Danfoss A/S
DK-6430 Nordborg
CVR No.: 20 16 57 15

E-mail: danfoss@danfoss.com
Homepage: www.danfoss.com

Novembre 3, 2026

AK-System Manager – Incident de cybersécurité en Europe – informations client

Cher client,

Plusieurs sites en Europe ont signalé des changements suspects aux premières heures du 2 novembre, y compris des températures de dégivrage anormalement élevées, des réglages de température modifiés et l'activation du dégivrage électrique.

Des systèmes Danfoss connus étaient directement exposés à Internet public (sans VPN, pas protégés par un pare-feu).

L'équipement concerné par les incidents signalés était :

1. Produits dérivés des systèmes AK-SM800 et AK-SC355
2. Systèmes AK-SM800A fonctionnant avec des versions logicielles obsolètes

Mesures d'urgence recommandées
(voir les détails sur les exigences obligatoires et les meilleures pratiques à la page suivante) :

1. Supprimez l'exposition à Internet des unités concernées et de toutes les unités possédant une IP publique
2. Restaurer et vérifier la configuration complète
3. Mettre à jour les systèmes AK-SM800A de la génération actuelle vers la version de firmware la plus récente disponibleSchakel Strikte Modus in op de AK-SM800A
4. Restaurez l'accès aux unités uniquement via un VPN sécurisé ou, en général, via un réseau sécurisé

Pour obtenir une assistance technique supplémentaire, vous pouvez contacter l'équipe d'assistance technique régionale.

En plus, Danfoss recommande de mettre à jour les appareils (AK-SC355, AK-SM800) vers des produits de la génération actuelle (série AK-SM800A), afin d'assurer des mises à jour continues en matière de cybersécurité.

Danfoss continue de suivre la situation et reste entièrement engagé à soutenir nos clients pendant cette période difficile.

Partagez également ces informations avec vos clients et utilisateurs finaux dans le supermarché afin de vous assurer que tous les sites concernés sont informés et peuvent prendre les mesures d'urgence recommandées.

Cordialement,

Jonas Hildebrandt | Senior Director Product Management
Electronic Controllers & Services | Danfoss Climate Solutions
jonas.hildebrandt@danfoss.com | Mobile: +49 151 2626 4387

AK-Systeemmanager Cybersecurity: Exigences obligatoires et meilleures pratiques recommandées

Cybersécurité - exigences obligatoires

Danfoss considère les aspects suivants comme obligatoires lors de la planification pour connecter votre System Manager aux réseaux numériques.
Ne pas mettre en œuvre les exigences obligatoires ci-dessous expose votre System Manager et les applications connectées à des attaques malveillantes et est en dehors de l'état de fonctionnement recommandé par Danfoss.

AK-SC355 (retiré de la vente en 2016, remplacé par le AK-SM800)

- Ne connectez pas un administrateur système directement à Internet public ou à des réseaux ouverts non fiables
- Protégez l'accès à distance avec un VPN sécurisé terminé derrière un pare-feu stateful avec une politique de refus par défaut
- Assurez-vous que l'utilisateur et le mot de passe d'usine ont été modifiés

AK-SM800 (hors vente en 2023, remplacé par le AK-SM800A)

- Ne connectez pas un administrateur système directement à Internet public ou à des réseaux ouverts non fiables
- Protégez l'accès à distance avec un VPN sécurisé terminé derrière un pare-feu stateful avec une politique de refus par défaut
- Assurez-vous que l'utilisateur et le mot de passe d'usine ont été modifiés

AK-SM800A (vendu et supporté à l'échelle mondiale)

- Ne connectez pas un System Manager directement à Internet public ou à des réseaux ouverts non fiables.
- Protégez l'accès externe avec un VPN sécurisé qui se termine derrière un pare-feu stateful avec une politique de refus par défaut.
- Assurez-vous que le System Manager utilise la version logicielle la plus récente pour maximiser les fonctionnalités de cybersécurité.
- Assurez-vous que le niveau de sécurité du System Manager est réglé sur le mode Strict (Configuration>Security-Strict).

Cybersécurité - bonnes pratiques (suivez ces bonnes pratiques en plus des exigences obligatoires)

- Changer régulièrement les mots de passe et ne pas les partager ou les publier
- Modifier les ports de gestion par défaut ou limiter l’accès uniquement aux sources autorisées
- Segmenter le réseau de contrôle (par ex. VLANs) ; Isoler les réseaux d’entreprise et invités
- Sauvegarder les configurations de manière sécurisée
- Consulter les normes industrielles disponibles (ex. ISO/IEC 27002:2013) pour plus de références et de conseils