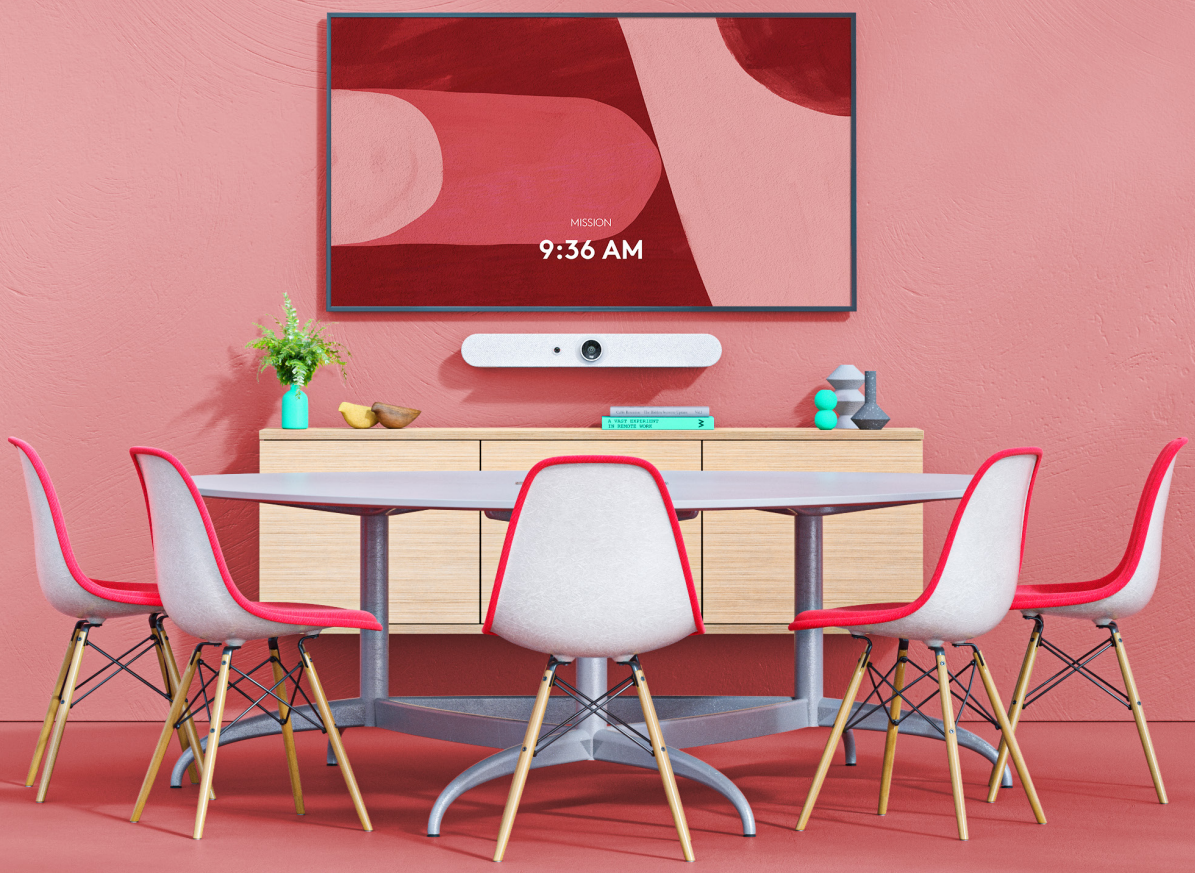
SÉCURITÉ ET CONFIDENTIALITÉ DE LA VIDÉO COLLABORATION LOGITECH



INTRODUCTION

La fréquence et la sophistication des cyberattaques s'accentuent à travers le monde, présentant des risques importants pour les organisations dans un espace de travail hybride de plus en plus distribué et virtuel.

Aujourd'hui, les cybercrimes peuvent provenir de n'importe où et à tout moment, les pirates exploitant les vulnérabilités des logiciels et du matériel, tels que les caméras, les casques et d'autres dispositifs.

