PREMIER MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CSPN-2024/01

Jizô

Version 12.04.02

Paris, le 04 Avril 2024

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

Vincent STRUBEL

[ORIGINAL SIGNE]

SÉCURITÉ Ti 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-2024/01**
Nom du produit **Jizô**
Référence/version du produit **Version 12.04.02**
Catégorie de produit **Détection d'intrusions**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **SESAME IT** 124 Bd de la République 92210 Saint-Cloud, France
Développeur **SESAME IT** 124 Bd de la République 92210 Saint-Cloud, France
Centre d'évaluation **LEXFO** 5 rue Saulnier 75009 Paris
Fonctions de sécurité évaluées Chiffrement Identification, authentification et contrôle d'accès Mise à jour des logiciels Mise à jour de règles de détection Journalisation de fonctionnement Protection des flux Activation/désactivation du stockage, de la remontée d'informations techniques complémentaires (fichiers extraits) nécessaires à la qualification d'incidents Cloisonnement Dimensionnement
Fonctions de sécurité non évaluées Sans objet
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 cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Jizô, Version 12.04.02 » développé par SESAME IT.

Ce produit est une solution logicielle de détection d'intrusion réseau (IDS) qui analyse le flux réseau, remonte des alertes et métadonnées et extrait des fichiers dans les flux.

La sonde Jizô :

- est connectée en dérivation derrière un ou plusieurs TAP(s) unidirectionnel(s) et un chiffreur sur le réseau à surveiller ;
- possède 6 interfaces de capture, pour un débit maximal de 12 Gbps ;
- est opérée et administrée via 8 profils utilisateurs ;
- met à la disposition de certains profils des alarmes, journaux, alertes et statistiques ;
- propose également quelques fonctionnalités métiers.

La figure ci-dessous explicite l'environnement d'utilisation du produit.

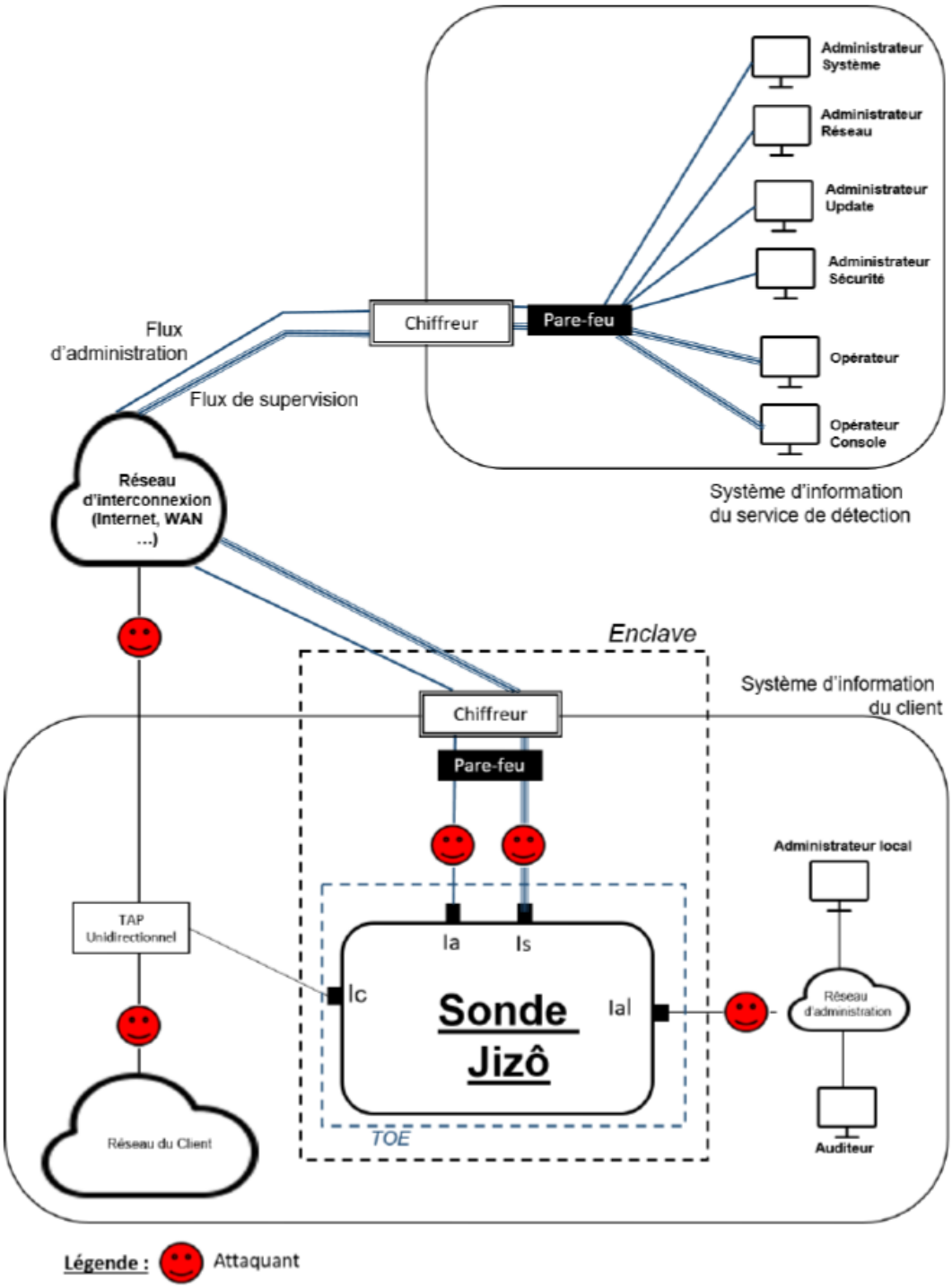

Figure 1 – Environnement d'utilisation du produit.

