Cible de sécurité CSPN

TIXEO

www.tixeo.com

v161025

1 Sommaire

2 Introduction

2.1 Objet du document

Ce document a pour objet de définir la cible de sécurité dans le cadre de l'évaluation Certification Sécurité de Premier Niveau (CSPN).

Il concerne la solution de vidéo conférence TixeoServer v11.5.2.0 de Tixeo.

Il a été rédigé par Tixeo sur fonds propres.

2.2 Identification du produit

Editeur	Tixeo
Lien vers l'organisation	https://www.tixeo.com
Nom commercial du produit	TixeoServer
Numéro de la version évaluée	V11.5.2.0
Catégories de produit	Communication sécurisée

La version évaluée correspond à l'ensemble des éléments de la solution (TMMS, TCS, TCC Windows et TCC macOS). Tous les éléments de solution portent le même numéro de version.

3 Description du produit

3.1 Description générale

La solution 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. Le système est conçu pour offrir un fort niveau de confidentialité des communications.

Il se compose de 3 éléments :

- Le serveur TMMS (Tixeo Meeting Management Server) : Gestion des utilisateurs, des réunions et de l'authentification
- Le serveur TCS (Tixeo Communication Server) : Gestion des communications temps réels, flux audio, vidéo et data pendant les réunions
- Le client TCC (Tixeo Communication Client) : Logiciel coté utilisateur qui permet d'organiser, rejoindre et participer à des réunions en lignes.

Le client TCC ne nécessite l'ouverture d'aucun port en écoute et communique avec le TCS et le TMMS en HTTPS sur le port 443. De ce fait, l'intégrité des postes et la politique de sécurité réseau restent inchangés.

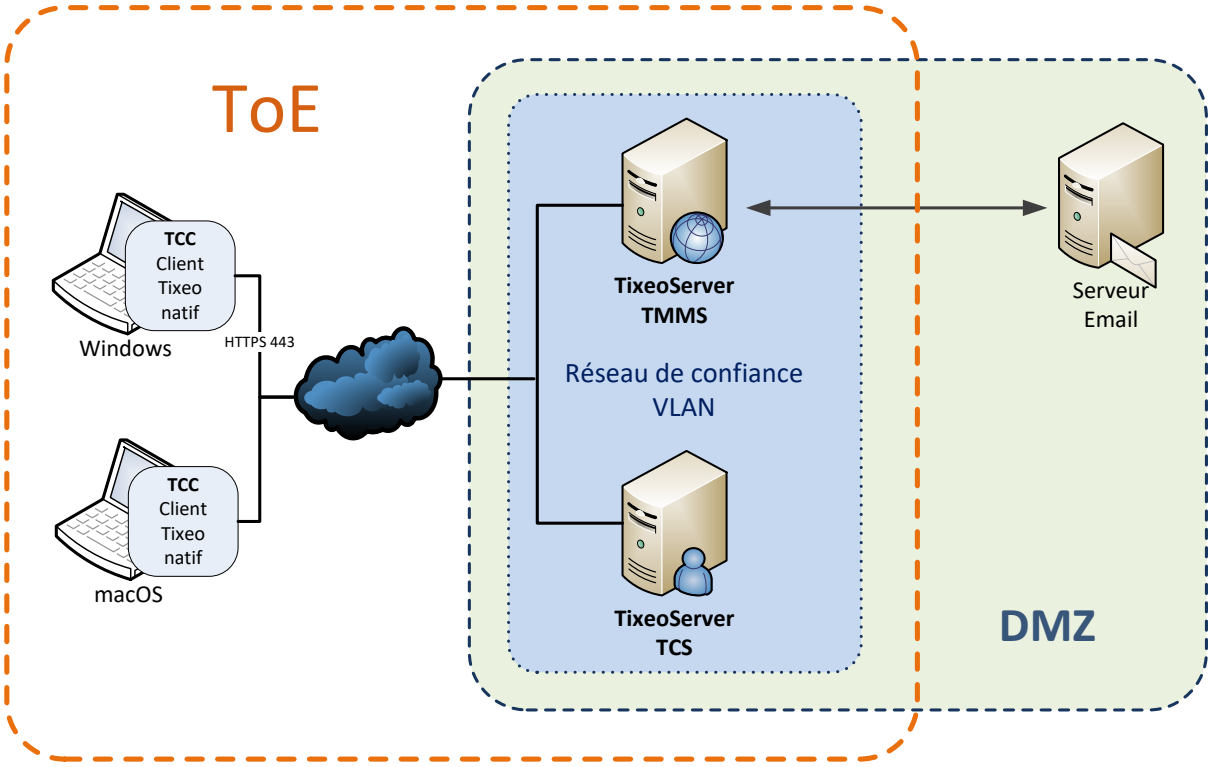

Fig.1 : Target of evaluation

3.2 Description de l'utilisation du produit

Lorsqu'un utilisateur est invité pour la première fois, il reçoit un email de validation de compte contenant un lien vers le server TMMS.

