PREMIÈRE 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-2022/12

TixeoServer

Serveurs TMMS/TCS et clients TCC, version 16.6.2.3

Paris, le 10 Février 2023

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

Vincent STRUBEL

[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-2022/12**
Nom du produit **TixeoServer**
Référence/version du produit **Serveurs TMMS/TCS et clients TCC, version 16.6.2.3**
Catégorie de produit **Communication sécurisée**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **TIXEO SARL** 244, rue Claude François 34080 Montpellier
Développeur **TIXEO SARL** 244, rue Claude François 34080 Montpellier
Centre d'évaluation **AMOSSYS** 11 rue Maurice Fabre 35000 Rennes
Fonctions de sécurité évaluées Chiffrement de bout en bout dans un tunnel TLS Protection des mots de passe des utilisateurs Authentification des utilisateurs HTTPS Tunneling
Fonctions de sécurité non évaluées Néant
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 www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit 6
1.1 Présentation du produit 6
1.2 Description du produit évalué 7
1.2.1 Catégorie du produit 7
1.2.2 Identification du produit 7
1.2.3 Fonctions de sécurité 7
1.2.4 Configuration évaluée 7
2 L'évaluation 9
2.1 Référentiels d'évaluation 9
2.2 Travaux d'évaluation 9
2.2.1 Installation du produit 9
2.2.2 Analyse de la documentation 9
2.2.3 Revue du code source (facultative) 9
2.2.4 Analyse de la conformité des fonctions de sécurité 9
2.2.5 Analyse de la résistance des mécanismes des fonctions de sécurité 9
2.2.6 Analyse des vulnérabilités (conception, construction, etc.) 10
2.2.7 Analyse de la facilité d'emploi 10
2.3 Analyse de la résistance des mécanismes cryptographiques 10
2.4 Analyse du générateur d'aléas 10
3 La certification 11
3.1 Conclusion 11
3.2 Recommandations et restrictions d'usage 11
ANNEXE A. Références documentaires du produit évalué 12
ANNEXE B. Références liées à la certification 13

1 Le produit

1.1 Présentation du produit

Le produit évalué est « TixeoServer, Serveurs TMMS/TCS et clients TCC, version 16.6.2.3 » développé par [TIXEO SARL].

Le produit TixeoServer est un système de vidéo conférence à installer en interne chez le client. Il propose en plus de la communication voix, vidéo en multipoints, des fonctions de partage d'écran et de transfert de fichiers.

Il se compose de 3 éléments :

- le serveur TMMS (*Tixeo Meeting Management Server*), en charge de la gestion des utilisateurs, des réunions et de l'authentification ;
- le serveur TCS (*Tixeo Communication Server*), en charge de la gestion des communications temps réels, flux audio, vidéo et *data* pendant les réunions ;
- le client TCC (*Tixeo Communication Client*), qui est le logiciel côté utilisateur qui permet d'organiser, rejoindre et participer à des réunions en ligne.

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

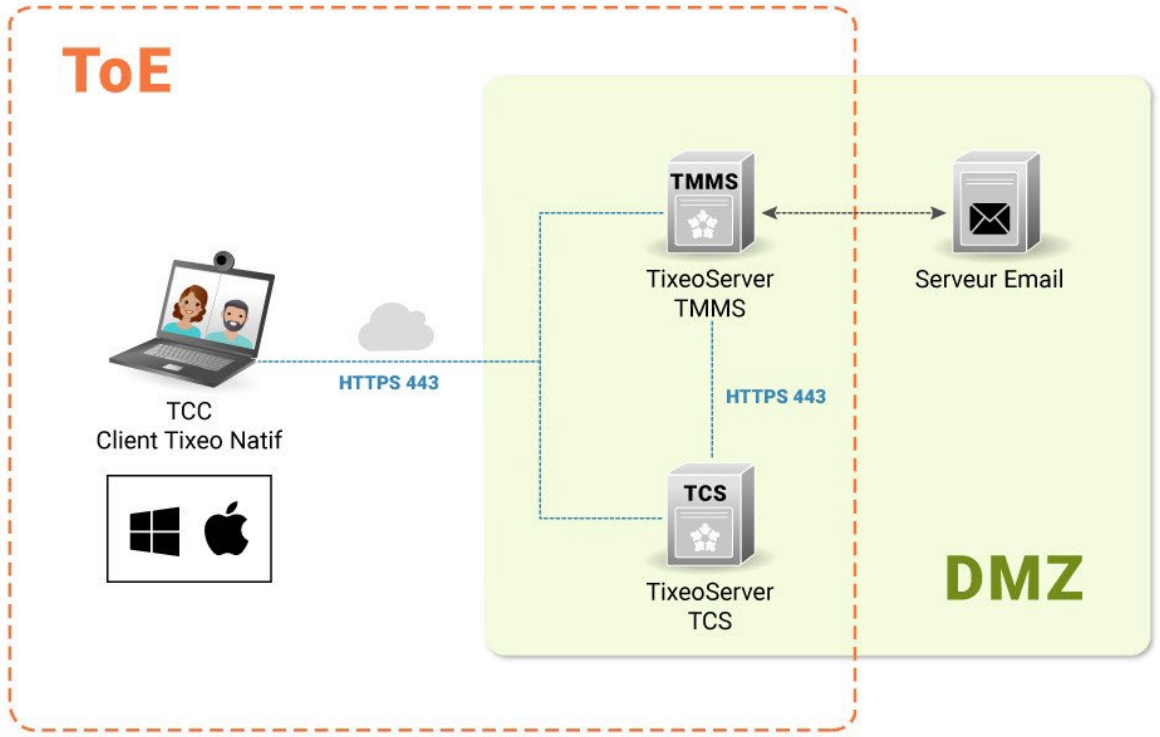

Figure 1 - Architecture Produit.