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	Jizô
Numéro de la version évaluée	Version 12.04.02

La version certifiée du produit peut être identifiée avec le compte de l'administrateur système « adminsys » et la commande « version » (seul l'administrateur est en mesure d'identifier la version du produit) :

```
0 Adminsys>version
Probe V12.4.02, updated at 20/11/2023
| Alert Pusher        | V4.0.1  | ea39be447c5530c9538a8422ef9a5601  | 20/11/2023
| Stat Aggregator     | V3.0.0  | 7efcd458ae9e02745fd6e1f38433c564  | 20/11/2023
| IDS Rule Manager    | V3.0.1  | 16e9b16de264c302f007f2da8326608a  | 20/11/2023
| IDS-DPI             | V       | 73bd9ba2726e1d18f322e8a35e51027c  | 20/11/2023
| Files Analyser      | V2.1.0  | 6323dedace359dd28cf6334fe8fa6072  | 20/11/2023
| DPI Pusher          | V3.3.0  | 6252696b09fec90f9886277ddbaa0724  | 20/11/2023
| Alarm Generator     | V3.2.0  | 37cf119da53acf90121556e23a14aff3  | 20/11/2023
| SFTP                | V3.1.0  | e3799418288a00cf4c85c64f1e66a51e  | 20/11/2023
| IDS Log             | V1.0.0  |                                   | 15/09/2018
| System Log          | V1.0.0  |                                   | 15/09/2018
| Rule Console        | V2.5.4 - SLib| c00277acc3f29c56cd79f60940f295d0  | 20/11/2023
| Admin Console       | V2.1.0  | 35e65f0bc4d7851aa19bb42dd429db80  | 20/11/2023
1 Adminsys>
```

Figure 2 – Identification de la version du produit.

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- le chiffrement du système de fichiers ;
- l'identification, l'authentification et le contrôle d'accès ;
- la mise à jour des logiciels ;
- la mise à jour de règles de détection ;
- la journalisation de fonctionnement ;
- la protection des flux ;
- l'activation/désactivation du stockage, de la remontée d'informations techniques complémentaires (fichiers extraits) nécessaires à la qualification d'incidents ;
- le cloisonnement ;
- le dimensionnement.

1.2.4 *Configuration évaluée*

La configuration évaluée et la plateforme de test sont conformes à [NOTE-05], qui exige en particulier la fourniture pour l'évaluation d'une sonde en version « production » et d'une sonde en version « développeur ».

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et aux dispositions de [NOTE-05].

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

L'installation des deux sondes (sonde en version « production » et sonde en version « développeur ») est réalisée en présence du développeur et comporte les étapes suivantes :

- Raccordement, branchement réseau ;
- Configuration réseau via l'utilisateur Administrateur Réseau, en SSH avec la commande « ip » ;
- Dépôt et activation d'une configuration VPN entre la sonde et l'ordinateur dédié à l'administration.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *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.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source :

- des programmes internes, développés en C++ ;
- de divers scripts en *bash* ;
- de l'interface web 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

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

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

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

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

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur familier.

La sonde en elle-même est simple d'emploi, celle-ci ne proposant qu'une interface limitée. Il y a plusieurs utilisateurs (4 en mode console et 3 sur les interfaces web). Les rôles sont bien séparés et chacun n'a que quelques commandes à sa disposition. Les documentations mises à disposition permettent d'utiliser correctement ces commandes et interfaces.

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 comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

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.

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 « Jizô, Version 12.04.02 » 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].

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - SESAME IT – JIZÔ – Sonde de détection des incidents de sécurité – Cible de sécurité, référence Profil de protection CSPN SESAME IT V12 - 2024, version 12, 19 février 2024.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN – *Solution Jizô – Sesame it,* référence SES20231127, version 1.3, 22 février 2024.
[GUIDES]	Guides d'utilisation, d'administration et d'installation du produit : - Sonde Jizô – *User Guide – Operator Console*, réf. 20240215-User Guide Operator Console.pdf ; - Sonde Jizô – *User Guide – Jizô System Administrator*, réf. 20240215- User Guide Jizô System Administrator.pdf ; - Sonde Jizô – *User Guide – Jizô Network Administrator*, réf. 20221012003-A- User Guide Jizô Network Administrator.pdf ; - Sonde Jizô – *User Guide – Jizô Local Administrator*, réf. 20240215- User Guide Jizô Local Administrator.pdf ; - Sonde Jizô – *User Guide – Jizô Security Administrator*, réf. 20221012005-B-User Guide Security Administrator.pdf ; - Sonde Jizô – *User Guide – Administrator Update*, réf. 20221012001-A-User Guide Administrator Update.pdf ; - Sonde Jizô – *User Guide – Jizô Operator*, réf. 20221012007-B-User Guide Operator.pdf ; - Sonde Jizô – *User Guide – Jizô Auditor*, réf. 20240215-User Guide Auditor.pdf ; - Jizô – *USB Key Usage Information Note*, réf. 20220915001 -A- USB Key Usage Information Note.pdf.

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.
[NOTE-05]	Note d'application - Méthodologie pour l'évaluation des sondes réseau sur base Linux de détection d'intrusion en vue d'une certification de sécurité de premier niveau pour une qualification selon le décret 2015/350, référence ANSSI-CSPN-NOTE-05, version 2.0, 28 juin 2020.