois fonctions principales :

- il rend possible une transmission haut débit (10 Gbits/s) sur une fibre optique multimode grâce à l'injection des données sur le mode spatial fondamental de la fibre, ce qui permet de s'affranchir de la dispersion modale qui limite généralement les débits atteignables sur ce type de fibre ;
- il permet d'obfusquer (camoufler) physiquement les données transmises dans la fibre, grâce à l'injection de bruit dans des modes spatiaux d'ordre supérieur de la fibre, appelés « modes boucliers » ;
- il permet de détecter une intrusion physique sur la fibre optique, grâce à la mesure de la puissance optique transmise sur différents modes spatiaux d'ordre supérieur de la fibre, appelés « modes témoins ».

La figure ci-dessous explicite le déploiement du produit, avec les différentes interfaces des deux châssis et la fibre optique multimode terrain du client.

Figure 1 – Schéma de déploiement du 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*

Produit	
Nom du produit	KAKOMA
Numéro de la version évaluée	KAKOMA-10G-0M1 (REV 01), version du logiciel Java code software version S6.4.100

La version certifiée du produit est indiquée sur une étiquette en face arrière du rack 1U supérieur.

La version de logiciel embarqué est consultable dans le logiciel lui-même pour chaque châssis (menu « Application » > « Inventory »)

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la fonction d'obfuscation (camouflage) des données dans la fibre ;
- la fonction de détection d'intrusion sur la fibre.

1.2.4 *Configuration évaluée*

La plateforme de test est constituée de deux *full systems* (Alice et Bob sur la figure 1), connectés via un kilomètre de fibre multimode, auxquels a été ajouté un *full system* (Eve) pour mener les attaques d'intrusion. La version du produit évaluée est celle décrite en section 1.2.2, (à savoir KAKOMA-10G-0M1 (REV 01) dont la version du logiciel Java code *software* est S6.4.100).

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 [CDS].

2.3.1 *Installation du produit*

L'installation a été effectuée par le développeur.

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

La phase d'installation comporte les étapes décrites dans la cible de sécurité [CDS]. En particulier, le câblage des châssis, l'épissage des fibres optiques multimodes et la calibration doivent être réalisées par une personne de CAILABS (ou formée par CAILABS). Du point de vue de l'utilisateur, le système est une configuration transparente.

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

Sans objet.

2.3.1.3 Durée de l'installation

L'installation dure une demi-journée, mais varie en fonction de la facilité d'inspection de la fibre multimode précédemment installée.

2.3.1.4 Notes et remarques diverses

Sans objet.

2.3.2 *Analyse de la documentation*

Dans le cadre de cette évaluation, l'évaluateur a eu accès aux documents : [KAK_UM_v2.3], [KAK_ADVUM_v1.1], [CDS], [KAK_NOIS_v1.0].

Les guides du produit permettent d'utiliser le produit sans causer de dégradation accidentelle de la sécurité. Néanmoins, les administrateurs réseau doivent faire particulièrement attention à ne pas modifier les paramètres de sécurité qui sont essentiels pour assurer la sécurité du système. Le manuel d'utilisation [KAK_UM_v2.3] met l'accent sur les paramètres de sécurité critiques. Il y a

suffisamment d'avertissements pour qu'un utilisateur régulier ne puisse pas manquer les paramètres critiques.

2.3.3 *Revue du code source (facultative)*

Le code source n'a pas fait l'objet d'une revue dans le cadre de cette l'évaluation.

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 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

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.7.2 Avis d'expert sur la facilité d'emploi

Le système est simple à utiliser une fois l'installation terminée.

2.3.7.3 Notes et remarques diverses

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

2.4 Analyse de la résistance des mécanismes cryptographiques

Le produit n'implémente pas de mécanismes cryptographiques.

2.5 Analyse du générateur d'aléas

Le produit n'implémente pas de générateur d'aléas.

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 « KAKOMA, version KAKOMA-10G-0M1 (REV 01), version du logiciel Java code software version S6.4.100 » 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]. Cela implique qu'un audit approfondi de la fibre doit être effectué avant l'installation afin de vérifier qu'une intrusion n'existe pas déjà entre les deux zones sécurisées.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de Sécurité CSPN – KAKOMA Référence : CLB-AOR-2020-11-02-01-v06 ; Révision : 1.6 ; Date : 4 juin 2021. Cible publique : Cible de sécurité CSPN – Kakoma Référence : CLB-AOR-2020-11-02-01-v07 ; Révision 1.7 ; 16 juillet 2021.
[RTE]	*CSPN Evaluation Technical Report - KAKOMA* Référence : LETI.CESTI.KAK.ETR.001 ; Version : v1.1 ; Date : 21 juin 2021.
[GUIDES]	Guides utilisateur : [KAK_UM_v2.3] : Kakoma: manuel d'utilisation, référence CLB-AOR-2020-10-14-02-v03, version 2.3, 4 juin 2021. [KAK_ADVUM_v1.1] : Kakoma: utilisation avancée, référence CLB-AOR-2020-08-16-01, version 1.1, 7 septembre 2020. [KAK_NOIS_v1.0] : Kakoma: génération du bruit d'obfuscation, référence CLB-AOR-2020-08-05-01, version 1.0, 5 août 2020.

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.