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-2024/03

Logiciel single-tenant Ého.Link en tant que service (SaaS) en hébergement Cloud privé sur socle PaaS

Version Ého.box EHOLINK_A2.2 avec software version 22.02.0.5, Ého.my version 24.03.0.1, Ého.cloud version 22.03.1.1

Paris, le 02 Juillet 2024

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

Emmanuel NAEGELEN

[ORIGINAL SIGNE]

SÉCURITÉ 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-2024/03

Nom du produit

Logiciel single-tenant Ého.Link en tant que service (SaaS) en hébergement Cloud privé sur socle PaaS

Référence/version du produit

Version Ého.box EHOLINK_A2.2 avec software version 22.02.0.5, Ého.my version 24.03.0.1, Ého.cloud version 22.03.1.1

Catégorie de produit

Administration et supervision de la sécurité

Critère d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

EHO.LINK
67, Montée de Saint-Menet
13011 Marseille, France

Développeur

EHO.LINK
67, Montée de Saint-Menet
13011 Marseille, France

Centre d'évaluation

OPPIDA
4-6 avenue du vieil étang, Bâtiment B
78180 Montigny le Bretonneux, France

Fonctions de sécurité évaluées

Bootloader sécurisé
Filtrage réseau
Génération de journaux d'évènements
Administration sécurisée à distance
Communications sécurisées
Mise à jour de la base de signatures
Mise à jour du *firmware*
Protection des clés
Authentification
Contrôle d'accès données globales bénéficiaires

Fonctions de sécurité non évaluées

Détection d'intrusion en tant que mécanisme
Auto-découverte des équipements connectés sur le réseau du bénéficiaire
Contrôle d'accès réseau

Restriction(s) d'usage

Non

Préface

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 « Logiciel single-tenant Ého.Link en tant que service (SaaS) en hébergement Cloud privé sur socle PaaS, Version Ého.box EHOLINK_A2.2 avec software version 22.02.0.5, Ého.my version 24.03.0.1, Ého.cloud version 22.03.1.1 » développé par EHO.LINK.

Ce produit est une solution d'administration et de supervision de la sécurité d'un système d'information, accessible aux petites et moyennes entreprises, et permettant :

- la détection des équipements connectés ;
- l'analyse de l'activité sur le réseau privé ;
- l'administration de l'utilisation d'Internet ;
- le stockage de données dans un *Cloud* personnel.

La solution Eho.link est composée des trois éléments suivants :

- Eho.box : boitier en coupure du réseau externe ;
- Eho.cloud : service de *Cloud* personnel
- Eho.my : portail web pour accès à Internet et/ou au *Cloud*.

La solution est accessible via le boîtier (Eho.box) branché après le routeur sur le réseau interne à protéger et qui nécessite une authentification sur une page web par utilisateur et permet en plus l'accès à un *Cloud* personnel, lui-même accessible depuis l'extérieur via l'authentification sur la même page web.

La figure ci-dessous explicite l'architecture du produit.

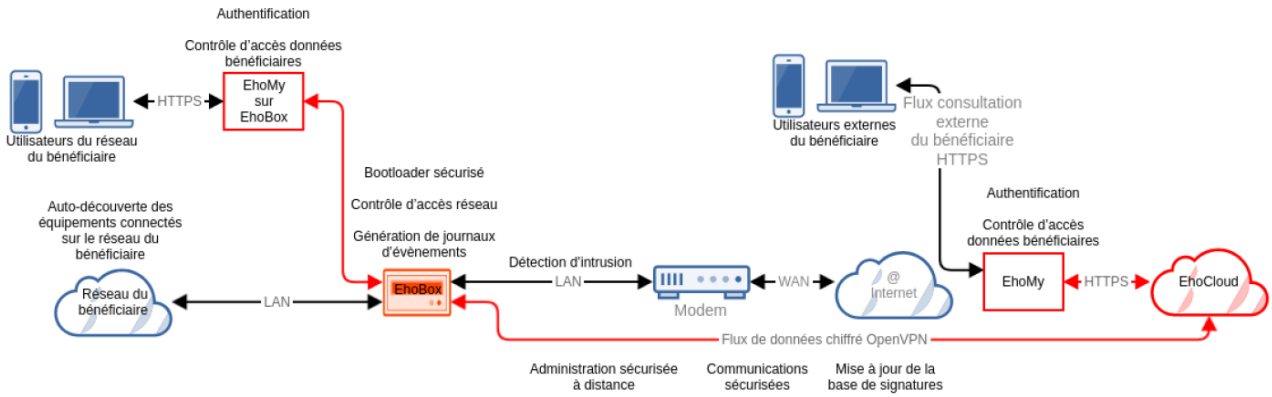


Figure 1 - Architecture Produit.

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*

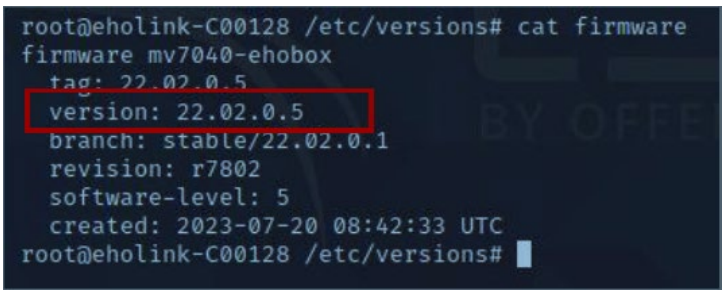
☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☒	**5**	**administration et supervision de la sécurité**
☐	6	identification, authentification et contrôle d'accès
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	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*