Dans ce livre blanc, nous partageons avec vous notre approche en matière de sécurité et de confidentialité pour les dispositifs fonctionnant sous CollabOS. Actuellement, ces dispositifs incluent Rally Bar, Rally Bar Mini, RoomMate, Tap Scheduler et Tap IP.

QU'EST-CE QUE COLLABOS?

CollabOS est le système d'exploitation unifié qui s'exécute sur certains dispositifs de vidéo collaboration Logitech. Grâce au système d'exploitation CollabOS, ces dispositifs fonctionnent de façon fluide et s'améliorent sans cesse. Il est en outre plus aisé que jamais de les déployer et de les gérer, ce qui permet à chacun de vivre une expérience juste et de qualité lors des réunions.

CollabOS simplifie le déploiement et la gestion de la visioconférence en intégrant le matériel Logitech et des applications tierces et des services de planification, tels que Microsoft Teams, Zoom et Robin.

Le système d'exploitation CollabOS améliore continuellement l'expérience utilisateur des participants aux réunions vidéo, tout en prolongeant la durée de vie de votre investissement dans la visioconférence. Les mises à jour du micrologiciel avec les nouvelles fonctionnalités, les améliorations et les dispositifs de sécurité sont automatiquement envoyées à vos dispositifs sans fil et sans frais.

DISPOSITIFS ALIMENTÉS PAR COLLABOS

- **Rally Bar** et **Rally Bar Mini** sont les premières barres vidéo tout-en-un de Logitech destinées aux grandes, moyennes et petites salles de réunion, avec une caméra optique unique, un son bidirectionnel simultané et une caméra secondaire dédiée à l'IA. Ces deux dispositifs peuvent être déployés en mode USB ou serveur, avec une flexibilité et une simplicité exceptionnelles.

  En savoir plus sur Rally Bar et Rally Bar Mini

- **RoomMate** est un appareil de visioconférence pour les caméras et périphériques pris en charge, y compris le système Rally, MeetUp et l'audio tiers. Il vous permet de déployer facilement Microsoft Teams® Rooms sous Android, des appareils Zoom Rooms et d'autres services de visioconférence de pointe.

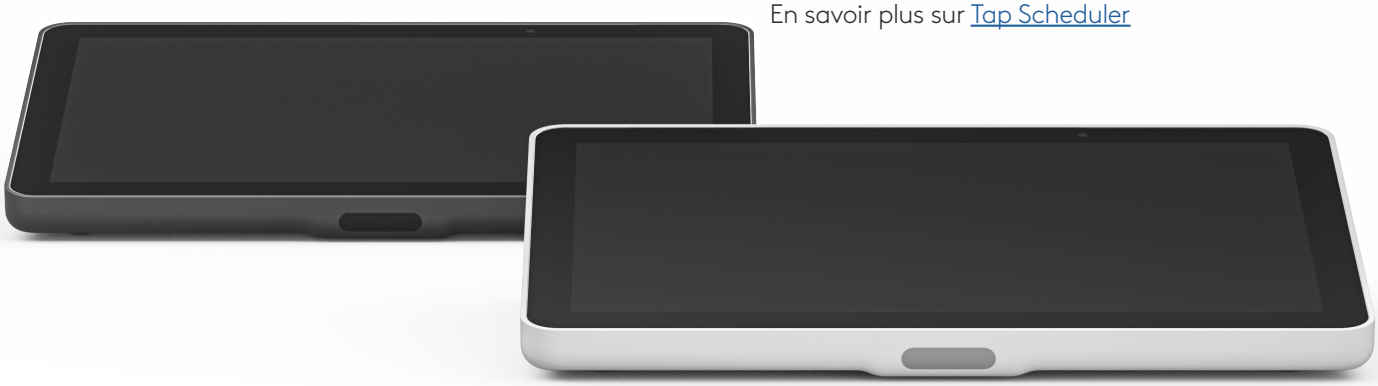
  En savoir plus sur RoomMate

- **Tap IP** est un contrôleur tactile connecté au réseau qui facilite la participation aux visioconférences sur différentes plateformes et applications. Avec un grand écran de 10,1 pouces, très fin, et un capteur de mouvement pour une disponibilité permanente, Tap IP permet facilement de partager du contenu et assure une expérience de réunion cohérente dans toutes les salles.

