Le SNEFCCA
SYNDICAT NATIONAL DES ENTREPRISES DU FROID, DES ÉQUIPEMENTS DE CUISINES PROFESSIONNELLES & DU CONDITIONNEMENT DE L'AIR

LES INFOS DU SNEFCCA

Réglementation technique n°2026/21 - Novembre 2026

Cybersécurité des installations frigorifiques et accès à distance – Point de situation

Plusieurs cyberattaques ont récemment visé des systèmes de supervision exploités notamment dans le secteur de la grande distribution. Ces événements démontrent que les installations connectées de nos clients constituent désormais une cible privilégiée pour les acteurs malveillants.

À ce stade, et sous réserve des conclusions définitives des autorités compétentes, il apparaît que les attaquants auraient exploité des points d'accès vulnérables présents sur les infrastructures informatiques de nos clients. Il est également probable que des identifiants administrateurs temporaires utilisés dans le cadre de certaines opérations de maintenance aient été compromis puis utilisés par les assaillants.

Il convient de rappeler que les installations frigorifiques ne constituent qu'un des éléments exposés du système d'information du client. Les enjeux de cybersécurité dépassent donc largement le seul périmètre du froid commercial et industriel.

La sécurisation des infrastructures informatiques permettant l'accès aux installations relève en premier lieu de la responsabilité du client exploitant, qui demeure responsable de son réseau et de son système d'information. Toutefois, les installateurs et mainteneurs frigoristes doivent mettre en œuvre les mesures de diligence nécessaires afin de limiter les risques d'intrusion via les solutions de télémaintenance qu'ils utilisent.

Situation actuelle

Les informations dont nous disposons montrent que la menace demeure active et que des attaques ont encore été constatées ces derniers jours. Les entreprises doivent considérer que des installations même si elles n’ont pas encore été compromises peuvent toujours être ciblées.

Depuis la diffusion des premières alertes au sein de la Profession le 12 octobre 2026, chaque intervenant doit prendre toutes les mesures nécessaires pour éviter la survenance de nouveaux sinistres.

Réalisation d'un audit des installations

Les entreprises sont invitées à procéder dans les meilleurs délais à un audit complet de leur parc d'installations sous contrat ou bénéficiant d'un accès à distance afin d'identifier :

- Les équipements accessibles depuis Internet ;
- Les mots de passe faibles ou inchangés depuis une longue période ;
- Les systèmes utilisant des logiciels ou firmwares obsolètes ;
- Les connexions distantes non conformes aux bonnes pratiques de cybersécurité de l’ANSSI.

Traitement des installations vulnérables

Lorsqu'une installation présente un niveau de vulnérabilité élevé et que les conditions minimales de sécurité ne sont pas réunies, il est recommandé de suspendre temporairement l'accès distant jusqu'à la mise en conformité de l'infrastructure informatique du client.

Durant cette période exceptionnelle :

- Le client doit être informé formellement des risques encourus ;
- **Les opérations de levée de doute à la suite d'une alarme devront être réalisées directement par le client ou son représentant** ;

- Un courrier de notification précisant les motifs de la suspension temporaire de la télémaintenance devra être adressé au client (voir courrier joint).

Recommandations en matière de cybersécurité :

Les accès permettant le pilotage ou la supervision des installations doivent respecter les principes de cybersécurité préconisés par l'ANSSI (voir ci-joint).

Certains professionnels préconisent l'utilisation de TeamViewer pour prendre la main à distance sur les installations frigorifiques de vos clients. Si cette solution peut sembler rassurante et pratique à première vue, elle peut également constituer une vulnérabilité de cybersécurité en ouvrant un accès supplémentaire au système du client. En conséquence cette pratique est généralement déconseillée.

Politique de gestion des mots de passe

Les entreprises doivent mettre en œuvre une politique rigoureuse portant notamment sur :

- La robustesse des mots de passe ;
- Leur renouvellement périodique ;
- L'interdiction du partage non contrôlé des identifiants ;
- La suppression immédiate des comptes inutilisés ;
- L'activation de l'authentification multifacteur dès que celle-ci est disponible.

Conclusion

La cybersécurité des installations frigorifiques est un enjeu majeur de continuité d'activité pour les exploitants et pour les entreprises de maintenance. Dans le contexte actuel, la vigilance doit être maximale.

Chaque entreprise est invitée à mener sans délai une revue de ses pratiques, à sensibiliser ses collaborateurs et à engager avec ses clients les actions nécessaires pour sécuriser durablement les accès distants aux installations.

Fichiers en téléchargement :

Guide ANSSI - Recommandations relatives à l'authentification multifacteur et aux mots de passe :
(https://www.snefcca.com/Data/downloads/Article/7085991266_1097_anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf)

Modèle courrier - Cyberattaque des installations frigorifiques – Mesures de sécurité et adaptation temporaire de la surveillance :
(https://www.snefcca.com/Data/downloads/Article/0442266798_1097_modele_courrier_clients_cyberattaque_snefcca_modifiable.docx)

Incident de sécurité ciblant les contrôleurs à distance des installations de réfrigération : (https://www.snefcca.com/Data/downloads/Article/6882262795_1097_incident-de-securite-ciblant-les-controleurs-a-distance-des-installations-de-refrigeration-cert-fr.pdf)