Sécurité Paxton10

Présentation

Paxton10 est un système de contrôle d'accès et de gestion vidéo basé sur le réseau, qui est contrôlé et configuré par le serveur Paxton10 via son interface utilisateur web. Ce document examine comment Paxton10 reste sécurisé et résistant face aux attaques de sécurité et aux violations de données.

Serveur Paxton10

Système d'exploitation et BIOS

Le serveur Paxton10 fonctionne sous Microsoft Windows 10 IoT (à partir de février 2020). Toutefois, certains modèles anciens (avant 2020) peuvent fonctionner sous Windows 7 Embedded - veuillez contacter l'assistance pour en savoir plus.

Le bureau à distance et le partage de fichiers sont activés sur le serveur, sécurisés par un mot de passe de 40 caractères du système d'exploitation, unique à chaque système.

Le BIOS du serveur est protégé de la même manière par un mot de passe.

Mises à jour Windows

Les serveurs sont fournis avec des correctifs et des patches de sécurité présélectionnés dans le cadre de Windows update. Ceux-ci sont mis à jour en arrière-plan lorsque cela est possible, et en même temps que les versions de service dans le cadre du processus de mise à jour contrôlé par l'Ingénieur système lorsque cela n'est pas possible. Le serveur peut avoir besoin d'être redémarré après une mise à jour de Windows - le logiciel Paxton10 fournira les moyens de le faire lorsque cela sera nécessaire. Une connexion Internet est requise pour recevoir le logiciel Paxton10 et les mises à jour Windows.

Protection anti-virale

Les serveurs fonctionnant sous Windows 10 IoT incluront Windows Defender avec des mises à jour automatiques. Une connexion Internet est requise pour recevoir les mises à jour.

Ports USB

Le serveur Paxton10 est fourni avec une clé USB pour la sauvegarde du système. Cette clé USB peut être insérée dans n'importe quel serveur Paxton10 pour restaurer/établir la base de données du système sur ce serveur. La sauvegarde de la base de données sur USB a lieu automatiquement toutes les 24 heures. La sauvegarde sur USB peut être désactivée simplement en retirant la clé USB.
The Les ports USB ne sont pas verrouillés et peuvent donc être utilisés pour accéder aux données du serveur ou exécuter des commandes. La sécurité des ports USB est assurée par la sécurisation de l'emplacement du serveur. Seuls les installateurs et le personnel informatique requis devraient avoir accès à l'emplacement du serveur.

Mots de passe et accès des clients

Paxton10 utilise une adresse e-mail et un mot de passe pour sécuriser chaque connexion. Lors de la création d'un mot de passe, les utilisateurs doivent respecter les exigences minimales suivantes : au moins sept caractères et une combinaison d'au moins trois types de caractères, notamment des lettres majuscules, des lettres minuscules, des chiffres et des signes de ponctuation.
Le système vérifie également les nouveaux mots de passe par rapport à une vaste liste open source de plus de 100,000 mots de passe courants ou précédemment compromis. Si un mot de passe figure sur cette liste, Paxton10 le rejettera afin d'éviter les choix faibles ou peu sûrs. Un indicateur de force intégré aide les utilisateurs à voir le niveau de sécurité de leur mot de passe au fur et à mesure qu'ils le saisissent.

Si nécessaire, les administrateurs peuvent augmenter la longueur minimale du mot de passe et peuvent également activer une politique qui oblige les utilisateurs à changer leur mot de passe tous les 60 jours. Ces deux options sont disponibles dans le menu Options.

Pour se protéger contre les tentatives de devinette répétées, Paxton10 autorise six tentatives de connexion infructueuses. Après la sixième tentative incorrecte, l'utilisateur est bloqué pendant 15 minutes avant de pouvoir réessayer.

Les mots de passe sont stockés en toute sécurité dans la base de données du serveur à l'aide d'un hachage salé.

Communication réseau

Accès au logiciel client

En accédant au logiciel Paxton10 depuis le réseau local (via l'URL locale du serveur), la communication se fait entre le client et le serveur. La communication est sécurisée par HTTPS, avec un certificat SSL auto-signé Paxton10, en plus de toutes les mesures de sécurité du réseau local en place.

En accédant au logiciel Paxton10 à distance (via l'URL d'accès à distance du serveur), le logiciel Paxton10 est hébergé en utilisant Microsoft Azure. La communication entre le serveur, le client et Azure est sécurisée par HTTPS avec un chiffrement AES-256. Une connexion Internet est requise. Aucune donnée relative à l'utilisateur ou à l'appareil n'est stockée dans Azure.

E-mails de la part de Paxton10

Paxton10 utilise les e-mails pour réinitialiser les mots de passe et délivrer les Identifiants Intelligents. Les e-mails sont envoyés à partir de l'adresse suivante : support@paxton10portal.com. Les e-mails envoyés par Paxton10 utilisent le chiffrement TLS.

Un serveur de messagerie supplémentaire peut être configuré dans Paxton10 pour être utilisé avec les Déclencheurs et les Actions. La sécurité de ce serveur de messagerie est déterminée par l'hôte.

Communication du contrôleur et mises à jour du firmware

La communication avec les contrôleurs Paxton10 se fait par HTTPS/SSL.
Nous utilisons TLS 1.2 pour le multisite, il utilise SHA-256 qui est un cryptage 256 bits.

For plus d'informations sur la sécurité réseau et les protocoles de communication utilisés, consultez Exigences, optimisation et sécurité réseau AN0051-F dans Paxton10 < www.Paxton.Info/6390 >.

Identifiants et Appareils intelligents

Étiquettes RFID et cartes

Les cartes et badges Paxton10 stockent leur numéro de série dans un secteur protégé par mot de passe, ce qui empêche toute lecture ou copie non autorisée. En plus, Paxton10 lit la carte ou le badge dans son intégralité, et pas seulement les données de la carte ; l'identifiant est ensuite créé à partir d'une combinaison des données de la carte (données du badge, numéro de série, date de fabrication, etc.), ce qui rend le clonage de la carte pratiquement impossible.

Le logiciel Paxton10 offre des caractéristiques et des fonctionnalités supplémentaires qui peuvent être configurées pour éliminer davantage tout risque de clonage de carte et d'accès par carte volée, comme l'anti-passback, les dates d'expiration des utilisateurs, l'interdiction des badges et la double authentification (badge + code ou badge + PIN).

Communication Bluetooth

Les Identifiants intelligents (smartphones, tablettes et montres) et les badges Bluetooth communiquent avec les lecteurs Paxton10 grâce au Bluetooth Low Energy (BLE). Un algorithme à code tournant est utilisé avec du chiffrement pour empêcher le clonage des identifiants et l'accaparement des codes.

Smart credentials

Les Identifiants intelligents (smartphones, tablettes et montres) sont délivrés avec un identifiant unique de 32 caractères. Chaque identifiant peut être enregistré sur un seul compte Android ou iOS, et une fois enregistré, il ne peut plus être délivré. L'identifiant est stocké dans le trousseau du compte ou dans un espace de stockage sécurisé.

Si une sécurité supplémentaire est requise, un système Paxton10 peut imposer à tous les appareils intelligents d'avoir un verrouillage d'écran, empêchant l'accès non autorisé à partir de appareils perdus ou volés. Une sécurité supplémentaire peut être obtenue en utilisant des fonctions logicielles telles que l'anti-passback et la gestion des identifiants, et une authentification supplémentaire peut être demandée en plus de celle de l'appareil et du verrouillage de l'écran, comme un PIN ou un code sur un clavier.