webdyn
Flexitron group

WebdynSunPM
Annex

Mécanismes de cybersécurité

Table of contents

Mécanismes de cybersécurité

1 Objectif

Cette note présente les principaux mécanismes de cybersécurité disponibles sur le WebdynSunPM pour protéger l'accès au produit, les échanges de données à distance et les commandes envoyées par SMS.

Elle s'adresse aux exploitants, intégrateurs et équipes IT qui doivent intégrer le concentrateur dans une architecture sécurisée.

2 Synthèse

Le WebdynSunPM combine plusieurs mécanismes de protection :

- un accès au serveur Web local protégé par authentification ;
- un mécanisme de chiffrement des commandes SMS ;
- la prise en charge de protocoles sécurisés pour les échanges distants : SFTP, WebDAV sur HTTPS et MQTTS ;
- la gestion de certificats pour les connexions TLS, notamment pour les intégrations cloud ;
- des paramètres de configuration permettant de limiter l'usage de protocoles non chiffrés.

3 Alignement avec l'EN 18031-1

Le WebdynSunPM suit les exigences applicables de la norme EN 18031-1, qui définit des exigences communes de sécurité pour les équipements radioélectriques connectés à Internet.

Les mécanismes décrits dans cette note contribuent à cet alignement, notamment l'authentification des accès, la protection des communications, l'usage de protocoles sécurisés, la gestion des certificats et la réduction de l'exposition aux protocoles non chiffrés.

4 Accès au serveur Web local

L'interface Web locale est protégée par un compte utilisateur et un mot de passe. Le mot de passe ne doit pas être vide et peut être modifié depuis l'interface de configuration.

Lors du premier paramétrage, le produit identifie l'état de première connexion et permet de définir le mot de passe d'accès. Pour les connexions suivantes, le changement de mot de passe nécessite l'ancien mot de passe.

Bonnes pratiques recommandées :

- définir un mot de passe propre à chaque équipement ou à chaque site ;
- limiter la diffusion du mot de passe aux personnes habilitées ;
- changer le mot de passe lors de la mise en service et après toute intervention de maintenance sensible ;
- éviter la réutilisation d'un mot de passe commun sur un parc complet.

5 Commandes SMS chiffrées

Le WebdynSunPM prend en charge un format de SMS chiffré identifié par le préfixe `xen2`.

Ce mécanisme permet de protéger les commandes envoyées par SMS lorsqu'un mot de passe SMS est configuré. Le produit utilise ce mot de passe pour déchiffrer le contenu reçu avant d'exécuter la commande.

Le format `xen2` repose sur :

- AES-256-GCM pour le chiffrement et l'authentification du message ;
- PBKDF2-HMAC-SHA256 pour dériver la clé à partir du mot de passe ;
- un sel aléatoire de 16 octets ;

- un nonce aléatoire de 12 octets ;
- une étiquette d'authentification de 16 octets ;
- un encodage Base64 standard ;
- un découpage automatique en plusieurs SMS lorsque le message dépasse la taille maximale d'un SMS.

Si le message ne peut pas être déchiffré ou si l'authentification cryptographique échoue, la commande n'est pas transmise au moteur applicatif.

6 Échanges fichiers sécurisés avec SFTP

Le WebdynSunPM peut échanger ses fichiers de configuration, commandes, journaux, alarmes, scripts, certificats et données via un serveur distant.

Pour les échanges fichiers, SFTP est le protocole recommandé lorsque le serveur distant le permet. Il apporte un canal chiffré basé sur SSH et évite l'exposition des identifiants et des fichiers en clair sur le réseau.

Le serveur SFTP doit autoriser un profil compatible avec le client du WebdynSunPM, notamment :

Catégorie	Paramètre requis
Algorithme de clé hôte	`ssh-rsa`
Échange de clés	`diffie-hellman-group-exchange-sha256`
Chiffrement	`aes128-ctr` ou `aes256-ctr`
Intégrité	`hmac-sha2-256` ou `hmac-sha2-512`
Compression	`none`

Le serveur doit aussi être configuré avec un compte dédié au concentrateur. Il est recommandé de limiter ce compte au répertoire strictement nécessaire, de désactiver l'accès shell interactif si possible et de restreindre l'accès réseau au serveur.

7 WebDAV sur HTTPS

Le WebdynSunPM peut utiliser WebDAV sur HTTPS pour les échanges fichiers avec un serveur distant.

HTTPS permet de chiffrer le transport et de protéger les identifiants utilisés pour l'authentification au serveur. Lorsque l'infrastructure le permet, l'usage de HTTPS doit être préféré à un transport non chiffré.

Bonnes pratiques recommandées :

- utiliser un certificat serveur valide et maintenu ;
- éviter les certificats expirés ou autosignés en production, sauf politique IT explicite ;
- limiter les droits du compte WebDAV aux répertoires utilisés par le concentrateur ;
- vérifier que les répertoires attendus existent côté serveur avant la mise en service.

8 MQTTS et intégrations cloud

Le WebdynSunPM prend en charge des types de serveur MQTT sécurisés, dont MQTTS et des variantes dédiées aux intégrations cloud.

MQTTS ajoute une couche TLS au protocole MQTT. Selon le type de serveur configuré, la connexion peut utiliser :

- un certificat d'autorité de certification ;
- un certificat client ;

- une clé privée client ;
- une version TLS configurée, avec TLS 1.2 comme valeur de référence pour les configurations sécurisées ;
- des paramètres spécifiques aux environnements cloud tels qu'AWS IoT ou Azure IoT.

Lorsque MQTTS est disponible côté plateforme de supervision, il doit être préféré au MQTT non chiffré.

9 Protocoles non chiffrés

Le produit conserve la possibilité de configurer certains protocoles non chiffrés pour compatibilité avec des environnements existants.

Ces modes doivent être évités pour les déploiements exposés ou mutualisés. FTP et MQTT sans TLS peuvent exposer les identifiants et les données applicatives sur le réseau. Ils ne doivent être utilisés que dans des environnements isolés, maîtrisés et explicitement acceptés par la politique de sécurité du client.

10 Recommandations de déploiement

Pour un déploiement sécurisé :

- privilégier SFTP ou WebDAV sur HTTPS pour les échanges fichiers ;
- privilégier MQTTS pour les échanges MQTT ;
- utiliser des comptes dédiés au WebdynSunPM sur les serveurs distants ;
- limiter les droits de ces comptes au strict nécessaire ;
- stocker et renouveler les certificats selon la politique IT du client ;
- activer le chiffrement SMS lorsque les commandes SMS sont utilisées ;
- définir des mots de passe propres au site ou à l'équipement ;
- restreindre l'accès réseau aux interfaces d'administration et aux serveurs distants.