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	TixeoServer
Numéro de la version évaluée	Serveurs TMMS/TCS et clients TCC, version 16.6.2.3

La version du produit peut être vérifiée comme suit
- Pour le serveur TMMS, dans le répertoire *[TixeoServerDir]\Tomcat\webapps\meet\WEB-INF\classes\VERSION.TXT* (voir §3.1 du guide d'administration [GUIDES]) ;
- Pour le serveur TCS, depuis l'interface web du TMMS, en passant la souris au-dessus du TCS (voir §3.4.1 du guide d'administration [GUIDES]) ;
- Pour les clients TCC, dans le fichier VERSION.TXT (voir §4.10 du guide d'administration [GUIDES]).

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :
- le chiffrement de bout en bout dans un tunnel TLS ;
- la protection des mots de passe des utilisateurs ;
- l'authentification des utilisateurs ;
- le HTTPS *Tunneling*.

1.2.4 *Configuration évaluée*

Pour le déploiement de TixeoServer, il a été choisi d'utiliser une architecture à plusieurs serveurs. Plus précisément, les serveurs TMMS et TCS sont déployés sur des machines différentes.

La plateforme d'évaluation est composée :

- de trois serveurs et trois clients :
  - serveur TMMS sous Windows Server 2019 ;
  - serveur TCS sous Windows Server 2019 ;
  - serveur DNS/SMTP sous Windows Server 2019 ;
- des trois types de clients envisagés pour l'évaluation :
  - Client Ubuntu 20.04 ;
  - Client MacOS Catalina 10.15 ;
  - Client Windows 11.

La version évaluée utilise la fonctionnalité de *Certificate Pinning* (voir §3.2).

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 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*

L'installation a suivi la documentation fournie par le développeur.

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

Néant.

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] lors de l'évaluation. Cette documentation contient plusieurs sections en rapport avec le produit. Une description de son architecture et ses caractéristiques au niveau matériel, logiciel, réseau et sécurité sont présents. Un guide d'installation, de configuration et de maintenance permet de déployer et gérer le produit étape par étape.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source des mécanismes cryptographiques du produit. L'analyse a été effectuée manuellement.

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*

L'évaluateur a relevé des non-conformités sur les fonctions de sécurité testées, mais aucune n'a été considérée comme entraînant un problème de sécurité dans le contexte d'utilisation du produit.

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 et ses briques tierce partie, mais aucune n'a été considérée par l'évaluateur comme exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

En outre, certaines vulnérabilités publiques n'en sont pas au regard du problème de sécurité restreint que présente [CDS]. Le paragraphe 3.2 donne plus de détails à ce sujet.

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 dans le contexte d'utilisation du produit et pour le niveau d'attaquant considéré.

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

La prise en main et la maintenance du serveur pour un administrateur sont détaillées dans la documentation.

Dans le cas d'un client, il n'a pas été observé de situations où une mauvaise manipulation mettrait à mal la sécurité 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 le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité à [ANSSI Crypto] ni de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé.

L'analyse n'a pas identifié de non-conformité à [ANSSI Crypto] ni 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 « TixeoServer, Serveurs TMMS/TCS et clients TCC, version 16.6.2.3 » 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].

L'utilisateur doit également garder en mémoire que la cible de sécurité de cette évaluation porte sur un problème de sécurité restreint. Cela entraîne les restrictions d'usage suivantes :

- Comme le signale la cible de sécurité [CDS] :
  - une compromission du TCS serait de nature à menacer le chiffrement de bout-en-bout de l'intégralité des flux ; l'utilisateur doit donc prendre une précaution particulière dans la protection de ce serveur,
  - le produit ne s'attache pas à protéger les métadonnées de réunion (sujet, date, durée, nom et mail de l'organisateur, ainsi que nom et mail des participants). Il est donc impératif pour les utilisateurs de ne pas inclure de données sensibles dans le sujet des réunions ;
- Comme le signale le guide d'administration [GUIDES]
  - Afin de s'assurer que le produit journalise les erreurs d'authentification, l'administrateur devra suivre le §4.12.1.1 pour passer en niveau de log INFO ;
  - l'administrateur devra suivre le § 1.5.4. pour
    - s'assurer que le *chat* textuel hors réunion est désactivé (fonction « Messages »), ainsi que la fonction « Donner le contrôle d'un partage »,
    - mettre en œuvre les fonctionnalités de *certificate pinning*, sur le TCS pour les communications entre serveurs, et sur les postes clients TCC pour les communications client-serveur. Idéalement, l'administrateur de sécurité devrait automatiquement déployer le *certificate pinning* sur les postes clients, en prenant en compte que ce *pinning* doit être effectué pour les communications avec les deux serveurs ;
- Comme le signale le guide d'administration [GUIDES], il est impératif de désactiver la fonctionnalité de stockage local des mots de passe utilisateur, ainsi que la fonctionnalité de stockage de mots de passe dans le navigateur *web*.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité CSPN TixeoServer Référence : sans ; Version : v221116 ; Date : sans.
[RTE]	Rapport technique d'évaluation : Rapport Technique d'Evaluation CSPN TixeoServer – version 16.6.2.3, référence CSPN-RTE-TixeoServer2-DR / TXO005, version 2.00, 5 octobre 2022.
[GUIDES]	TixeoServer - Admin guide Version : sans ; Date : décembre 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 4.0, 3 mars 2022. 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.