ACTIONS DE REMÉDIATION SUITE À L'INCIDENT SUR LES CAPTEURS CHIYU DÉPLOYÉS PAR SOLAR-OT

Déploiement de la dernière version des firmwares & Durcissement de la plateforme de supervision SOLAR-OT

Auteur	Validé par
Deirdre STARSKY, Chef de projet technique	Elena PIZARI, Directeur Général Industrie

OBJECTIF

Le présent document précise les 2 actions de remédiation suite à l'incident sur les systèmes de contrôle d'accès déployés par SOLAR-OT :

1. Le déploiement en urgence de la mise à jour du micrologiciel sur tous les systèmes
2. Le renforcement de la configuration de la plateforme de supervision

1. DEPLOIEMENT EN URGENCE DE LA MISE A JOUR DU MICROLOGICIEL

Le constructeur CHIYU a développé une mise à jour du micrologiciel des systèmes 'SEMAC' de contrôle d'accès corrigeant la vulnérabilité => elle doit être déployée par SOLAR-OT en urgence sur tous les sites

Voici le numéro de la version du micrologiciel à déployer sur les SEMAC S2 (67% du parc) : 670VYJLN
Voici le numéro de la version du micrologiciel à déployer sur les SEMAC S3V3 (33% du parc) : 628AUYSD

2. RENFORCEMENT DE LA CONFIGURATION DE LA PLATEFORME DE SUPERVISION

CONFIGURATION

L'objectif est de limiter les éléments techniques qui peuvent être utilisés pour réaliser une attaque, en installant uniquement les services et équipements indispensables.

Le renforcement du niveau de sécurité passe par un durcissement incluant :

- La limitation des fonctions de la plateforme
- La maîtrise des éléments matériels de la plateforme

A. Modification de la configuration par défaut

Chaque composant est configuré selon les standards, incluant :

- Les comptes techniques et éléments d'authentification associés
- Les ports reseau utilisés
- Les répertoires d'installation et de travail
- Les droits d'accès sur les répertoires et fichiers
- Le compte utilisé pour executer un service ou un processus, et les droits associés à ce compte
- Les fichiers de configuration des éléments de sécurité, en particulier de traçabilité.

B. Restriction des fonctionalités accessibles

Seuls les modules indispensables au fonctionnement et à la sécurité de la plateforme sont maintenus et font l'objet d'une configuration appropriée, d'une maintenance régulière et d'une supervision.

A ce titre l'opérateur analyse le fonctionnement technique de la plateforme pour exclure les services ou fonctionnalités installés mais non utilisés.

Chaque configuration matérielle ou logicielle est inventoriée sous la forme d'une configuration de référence.

C. Inventaire des éléments connectés

L'opérateur procède à un inventaire technique complet des éléments constituant la plateforme et les cartographie. L'inventaire comprend les équipements pouvant se connecter à la plateforme de façon permanente ou temporaire, physiquement ou à distance (poste de travail, serveur, périphérique…).

Dans le cas où une tierce partie se connecte à la plateforme, l'opérateur le note dans sa cartographie et en prend compte dans l'analyse de risques.

D. Utilisation d'éléments maîtrisés

L'opérateur gère les éléments directement, dont :

- Le déploiement de mises à jour
- L'administration des éléments
- La configuration à distance

CLOISONNEMENT

La plateforme suit une logique de segmentation en restreignant chaque sous-système à ses actions en propre afin de :

- Limiter la surface d'attaque
- Contenir une éventuelle attaque
- Limiter l'impact d'une compromission
- Permettre d'adapter le niveau de sécurité de chaque sous-sytème

Le cloisonnement s'applique à la fois aux moyens physiques et aux moyens logiques.

A. Segmentation en sous-systèmes

La segmentation en sous-systèmes s'effectue selon les critères suivants :

- Fonctionnalités
- Niveau de protection des donnés
- Niveau d'exposition
- Niveau de sécurité

Toute connexion entre sous-systèmes doit être justifiée par un besoin fonctionnel.

B. Cloisonnement physique

Un serveur est dédié aux applications les plus critiques

C. Cloisonnement logique

Toute donnée stockée sur le serveur est chiffrée au préalable. Chaque sous-système suit un mécanisme de chiffrement en propre.

Toute communication entre sous-systèmes transite par le réseau privé virtuel chiffré et authentifié.

ACCES A DISTANCE

A. Accès public

L'accès public suit le protocole HTTPS et la plateforme est authentifiée par la présentation d'un certificat serveur.

L'authentification à double facteur est mise en place pour les utilisateurs de la plateforme.

B. Accès nomade

Les postes nomades sont configurés pour établir le tunnel authentifié et chiffré vers la plateforme. Le tunnel n'est pas désactivable, et l'accès à internet ou à un réseau local est impossible.
La partition système et la partition des données sont intégralement chiffré

L'authentification à double facteur est en place sur le poste de travail.

FILTRAGE RESEAU

En complément du cloisonnement, des mécanismes de filtrage sont mis en place.

A. Points de filtrage

Les interconnexions entre sous-systèmes sont les principaux points de filtrage auxquels sont appliqués les filtrages périmétrique et local.

B. Règles de filtrage

La matrice de flux globale comprend les règles de filtrage en vigueur. Elle est mise à jour annuellement.

C. Mise en œuvre

Le filtrage est assuré par des pare-feux dédiés reposant sur le principe des listes d'autorisation.