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-2025/17

VirtualBrowser

Version 4.0.9, on-premise, déploiement « single »

Paris, le 16/12/2025 | 12:32 CET

Vincent Strubel

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-2025/17

Nom du produit

VirtualBrowser

Référence/version du produit

Version 4.0.9, on-premise, déploiement « single »

Catégorie de produit

Communication sécurisée

Critère d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

VirtualBrowser SAS
18 rue de Miromesnil
75008 Paris, France

Développeur

VirtualBrowser SAS
18 rue de Miromesnil
75008 Paris, France

Centre d'évaluation

AMOSSYS
11 rue Maurice Fabre
35000 Rennes, France
12 rue du Bourg Nouveau
35000 Rennes, France

Accord de reconnaissance applicable

fixed time certification

Ce certificat est reconnu dans le cadre du [BSZ_CSPN]

Fonctions de sécurité évaluées

Identification et authentification du bénéficiaire
Contrôle d'accès et gestion des droits/privilèges entre utilisateurs appartenant au bénéficiaire
Communications sécurisées
Protection des données incluant l'effacement sécurisé
Journalisation
Innocuité
Autoprotection

Fonctions de sécurité non évaluées	Mise à jour Catégorisation des URLS Authentification par certificat client
Restriction(s) d'usage	Oui

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 « VirtualBrowser, Version 4.0.9, on-premise, déploiement « single » » développé par VirtualBrowser SAS.

Ce produit est une solution de navigation déportée *(Remote Browser Isolation)* visant à protéger de manière proactive le poste de l'utilisateur en isolant physiquement son activité de navigation.

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)

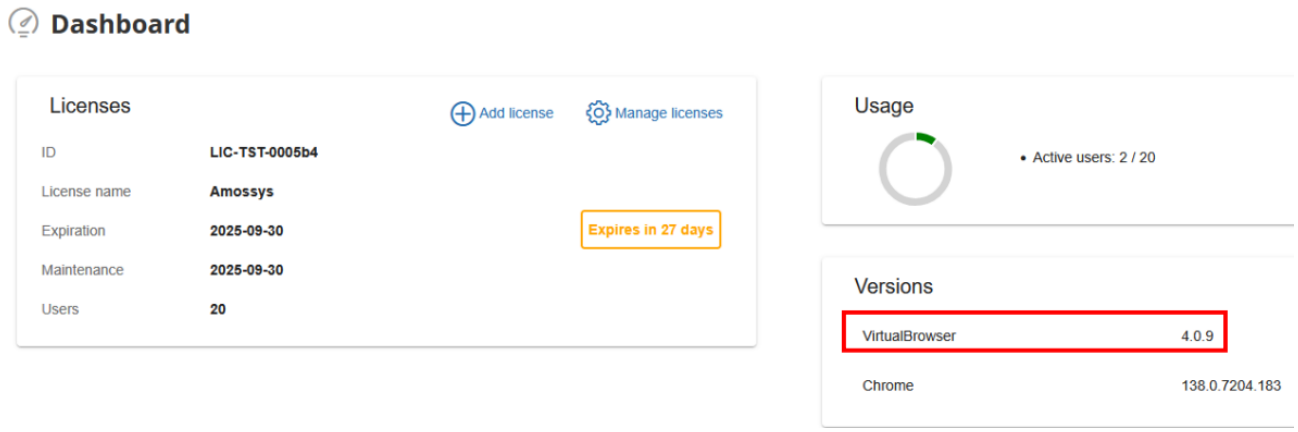
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	VirtualBrowser
Numéro de la version évaluée	*Version 4.0.9, on-premise, déploiement « single »*

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

- La version est disponible depuis l'interface d'administration :



1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- Identification et authentification du bénéficiaire
- Contrôle d'accès et gestion des droits/privilèges entre utilisateurs appartenant au bénéficiaire
- Communications sécurisées
- Protection des données incluant l'effacement sécurisé
- Journalisation
- Innocuité
- Autoprotection