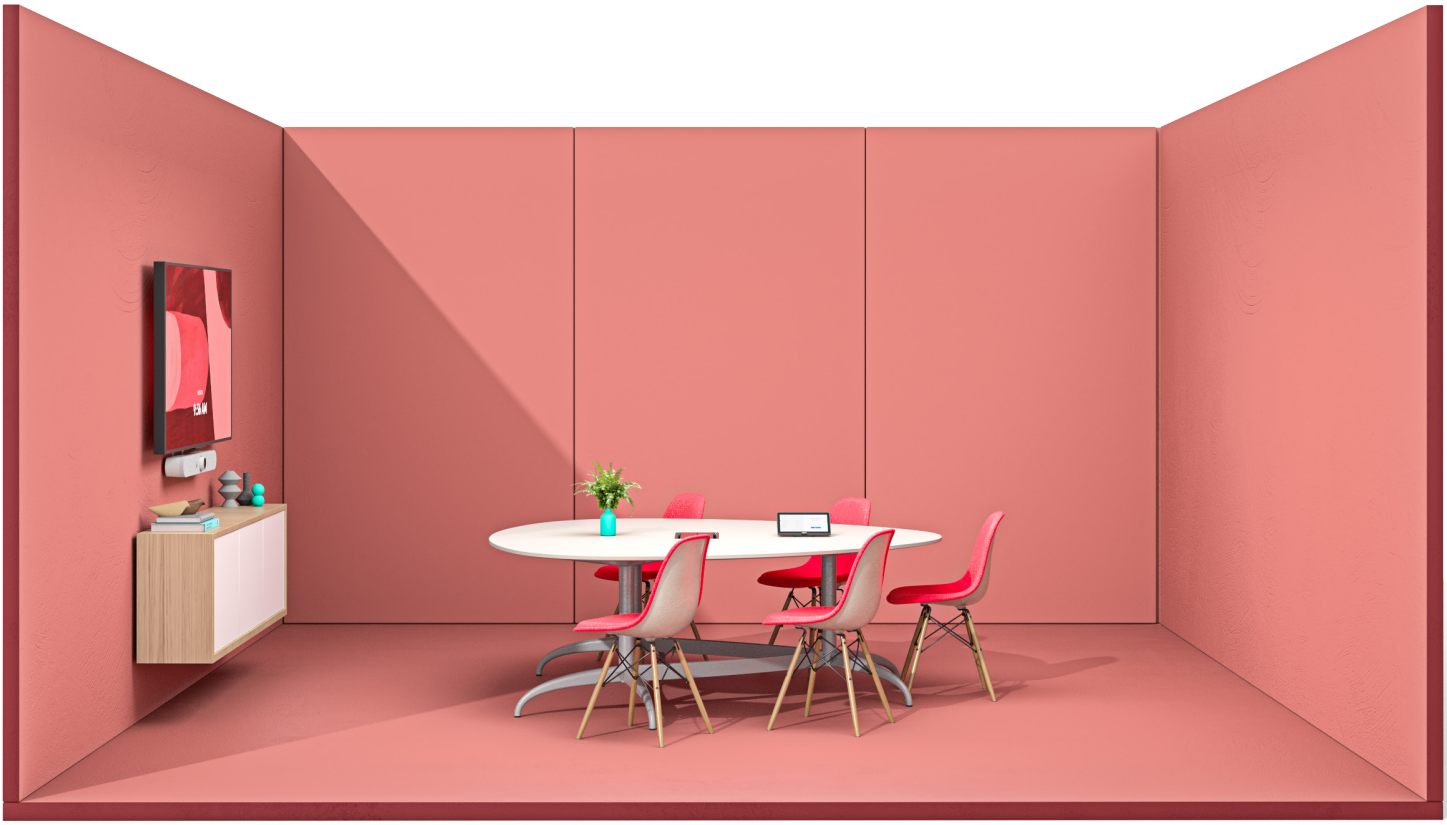
  En savoir plus sur Tap IP

- **Tap Scheduler** est un panneau de planification spécialement conçu pour les salles de réunion qui améliore l'expérience au bureau. Tap Scheduler permet d'accéder facilement aux informations sur les réunions et de réserver une salle pour des réunions ponctuelles ou futures, avec des témoins lumineux colorés indiquant la disponibilité à distance pour aider les employés à trouver rapidement une salle libre.

