Cible de sécurité CSPN TixeoServer

TIXEO

www.tixeo.com

v221116

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 v16.6.2.3 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	V16.6.2.3
Catégories de produit	Communication sécurisée

La version évaluée correspond à l'ensemble des éléments de la solution (TMMS, TCS, TCC Windows, 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 et de transfert de fichiers. 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.

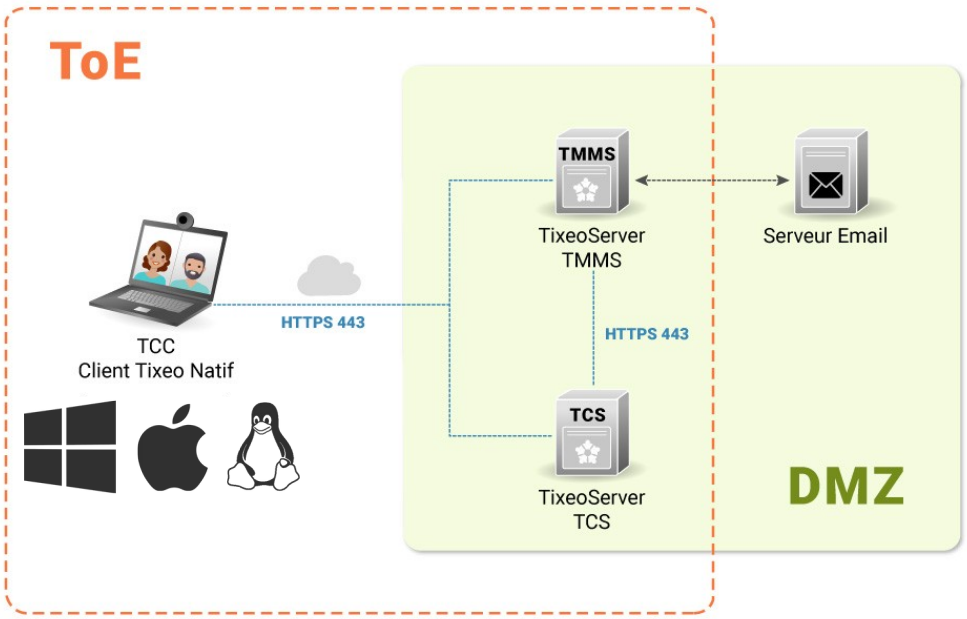

Fig.1 : Target of evaluation

Dans le cadre d'un déploiement avancé (redondance, proximité des utilisateurs, isolement…), il est possible d'avoir plusieurs TCS. Dans ce cas de figure, lorsqu'une réunion est lancée sur un TCS, il est possible d'y accéder par le relai d'un autre TCS. L'utilisateur se connectera toujours par le biais du TCS avec lequel il a la meilleure connectivité (ou tout simplement une connectivité).

L'administrateur a également la possibilité de configurer une journalisation centralisée pour le TMMS et les TCS (et éventuellement les TCC).

3.2 Description de l'utilisation du produit

Lorsqu'un utilisateur est invité pour la première fois, il reçoit un e-mail de validation de compte contenant un lien vers le serveur 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. Pour les plateformes Windows et macOS, 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 (e-mail 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 partager son écran, mais également proposer un fichier qui sera transféré aux seuls participants ayant accepté ce transfert (cette fonction peut être désactivée par l'administrateur sur le serveur TMMS.

La confidentialité des communications (voix, vidéo et data) 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 suivants :

- Windows 7, 8, 8.1, 10, 11
- Mojave 10.14, Catalina 10.15, Big Sur 11, Monterey 12, Ventura 13
- Ubuntu 18.04, 20.04; Debian 10

Afin de pouvoir communiquer en voix et vidéo, le client TCC nécessite une webcam (ou caméra intégrée) et un microphone.

Les serveurs TMMS et TCS sont installés dans des environnements Windows Server 2012 r2, 2016 ou 2019.

Les fonctions « Donner le contrôle d'un partage », « Messages » en « Code PIN » sont désactivée par l'administrateur sur le TMMS. Ces fonction ne peut être activée ou désactivée que par l'administrateur.

3.4 Description des hypothèses sur l'environnement

L'utilisateur doit considérer le TMMS et le TCS comme centraux du point de vue de la sécurité du système. En particulier, une compromission du TCS serait de nature à menacer le chiffrement bout-en-bout de l'intégralité des flux ; l'utilisateur doit donc prendre une précaution particulière dans le respect des hypothèses suivantes, afin de garantir le maintien en condition de sécurité de son environnement logique, réseau, physique et organisationnel.

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 e-mail utilisé ainsi que les clients e-mails 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. Les serveurs sont protégés des attaques DoS/DDoS par la mise en place de systèmes de protections recommandés par l'ANSSI tels que décrits dans le guide « Comprendre et anticiper les attaques DDoS ».

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 maîtrisent l'usage du client TCC. Les administrateurs maîtrisent également la configuration des serveurs Tixeo TMMS et TCS.

3.5 Description des dépendances

3.5.1 Serveur TMMS

- JDK 17 de Eclipse Temurin. Il est recommandé d'utiliser la dernière version en date.
- Apache Tomcat 9.0. 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 1.1.1q.

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 e-mails, 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 Droits des utilisateurs pendant une réunion

- Microphone : L'utilisateur peut activer son microphone et être entendu.
- Caméra : L'utilisateur peut activer sa caméra et être vu.
- Partage : L'utilisateur peut partager (partage d'écran et transfert de fichiers).
- Modération : L'utilisateur changer les droits des autres participants. Par défaut, seul l'organisateur de la réunion a ce droit.

