RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
CERT-FR

⚠️ Ciblage de téléphones Apple 📱 ⚠️ Nouvelle campagne de notification le 29 octobre 2026

Bulletin d'alerte du CERT-FR

</> Json

Objet : Incident de sécurité ciblant les contrôleurs à distance des installations de réfrigération

Gestion du document

Référence	**CERTFR-2026-ALE-012**
Titre	**Incident de sécurité ciblant les contrôleurs à distance des installations de réfrigération**
Date de la première version	**12 octobre 2026**
Date de la dernière version	**16 octobre 2026**
Source(s)	

Une gestion de version détaillée se trouve à la fin de ce document.

Risque

- Non spécifié par l'éditeur

Systèmes affectés

- Copeland xweb
- Danfoss série AK-SC
- Danfoss série AK-SM
- Dixell xweb

Résumé

Le CERT-FR a connaissance de nombreuses compromissions des controleurs à distance d'installation de réfrigération Danfoss série AK-SM, AK-SC ainsi que Copeland xweb et Dixell xweb.

De manière générale l'exposition d'une interface de gestion sur Internet est contraire aux bonnes pratiques.

Solutions

- **Si les équipements ne sont pas compromis :**
    - Sortir de la zone de danger :
        1. Supprimer l’exposition Internet des unités concernées et de toutes les unités exposées sur une adresse IP publique.
            - Vérifier les conditions contractuelles d’assurance avant de couper la remontée des données Internet vers le prestataire frigoriste.
        2. Vérifier l’intégralité de la configuration, notamment les plages de dégivrage.
    - Rétablir le service :
        1. Rétablir l’accès uniquement via un VPN sécurisé ou un réseau protégé.
            - Dans l'urgence, un simple filtrage des IP sources des prestataires frigoristes sur un pare-feu est possible, mais cette solution ne doit pas être considérée comme pérenne.
        2. Mettre en place les bonnes pratiques recommandées par le constructeur (mise à jour du firmware, etc.).
            - *Exemple pour les équipements Danfoss : mettre à jour le firmware, configurer le niveau de sécurité en mode Strict, s'assurer que les mots de passe par défaut ont été changés, etc.*

- **Si les équipements sont compromis :**
    - Sortir de la zone de danger :
        1. Supprimer l’exposition Internet des unités concernées et de toutes les unités exposées sur une adresse IP publique.

- Vérifier les conditions contractuelles d'assurance avant de couper la remontée des données Internet vers le prestataire frigoriste.

2. Redémarrer l'équipement Danfoss, sinon restaurer l'équipement (Reset Factory).

- Rétablir le service :

1. Rétablir l'accès uniquement via un VPN sécurisé ou un réseau protégé.
   - Dans l'urgence, un simple filtrage des IP sources des prestataires frigoristes sur un pare-feu est possible, mais cette solution ne doit pas être considérée comme pérenne.
2. Reconfigurer l'équipement pour sa remise en service.
3. Mettre en place les bonnes pratiques recommandées par le constructeur (mise à jour du firmware, etc.).
   - *Exemple pour les équipements Danfoss : mettre à jour le firmware, configurer le niveau de sécurité en mode Strict, s'assurer que les mots de passe par défaut ont été changés, etc.*.

ATTENTION : Des campagnes d'attaques sont probablement toujours en cours visant ces équipements. Maintenir une exposition Internet à un équipement sans correctif de sécurité (End of Life - EOL) est l'exposer à une très forte probabilité de compromission. N'effectuer qu'un *Reset Factory* est dans ce cas insuffisant, les persistances d'une instance compromise seront supprimées mais l'équipement restera vulnérable et sera certainement de nouveau compromis.

Documentation

- Recommandations pour une utilisation sécurisée des superviseurs XWEB https://dixell.fr/wp-content/uploads/2026/10/Recommandations-pour-une-utilisation-securisee-des-superviseurs-XWEB-v1.0.pdf

Gestion détaillée du document

Date	Description
12 octobre 2026	Version initiale

Date	Description
13 octobre 2026	Ajout d'autres équipements ciblés
16 octobre 2026	Mise à jour des recommandations

↑ Haut de page