En cliquant sur ce lien, il valide son identité, confirme son nom et prénom, et choisi un mot de passe personnel.

Il est ensuite invité à installer le client Tixeo TCC. L'installation du client TCC se fait dans le profil local de l'utilisateur. Il n'a donc pas besoin de droit administrateur. Notez qu'il est possible de définir au travers de GPO (Stratégies de groupe) un emplacement d'installation différent.

A partir du TCC, l'utilisateur pourra rejoindre une réunion à laquelle il est invité. S'il en a les droits (définis par l'administrateur sur le serveur TMMS), il pourra également organiser des réunions.

Tout utilisateur de la solution, quel que soit son rôle (simple utilisateur, organisateur ou administrateur) doit s'authentifier sur le TMMS en utilisant ses identifiants (email et mot de passe).

Une fois connecté dans une réunion (hébergée par le serveur TCS), l'utilisateur peut communiquer en voix et vidéo. Si l'organisateur (modérateur) de la réunion l'y autorise, il pourra également partager des documents en faisant un partage d'écran.

La confidentialité des communications en réunion est assurée par deux chiffrements, un chiffrement de lien du TCC vers le TCS, et un chiffrement de bout en bout entre les différents clients TCC connectés à la réunion (cf. Fourniture Crypto - Tixeo).

3.3 Description de l'environnement prévue pour son utilisation

Le client TCC fonctionne dans les environnements Windows XP SP3, Vista, 7, 8, 8.1, 10 ainsi que sous macOS Sierra 10.12.

Afin de pouvoir communiquer en voix et vidéo, le client TCC nécessite une webcam et un microphone.

Les serveurs TMMS et TCS sont installés dans des environnements Windows Server 2008 r2, 2012.

3.4 Description des hypothèses sur l'environnement

3.4.1 Environnement logique

Le client TCC, le serveur TMMS et le serveur TCS, doivent être intègres et signés par Tixeo (« Thawte Code Signing Certificate pour Windows » et « Apple Developer ID Certificarte » pour macOS). Ils doivent être installés sur des OS sains et à jours des correctifs de sécurité. Les éléments logiciels dont ils dépendent doivent également être sains et à jours des correctifs de sécurité. Le serveur email utilisé ainsi que les clients emails sur les postes utilisateurs sont considérés fiables. Les serveurs et les postes de travail sont installés suivant les bonnes pratiques et recommandations de l'ANSSI, notamment EMET (Enhanced Mitigation Experience Toolkit) pour Windows.

3.4.2 Environnement réseau

Sur les serveurs TMMS et TCS, seul le port HTTPS (443) est ouvert en entrée. Un équipement anti DoS/DDoS est positionné en frontal des serveurs TMMS et TCS.

3.4.3 Environnement physique

Les serveurs TMMS et TCS doivent être installés sur des serveurs respectant leur prérequis en termes de performance. Les serveurs physiques doivent être positionnés dans une salle serveur à accès protégé et restreint seulement aux administrateurs. Les serveurs TMMS et TCS sont administrés « au pied de la machine ». L'accès aux locaux de l'entreprise doit être contrôlé. L'usage des postes informatiques est restreint aux seuls employés de l'entreprise.

3.4.4 Mesures organisationnelles

Les administrateurs de la solution et les administrateurs OS sont considérés fiables, intègres et non hostiles. Les utilisateurs et les administrateurs sont formés aux bonnes pratiques de sécurité et maitrisent l'usage du client TCC. Les administrateurs maitrisent également la configuration des serveurs Tixeo TMMS et TCS.

3.5 Description des dépendances

3.5.1 Serveur TMMS

- Oracle JDK 1 .8 d'Oracle. Il est recommandé d'utiliser la dernière version en date.
- Apache Tomcat 8.0. Il est recommandé d'utiliser la dernière version en date.

3.5.2 Serveur TCS et client TCC

Le serveur TCS et le client TCC utilisent et embarquent tous deux la bibliothèque OpenSSL version 1.0.2j.

3.6 Description des utilisateurs typiques concernés

3.6.1 Administrateur

Il a un contrôle total sur la solution au travers des serveurs TMMS et TCS. Il peut configurer le comportement global de la solution, l'envoi des emails, la délégation d'authentification à un annuaire, des restrictions de fonctions sur des groupes d'utilisateurs. Il a accès à la liste complète des utilisateurs, peut les modifier et les élever aux rôles d'organisateur ou d'administrateur. Il a accès à la liste complète des réunions et peut les annuler. Il gère les mises à jour des serveurs TMMS et TCS.

3.6.2 Rôles utilisateurs hors réunion

- Organisateur : Il peut inviter d'autres utilisateurs dans des réunions.
- Utilisateur : Il peut uniquement rejoindre les réunions auxquelles il est invité.