  En savoir plus sur Tap Scheduler



SÉCURITÉ ET CONFIDENTIALITÉ



La sécurité et la confidentialité sont des aspects essentiels de la conception de tous les produits de visioconférence Logitech. CollabOS fonctionne sous Android 10, qui garantit une sécurité, une confidentialité et des performances optimales.

Les produits Logitech sont développés selon un cycle de développement sécurisé qui applique les meilleures pratiques du secteur lors de la conception, du développement et du déploiement de produits. Nous respectons et dépassons les attentes en matière de sécurité en intégrant cet aspect dès les premières phases de conception, avec notamment une étude de la conception des produits menée par un comité de contrôle de la sécurité composé d'experts en la matière issus de toute l'organisation. Nous vérifions scrupuleusement la sécurité des systèmes et des logiciels au cours des phases de développement et d'évaluation. Nous nous conformons également à STRIDE, la norme du secteur en matière de classification des menaces de sécurité.

Remarque: « Sauf indication contraire, les fonctionnalités de sécurité et de confidentialité décrites dans ce livre blanc s'appliquent aux cinq dispositifs répertoriés ci-dessus, qui sont qualifiés dans le présent document de "dispositifs CollabOS". »

SÉCURITÉ DES INFORMATIONS

CYCLE DE VIE DE DÉVELOPPEMENT SÉCURISÉ (SDLC)

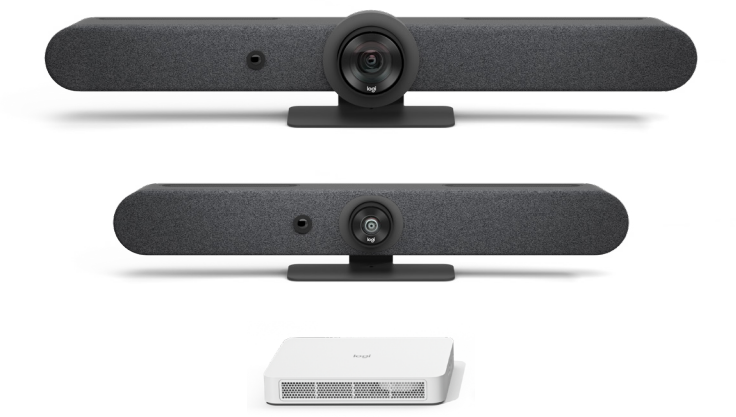
Les portes de vérification de la sécurité sont mises en œuvre à chaque étape du développement système dans le SDLC de Logitech pour les dispositifs CollabOS, y compris la conception, la mise en œuvre et le lancement. Au cours de la phase de conception, tous les documents afférents sont examinés par des experts internes et externes en matière de sécurité.

La phase de mise en œuvre comporte des examens manuels et automatisés du code produit par l'équipe de développement. Une analyse statique est réalisée sur l'ensemble du code source, et les problèmes identifiés sont signalés et examinés par l'équipe de développement et des spécialistes de la sécurité.

Le développement logiciel associé aux dispositifs CollabOS suit les normes du secteur, notamment:

- Norme de codage sécurisé Android
- Norme de codage Oracle SEI CERT pour Java
- Norme de codage en C SEI CERT C
- Norme de codage en C++ SEI CERT

Avant sa mise en service, un logiciel est soumis à une série de tests rigoureux portant à la fois sur sa fonctionnalité et sa sécurité. Les mises à jour et les nouvelles versions des systèmes obéissent également au SDLC, et les logiciels déployés sont gérés et mis à jour avec tous les correctifs de sécurité permettant de résoudre les problèmes identifiés entre deux versions importantes.