Quels que soient les droits affectés à un utilisateur connecté à une réunion, celui-ci reçoit les communications voix, vidéo et partages des autres participants.

3.7 Définition du périmètre de l'évaluation

L'évaluation porte sur la confidentialité des communications (voix, vidéo, partages d'écran et transfert de fichiers) 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, ainsi que les risques d'élévation de privilèges et d'usurpation d'identité d'un utilisateur ou d'un serveur.

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 i5
- RAM : 8 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 11 64 bits, macOS Monterey 12 et Ubuntu 20.04. Les clients TCC Windows, macOS et Linux sont identiques du point de vue de l'utilisateur.

Système d'exploitation pour les serveur TMMS et TCS : Microsoft Windows Server 2019

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 16.6.2.3

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.

B3 : La confidentialité et l'intégrité des fichiers transférés lors d'une réunion.

Le fichier de configuration du TCC ne dispose pas de biens sensibles autres qu'un éventuel mot de passe chiffré de l'utilisateur (s'il a choisit de la mémoriser).

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, c'est à dire tout utilisateur de la solution Tixeo n'étant pas administrateur.

6.2 Menaces

M1 : Un attaquant capture ou modifie les trames réseau afin d'écouter les communications voix, vidéo, partages et transferts de fichiers lors d'une réunion Tixeo (B1 et B3).

M2 : Un attaquant prend connaissance des 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, partages et transferts de fichiers lors d'une réunion Tixeo (B1 et B3).

M4 : Élévation de privilège dans l'objectif d'accéder aux biens sensibles.

M5 : Usurpation d'identité d'un utilisateur.

M6 : Usurpation d'identité d'un serveur : un attaquant se fait passer pour le serveur dans l'objectif de compromettre des biens sensibles.

M7 : Un attaquant modifie les trames réseau afin de corrompre un fichier transféré lors d'une réunion Tixeo (B3).

7 Description des fonctions de sécurité du produit

7.1 F1 : Chiffrement de bout en bout dans un tunnel TLS

Les communications (voix, vidéo, partages et transferts de fichiers) 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.

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 / TLS 1.3), qui transite par le TCS. La sécurité des flux repose sur la confidentialité et l'intégrité de ces clés et donc sur l'hypothèse de la non-compromission de l'environnement du TCS (voir 3.4).

7.2 F2 : Protection des mots de passes des utilisateurs

L'utilisateur peut s'authentifier directement sur les pages Web du TMMS ou depuis le TCC. Dans ces deux situations le mot de passe de l'utilisateur est transmis hashés et salés, ainsi le serveur n'a jamais connaissance des mots de passes saisis par les utilisateurs.

Sur le TCC, dès que l'utilisateur entre son mot de passe, celui-ci est haché, le hash du mot de passe devient le mot de passe du système Tixeo et le mot de passe en clair est effacé de la mémoire du TCC. Si l'utilisateur a choisit de mémoriser le mot de passe sur le TCC, son hash est stocké chiffré.

Le serveur ne stocke pas directement le hashé du mot de passe de l'utilisateur, mais refait une phase de hashage avant de le stocker en base.

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 e-mail 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, et entre le TCS et le TMMS, est également chiffré et protégé par l'utilisation du

protocole HTTPS (TLS 1.2 / TLS 1.3). Le déploiement de la solution Tixeo est transparent et ne nécessite pas d'intervention sur la politique de sécurité réseau. Le Certificate Pinning permet également de garantir une communication HTTPS chiffrée en cas de compromission de l'autorité de certification ayant émis les certificats du TMMS ou des TCS.

8 Matrice de couverture

8.1 Menaces et biens sensibles

La matrice suivante présente la couverture des menaces sur les biens sensibles (les lettres "D", "I", "C" et "A" représentent respectivement les besoins de Disponibilité, Intégrité, Confidentialité et Authenticité) :

	B1. VOIX, VIDÉO ET PARTAGES LORS D'UNE RÉUNION	B2. CLES DE CHIFFREMENT ET DES MOTS DE PASSE DES UTILISATEURS	B3. FICHIERS TRANSFERES LORS D'UNE RÉUNION
M1. CAPTURE MODIFICATION RÉSEAU LORS D'UNE RÉUNION	CIA		CIA
M2. CONNAISSANCE MOT DE PASSE	CIA	C	CIA
M3. PARTICIPATION ILLÉGITIME À UNE RÉUNION	CIA		CIA
M4. ÉLÉVATION DE PRIVILÈGES	CIA		CIA
M5. USURPATION D'IDENTITÉ D'UN UTILISATEUR	CIA		CIA
M6. USURPATION D'IDENTITÉ D'UN SERVEUR	CIA	CIA	CIA
M7. MODIFICATION FICHIER TRANSFÉRÉ			CIA

8.2 Menaces et fonctions de sécurité

La matrice suivante présente la couverture des menaces par les fonctions de sécurité :

	F1. CHIFFREMENT BOUT EN BOUT	F2 . PROTECTION DES MOTS DE PASSE DES UTILISATEURS	F3. AUTHENTIFICATION DES UTILISATEURS	F4. HTTPS TUNNELING
M1. CAPTURE MODIFICATION RÉSEAU LORS D'UNE RÉUNION	X			X
M2. CONNAISSANCE MOT DE PASSE		X		X

M3. PARTICIPATION ILLÉGITIME À UNE RÉUNION		X	X
M4. ÉLÉVATION DE PRIVILÈGES	X	X	
M5. USURPATION D'IDENTITÉ D'UN UTILISATEUR		X	
M6. USURPATION D'IDENTITÉ D'UN SERVEUR			X
M7. MODIFICATION FICHIER TRANSFÉRÉ	X		X