1.2.4 *Configuration évaluée*

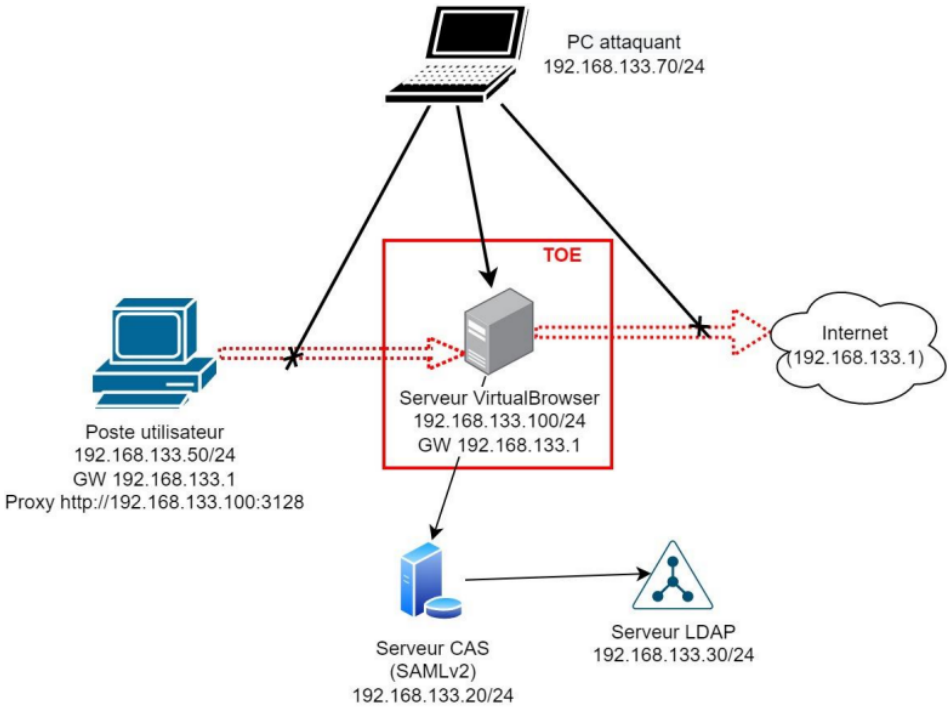
La configuration évaluée correspond à :

-Le navigateur web Firefox a été configuré pour utiliser la TOE en tant que proxy HTTP et HTTPS.

-Le serveur VirtualBrowser a été déployé sur une machine Ubuntu 22.04. La plateforme de virtualisation utilisée est Proxmox

-Lors de l'évaluation initiale, des machines Linux Debian 12 ont été utilisées pour déployer les serveurs CAS et LDAP.

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].

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

Pour réaliser l'installation, l'évaluateur a suivi la documentation en ligne fournie par le développeur. Toutes les étapes y sont décrites pour que l'intégrateur ne fasse pas d'erreurs pour installer le produit en mode proxy. L'installation doit être réalisée par un administrateur qui a accès en local à une VM basée sur le fichier OVA fourni par le développeur. L'évaluateur a suivi scrupuleusement chaque étape indiquée dans la documentation.

2.2.1.3 Notes et remarques diverses

Seule le déploiement « single » a été évalué et testé et non le déploiement *« cluster »* proposé également par le développeur.

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

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables 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

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.

2.2.7.3 Notes et remarques diverses

Certains flux au sein de la TOE sont en clairs. Cependant il n'a pas été identifié de scénario ou un attaquant pourrait intercepter ces communications.

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 [ANA_CRY].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. 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 « VirtualBrowser, Version 4.0.9, on-premise, déploiement « single »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

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].

3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ *(Beschleunigte Sicherheitszertifizierung* ou Certification de sécurité accélérée).

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - CIBLE DE SECURITE DU LOGICIEL *SINGLE-TENANT VIRTUALBROWSER* EN TANT QUE SERVICE (SAAS) VERSION 4.0.9 EN HEBERGEMENT *ON-PREMISE,* référence CSPN-CDS-VirtualBrowser-1.05, version 1.05, 6 août 2025 Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - CIBLE DE SECURITE DU LOGICIEL *SINGLE-TENANT VIRTUALBROWSER* EN TANT QUE SERVICE (SAAS) VERSION 4.0.9 EN HEBERGEMENT *ON-PREMISE,* référence CSPN-CDS-VirtualBrowser-1.07, version 1.07, 8 décembre 2025
[RTE]	Rapport technique d'évaluation : - RAPPORT TECHNIQUE D'EVALUATION CSPN VIRTUAL BROWSER VERSION 4.0.9, référence CSPN-RTE-BOWSER2-2.10, version 2.10, 12 novembre 2025
[ANA_CRY]	Rapport d'expertise cryptographique : - EXPERTISE DES MECANISMES CRYPTOGRAPHIQUES VIRTUAL BROWSER VERSION 4.0.9, référence CSPN-CRY-BOWSER2-2.00, version 2.00, 9 octobre 2025
[GUIDES]	Guide d'installation du produit : VirtualBrowser 4.0 – Guide d'installation serveur, version 2025-08-r1 du 31/07/2025 Guide d'administration du produit : - VirtualBrowser 4.0 – Guide d'administration, version 2025-08-r1 du 01/08/2025 Guide d'utilisation du produit : - VirtualBrowser 4.0 – Guide d'utilisation, version 2025-08-r1 du 29/07/2025

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 5.0, 12 juillet 2024. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 4.0, 12 juillet 2024.
[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.
[BSZ_CSPN]	*Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI,* référence *bsz_cspn_mutual_recognition_agreement,version* 2.0, mai 2024.