3.6.3 Rôles utilisateurs pendant une réunion

- Participant passif : Il ne peut qu'observer ce qui se passe (réception des communications voix, vidéo et partages, mais pas d'envoi).
- Participant actif : Il peut communiquer (envoi voix et vidéo) en plus d'observer. C'est le rôle par défaut des invités à une réunion.
- Présentateur : Il peut observer, communiquer et partager des documents (partage de bureau, d'écran ou d'applications).
- Modérateur : Par défaut, seul l'organisateur de la réunion a ce rôle lorsqu'il rejoint la réunion. Ce rôle lui permet de changer le rôle des autres participants.

3.7 Définition du périmètre de l'évaluation

L'évaluation porte sur la confidentialité des communications lors d'une réunion Tixeo. Plus précisément sur le chiffrement de lien TLS entre client TCC et le serveur TMMS, le chiffrement de lien TLS entre le client TCC et le serveur TCS, le chiffrement de bout en bout (de client TCC à client TCC), et l'échange des clés Diffie-Hellman. L'évaluation porte également sur la protection des mots de passes des utilisateurs.

4 Description de l'environnement technique de fonctionnement

4.1 Environnement matériel

Les matériels retenus dans le cadre de l'évaluation sont de simples PC et serveurs compatibles avec les systèmes d'exploitation retenus ci-dessous. Les serveurs TMMS et TCS seront installés sur le même serveur avec deux cartes réseaux.

Pour le client TCC :

- CPU : Intel core i3
- RAM : 4 Go
- Disque dur : 60 Go

Pour les serveur TMMS et TCS :

- CPU : Intel Xeon E3
- RAM : 8 Go
- Disque dur : 120 Go
- 2 cartes réseau

4.2 Environnement logiciel

Systèmes d'exploitation pour les clients TCC : Microsoft Windows 10 64 bits et macOS Sierra 10.12. Les clients TCC Windows et macOS sont identiques du point de vue de l'utilisateur.

Système d'exploitation pour les serveur TMMS et TCS : Microsoft Windows Server 2012 R2 64 bits

Navigateur Internet pour l'accès web au TMMS : Firefox dernière version

4.3 La solution Tixeo

La solution Tixeo utilisée dans le cadre de l'évaluation est le version 11.5.2.0

5 Description des biens sensibles

Dans le cadre de cette évaluation, les biens sensibles à protéger sont les suivants :

B1 : La confidentialité des communications voix, vidéo et partages lors d'une réunion.

B2 : La confidentialité des clés de chiffrement et des mots de passes des utilisateurs.

6 Description des menaces

6.1 Agents menaçants

Dans le cadre de l'évaluation, les menaces sur les biens sensibles définis précédemment sont portées par des attaquants externes et/ou des attaquants avec des accès restreints.

6.2 Menaces

M1 : Un attaquant capture les trames réseau afin d'écouter les communications voix, vidéo et partages lors d'une réunion Tixeo (B1).

M2 : Un attaquant prend connaissance des informations stockées dans la base de données afin de récupérer les mots de passes des utilisateurs (B2).

M3 : Un attaquant ayant ou non un accès restreint à la solution Tixeo cherche à entrer dans une réunion à laquelle il n'est pas invité afin d'écouter les communications voix, vidéo et partages lors d'une réunion Tixeo (B1).

7 Description des fonctions de sécurité du produit

7.1 F1 : Chiffrement de bout en bout

Les communications entre les différents TCC connectés à une même réunion (exécuté dans un serveur TCS) sont protégées par un chiffrement de bout en bout. Les flux sont chiffrés localement sur le TCC et déchiffrés sur les TCC des autres participants à la réunion. Le serveur TCS manipule les flux de communication chiffrés sans jamais avoir accès au contenu de ces communications.

Les clés utilisées pour le chiffrement de bout en bout des flux de communication sont volatiles et échangées par Diffie-Hellman dans un lien chiffré HTTPS (TLS 1.2).

7.2 F2 : Protection des mots de passes des utilisateurs

Les mots de passes des utilisateurs dans la base de données sont stockés hashés et salés. Le serveur n'a jamais connaissance des mots de passes saisis par les utilisateurs.

7.3 F3 : Authentification des utilisateurs

Les utilisateurs de la solution (invités, organisateurs et administrateurs) doivent s'authentifier sur le TMMS (par page web ou depuis le client TCC) en utilisant leur email et mot de passe. L'accès à une réunion est strictement réservé aux personnes y étant invitées.

7.4 F4 : HTTPS Tunneling

Les solutions traditionnelles de visioconférence nécessitent l'ouverture de ports réseau, non seulement sur le poste utilisateur, mais aussi sur l'infrastructure réseau. Ceci constitue un affaiblissement de la politique de sécurité.

Les communications (audio, vidéo et données) entre le TCC et le serveur TCS sont encapsulées dans un flux HTTPS unique, clairement identifié sur le réseau. Le lien de communication entre le client TCC et le serveur TMMS est également chiffré et protégé par l'utilisation du protocole HTTPS (TLS 1.2). Le déploiement de la solution Tixeo est transparent et ne nécessite pas d'intervention sur la politique de sécurité réseau.