SÉCURITÉ ET CONFIDENTIALITÉ GARANTIES DÈS LA CONCEPTION

La sécurité et la confidentialité sont intégrées aux dispositifs CollabOS dès le début du développement du produit, jusqu'à leur mise en œuvre, leur lancement et leurs mises à jour.

Voici une liste non exhaustive des mesures prises pour renforcer la sécurité de nos dispositifs:

- **Établissez une base solide:** la plateforme repose sur Android 10, qui offre une sécurité et une stabilité renforcées.
- **Évitez les mots de passe universels par défaut:** les dispositifs Logitech CollabOS obéissent aux bonnes pratiques du secteur et à la législation de l'État de Californie, et n'ont ainsi pas de mot de passe par défaut.
- **Mise à jour du logiciel:** les mises à jour sans fil du micrologiciel permettent aux dispositifs CollabOS de rester constamment à jour avec la dernière version.
- **Gestion de l'intégrité logicielle:** toutes les images logicielles sont signées numériquement pendant la production et distribuées via des liens de communication sécurisés. Les dispositifs CollabOS vérifient la signature de chaque image logicielle avant d'installer ou de mettre à jour leur logiciel, préservant ainsi leur intégrité et leur authenticité.
- **Communiquez en toute sécurité:** depuis la version 1.7 de CollabOS, toutes les communications entre les dispositifs CollabOS et le nuage utilisent les versions 1.2 et 1.3 du protocole TLS (Transport Level Security). TLS 1.1 et 1.0 sont désactivés sur les dispositifs CollabOS et n'apparaîtront plus dans les analyses de sécurité. Les applications exécutées sur la plateforme peuvent utiliser des formes de communication similaires ou complémentaires. Nous vous conseillons de vous renseigner auprès des fournisseurs de services applicatifs concernant leurs protocoles de sécurité.
- **Protection des données à caractère personnel:** si les dispositifs CollabOS ne contiennent ni ne stockent d'informations d'identification personnelle, les fournisseurs de services vidéo peuvent stocker ces dernières dans leurs applications. Nous vous conseillons de vous renseigner auprès de ces fournisseurs de services concernant leur politique relative aux informations d'identification personnelle.

SÉCURITÉ DES INFORMATIONS

SÉCURITÉ APPLICATIVE DES DISPOSITIFS

Les dispositifs CollabOS contiennent plusieurs applications servant à leur fonctionnement quotidien. Afin de garantir la sécurité des dispositifs, Logitech gère avec soin les applications qu'ils contiennent.

Le processus de mise en liste verte des applications nous permet de contrôler avec précision quelles applications sont autorisées à être utilisées. Dans le cadre de la sécurisation des logiciels avant leur expédition, nous supprimons ou désactivons également les applications, services et pilotes non essentiels, réduisant ainsi la surface d'attaque. Tous les dispositifs CollabOS utilisent les stratégies SELinux intégrées, qui font partie du système Android.

FONCTION ANTI-RESTAURATION

Les dispositifs pris en charge par CollabOS disposent d'une fonctionnalité qui empêche la restauration d'un système mis à jour à une version logicielle antérieure, potentiellement moins sécurisée.

SÉCURITÉ MATÉRIELLE

Tous les dispositifs pris en charge par CollabOS sont dotés de plusieurs fonctionnalités qui améliorent leur sécurité. Une enclave de confiance est utilisée pour protéger l'ensemble des secrets ou des clés nécessaires sur chaque dispositif. Le matériel utilise un système de démarrage sécurisé pour vérifier la validité du logiciel de démarrage et du micrologiciel système, qui ont été signés pendant la production.

VALIDATION DE SÉCURITÉ

Les processus internes d'assurance qualité utilisent des suites de tests de sécurité des composants logiciels afin d'identifier les potentielles vulnérabilités de sécurité de chaque version logicielle. Les logiciels ne peuvent être mis en service tant qu'ils n'ont pas réussi la suite de tests.

RÈGLES DE PARE-FEU - FILTRAGE/BLOCAGE DES PORTS

Les dispositifs CollabOS mettent en œuvre leurs propres règles de pare-feu pour assurer le filtrage et le blocage des ports, réduisant ainsi la surface d'attaque exposée au réseau.

