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-2022/01

PEXIP Infinity On Premise

Version 26.2

Paris, le 27 janvier 2022

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

Guillaume POUPARD

[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 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-2022/01**
Nom du produit	**PEXIP Infinity On Premise**
Référence/version du produit	**Version 26.2**
Catégorie de produit	**Communication sécurisée**
Critère d'évaluation et version	**CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire	**PEXIP** 195 avenue Charles de Gaulle 92200 Neuilly-sur-France
Développeur	**PEXIP** 195 avenue Charles de Gaulle 92200 Neuilly-sur-France
Centre d'évaluation	**LEXFO** 5 rue Drouot 75009 Paris, France
Fonctions de sécurité évaluées	Authentification administrateur système Authentification administrateur applicatif Intégrité et chiffrement des échanges client/serveur Intégrité et chiffrement des échanges client/client Cloisonnement des salles virtuelles Accès aux salles contrôlé par un code PIN Intégrité et chiffrement des échanges serveur/serveur
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 www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « PEXIP Infinity On Premise, Version 26.2 » développé par PEXIP.

Ce produit est une solution de vidéoconférence sécurisée.

L'infrastructure sur laquelle repose la solution est basée sur des machines virtuelles pouvant être déployées soit *on premise* sur des serveurs ou chez des hébergeurs *Cloud* tierce partie. Seul le déploiement *on premise* est considéré dans le cadre de ce certificat.

Cette infrastructure se compose :

- d'un *Management node* permettant de piloter l'ensemble de la solution ;
- d'un ou plusieurs *Conference nodes* qui peuvent :
    - héberger et offrir les fonctionnalités de conférence de la solution (*transcoding node*), ou :
    - avoir un rôle de *proxyfication* des flux (*proxying node*).

Dans le cadre du présent certificat, les conférences sont joignables uniquement par client léger sur navigateur web. D'autres configurations, non évaluées, permettent de rejoindre les conférences par client lourd, applications mobiles, terminaux de vidéoconférence SIP ou H.323, téléphone, ou encore interconnexion avec des solutions tierces telles que Microsoft Teams ou Google Meet.

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.

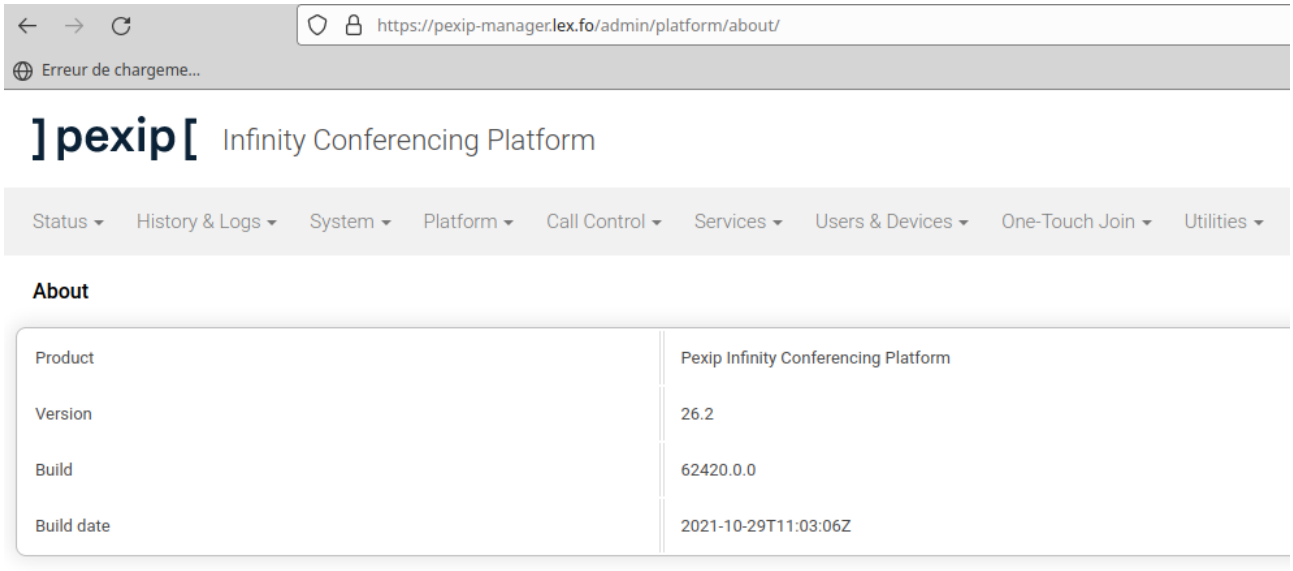
1.2.1 *Catégorie du produit*

☐	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	PEXIP Infinity On Premise
Numéro de la version évaluée	Version 26.2

La version de la solution est identifiée en se connectant à l'interface d'administration :



1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'authentification de l'administrateur système ;
- l'authentification de l'administrateur applicatif ;
- l'intégrité et le chiffrement des échanges client/serveur ;
- l'intégrité et le chiffrement des échanges client/client ;
- le cloisonnement des salles virtuelles ;
- l'accès aux salles contrôlé par un code PIN ;
- l'intégrité et le chiffrement des échanges serveur/serveur.

1.2.4 *Configuration évaluée*

L'évaluation considère la solution PEXIP Infinity dans un déploiement *on premise*, avec accès via client léger sur navigateur. Les différentes interconnexions avec les solutions telles que Microsoft Teams, Google Meet, les équipements de visioconférence de salle ne sont pas inclus dans l'évaluation.

La configuration évaluée est un déploiement de la solution sur KVM.

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.

L'installation a été effectuée en suivant le guide d'installation et le guide de sécurisation du produit (voir [GUIDES]).

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

Sans objet

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 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 pour le niveau d'attaquant considéré et 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 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 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 « PEXIP Infinity On Premise, Version 26.2 » 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]. En particulier, comme l'indique le guide *Security best practices*, l'utilisateur doit mettre en œuvre un pare-feu pour que seuls les personnels autorisés puissent avoir accès aux interfaces de management (identifiées dans la section *Administration access* du guide *Pexip Infinity port usage and firewall guidance)*.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité CSPN PEXIP Infinity, référence PEX20210827, version 1.1, 21 janvier 2022.
[RTE]	Rapport technique d'évaluation : - Rapport technique - Évaluation CSPN Solution PEXIP Infinity, référence PEX20211223, version 1.3, 21 janvier 2022. - Lexfo – Analyse des mécanismes cryptographiques – Evaluations CSPN - Référence CRY20220118, version 1.2, 18 janvier 2022.
[GUIDES]	Guide d'installation du produit : *Installing Pexip Infinity in a KVM environment*, accessible en ligne à l'adresse https://docs.pexip.com/getting_started/gs_kvm.htm, accédé le 21 janvier 2022 Guide de sécurisation du produit : - *Security best practices*, accessible en ligne à l'adresse https://docs.pexip.com/admin/security_best_practice.htm, accédé le 21 janvier 2022, et - *Pexip Infinity port usage and firewall guidance*, accessible en ligne à l'adresse https://docs.pexip.com/admin/port_usage.htm, accédé le 21 janvier 2022

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 3.0, 12 avril 2021. 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.
[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.