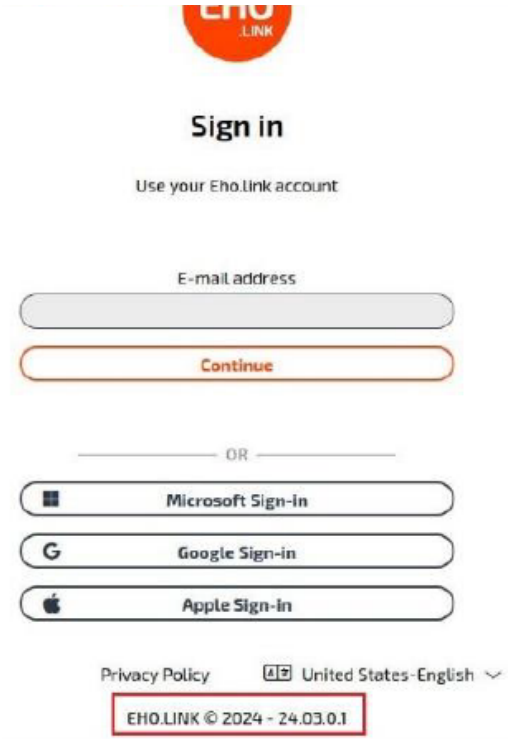
Produit	
Nom du produit	Logiciel single-tenant Ého.Link en tant que service (SaaS) en hébergement Cloud privé sur socle PaaS
Numéro de la version évaluée	Version Ého.box EHOLINK_A2.2 avec software version 22.02.0.5, Ého.my version 24.03.0.1, Ého.cloud version 22.03.1.1

La version certifiée du produit peut être identifiée de la manière suivante :

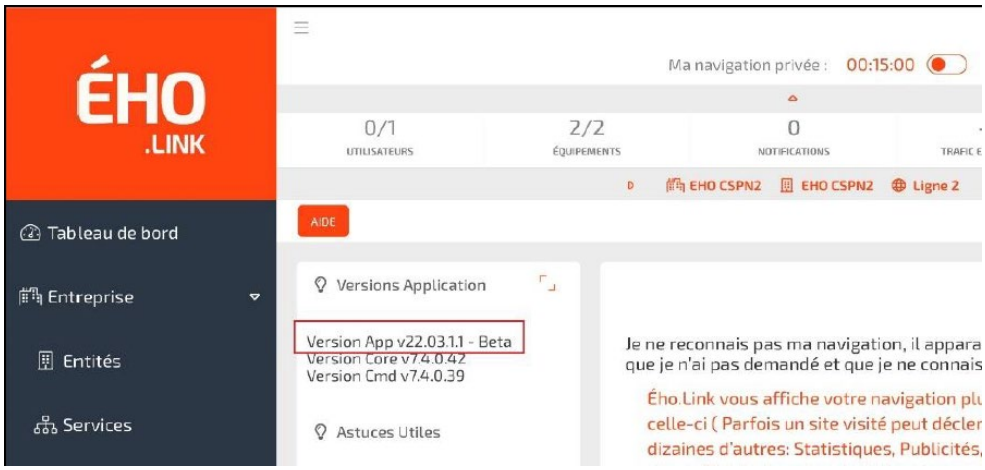
- **Ého.box** : effectuer une connexion ssh à Ého.box et afficher le contenu du fichier /etc/versions/firmware :



- **Ého.my** : afficher la page d'accueil du portail web :



- **Ého.cloud** : se connecter au portail web et afficher la page d'aide :



1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- le *bootloader* sécurisé ;
- le filtrage réseau ;
- la génération de journaux d'évènements ;
- l'administration sécurisée à distance ;
- les communications sécurisées ;
- la mise à jour de la base de signatures ;
- la mise à jour du *firmware* ;
- la protection des clés ;
- l'authentification des utilisateurs ;
- le contrôle d'accès aux données globales des bénéficiaires.

1.2.4 *Configuration évaluée*

La plateforme de test est constituée :

- du boitier Ého.box, placé en coupure du réseau interne et du réseau externe du bénéficiaire ;
- de la partie Ého.cloud, qui est supportée par un ordinateur paramétré et fourni par le 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-06].

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

Comme exigé par [NOTE-06], l'installation de la partie Eho.cloud a bien été réalisée en local par le CESTI, même si la cible de sécurité [CDS] vise un déploiement sur un service Cloud commercial.

2.2.1.3 Notes et remarques diverses

L'installation du produit est simple et ne nécessite aucun paramétrage.

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.

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

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].

2.2.7 *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 a identifié des non-conformités par rapport au référentiel. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont 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 « Logiciel single-tenant Ého.Link en tant que service (SaaS) en hébergement Cloud privé sur socle PaaS, Version Ého.box EHOLINK_A2.2 avec software version 22.02.0.5, Ého.my version 24.03.0.1, Ého.cloud version 22.03.1.1 » 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].

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité Ého.Link, référence 2024_05_07_EHOLINK_CS_V2.5, version 2.5, 7 mai 2024.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN - Logiciel single tenant Ého.Link en tant que service (SaaS) En hébergement Cloud privé sur socle PaaS - MARLEY2, référence OPPIDA/CESTI/2023/MARLEY2/RTE, version 1.7, 27 mai 2024.
[GUIDES]	Guides d'installation du produit : - https://eho.link/documentation

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-06]	Note d'application - Méthodologie d'évaluation CSPN pour les logiciels déployés sur des infrastructures de *cloud computing*, référence ANSSI-CSPN-NOTE-06, version 1.0, 2 mars 2021.