INDICATEURS D'ENREGISTREMENT ET CONFIDENTIALITÉ DES DISPOSITIFS EXTERNES

Tous les dispositifs d'enregistrement CollabOS, y compris les microphones et les indiquent clairement qu'ils sont en cours d'utilisation. Les dispositifs Rally Bar et Rally Bar Mini sont fournis avec des caches d'objectif destinés aux caméras de conférence.

Remarque: cette fonctionnalité ne concerne pas Tap IP, Tap Scheduler ou RoomMate qui ne disposent pas de caméras ou de micros et ne sont pas capables d'enregistrer de la vidéo ou du son.

ISOLEMENT APPLICATIF

Les applications ne peuvent interférer entre elles sur la plateforme grâce à un système de bac à sable applicatif intégré. Chaque application et ses données disposent de leur propre espace de travail et ne peuvent communiquer ou interférer avec l'exécution d'autres applications, y compris la capacité de lire et d'écrire les données qui sont conservées dans le bac à sable spécifique à chaque application.

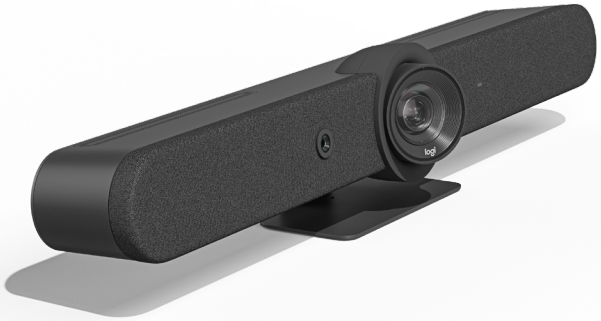
SÉCURISATION DES DONNÉES - STOCKAGE CHIFFRÉ

Un système de stockage chiffré au niveau matériel est utilisé pour stocker l'ensemble des données sur les dispositifs pris en charge par CollabOS.

SÉCURITÉ DES DONNÉES EN SYSTÈME DORSAL

La communication entre les dispositifs pris en charge par CollabOS et les systèmes dorsaux Logitech qui les prennent en charge, y compris les mises à jour sans fil, passe par des canaux chiffrés utilisant le protocole TLS (Transport Layer Security). Cela permet à la fois de chiffrer les données en transfert et d'authentification du système avec lequel le dispositif communique.

Nous exploitons le cadre et l'infrastructure de l'Internet des objets d'Amazon pour permettre une communication sécurisée entre chaque dispositif et le système dorsal, ainsi que la sécurisation des données au repos sur le nuage.



VULNÉRABILITÉ ET GESTION DES RISQUES

Nous surveillons activement la sécurité de nos produits et effectuons des mises à jour régulières pour corriger toute vulnérabilité connue.

RÉPONSE AUX INCIDENTS

Logitech invite les clients ainsi que les chercheurs en sécurité à signaler tout problème rencontré dans nos produits afin de les résoudre en pratique. Nous participons à un programme public de prime aux bogues dans le cadre duquel les chercheurs peuvent contribuer à améliorer la sécurité de nos produits en signalant les problèmes identifiés, leur permettant ainsi d'obtenir des récompenses pour leurs découvertes. Logitech offre une récompense appropriée aux personnes qui signalent des incidents de sécurité jugés pertinents et nécessitant une intervention.

De plus, les incidents sont enregistrés et traités aussi rapidement que possible. Nous demandons aux personnes qui les signalent de se conformer aux pratiques en vigueur en matière de divulgation responsable.

RESSOURCES SUPPLÉMENTAIRES

Pour en savoir plus sur les dispositifs compatibles CollabOS, notamment Rally Bar, Rally Bar Mini, RoomMate, Tap IP et Tap Scheduler, rendez-vous sur logitech.com/vc.

CONTACT

Pour signaler un problème de sécurité concernant les produits Logitech, rendez-vous sur logitech.com/security. Pour toute autre demande, rendez-vous sur logitech.com/contact.

Logitech, Inc.
7700 Gateway Blvd.
Newark, CA 94560
Publié en novembre 2023