AIRNITE

# ZERO DAY

NUMÉRO 01/2026 · SÉCURITÉ INFORMATIQUE

# Congélateurs à 50 degrés : comment des pirates prennent le contrôle du froid des supermarchés

En octobre 2026, des attaquants ont pris le contrôle des régulateurs de froid d'environ 700 sites en France, imputés à une unité iranienne. Ce qui s'est passé, comment cela fonctionne et ce qu'il faut faire.

Publié le: 20 novembre 2026 Mis à jour le: 21 novembre 2026 Temps de lecture: 8 min
Auteur: Rédaction Airnite

SOFTWARE. SECURITY. CODE.

// LA SITUATION EN CHIFFRES

**≈ 700**
**sites attaqués en France**
surtout la grande distribution (rapport du C4 du 09/11/2026)

**≥ 15**
**départs de feu**
conséquence des paramètres de dégivrage modifiés (C4)

**≤ 5.3.2**
**firmware Danfoss AK-SM800A concerné**
pas encore de numéros CVE (BSI, version 1.1 du 17/11/2026)

**3 chiffres**
**appareils exposés sur Internet en Allemagne**
« un nombre à trois chiffres peu élevé » selon le BSI

Dans la nuit du 11 au 12 octobre 2026, les congélateurs se réchauffent dans des centaines de supermarchés français. Des attaquants ont pris à distance le contrôle des régulateurs de froid et fixé les paramètres de dégivrage à de hautes températures. Au matin, les magasins doivent jeter des produits frais et surgelés. Trois semaines plus tard, des magasins en Suède, en Belgique et au Luxembourg sont touchés. Le 9 novembre 2026, la France désigne officiellement un auteur : une unité cyber des Gardiens de la Révolution iraniens.

## // Que s'est-il passé ?

Le 9 novembre 2026, le Centre de coordination des crises cyber (C4), qui réunit l'ANSSI, le COMCYBER, la DGA, la DGSE et la DGSI, a publié un rapport sur l'attaque. Selon ce document, les contrôleurs de froid d'**environ 700 sites de la grande distribution** ont été compromis dans la nuit du 11 au 12 octobre, principalement dans les groupes Casino, Leclerc, Coopérative U, Metro, Carrefour et Intermarché. De petites boucheries, un abattoir et des usines agroalimentaires coopératives ont également été touchés. Conséquences : d'importantes pertes de marchandises et, dans **au moins 15 cas, des départs de feu**.

Le C4 impute l'attaque à l'unité **Shahid Kaveh**, rattachée au Centre électronique et cyber du Corps des Gardiens de la Révolution islamique. Les autorités évoquent un faisceau d'indices : la même infrastructure a servi au même moment à reconnaître des équipements Schneider Electric, les opérateurs ont utilisé l'outil de scan FOFA, l'attaque a été relayée dès le 13 octobre par l'organe de propagande CyberbanNews, et des traces de farsi ont été retrouvées dans l'infrastructure d'attaque. Aucune demande de rançon n'est connue ; selon le C4, l'objectif était le sabotage et la déstabilisation.

Les chiffres par enseigne proviennent de premiers articles de presse : selon l'AFP et BFMTV, repris par IT-Connect, entre 150 et 200 magasins Intermarché et moins d'une centaine de magasins Coopérative U ont été touchés. Selon Malwarebytes, le groupement Les Mousquetaires (Intermarché, Netto) estime les pertes à plusieurs millions d'euros. L'ANSSI avait déjà publié une alerte via le CERT-FR le 12 octobre, citant les contrôleurs à distance des gammes **Danfoss AK-SM et AK-SC**, **Copeland xweb** et **Dixell xweb**. Danfoss a indiqué à l'AFP que la plupart des équipements touchés étaient des produits anciens sans mises à jour logicielles ni de sécurité.

Dans la nuit du 1er au 2 novembre 2026, d'autres incidents ont suivi en Suède (magasins ICA et Coop), en Belgique et au Luxembourg ; en Belgique, environ 40 magasins Delhaize auraient été touchés selon heise. Rien ne confirme qu'il s'agissait des mêmes auteurs et de la même méthode ; le rapport du C4 porte sur la France. En Bavière, le journal local Kreisbote a signalé le 18 novembre des points de vente Edeka et Rewe ainsi qu'une boucherie touchés.

## // Comment fonctionne l'attaque ?

Le froid d'un supermarché n'est pas un simple circuit avec un thermostat, mais un petit réseau informatique. Un superviseur central pilote les meubles frigorifiques, les chambres froides et les centrales. Pour que le frigoriste ou le prestataire de maintenance n'ait pas à se déplacer pour chaque réglage, l'appareil dispose d'une interface web accessible à distance. C'est précisément ce confort qui ouvre la porte.

Si l'interface est accessible directement depuis Internet, des failles logicielles ou des identifiants faibles suffisent pour prendre le contrôle. L'attaquant n'a rien à chiffrer ni à voler : il modifie seulement des valeurs. Il faut ici distinguer trois choses. **D'abord la consigne :** la presse, citant BFMTV, a rapporté une consigne de 50 °C ; le C4 évoque de manière plus générale des paramètres de dégivrage fixés à de hautes températures. **Ensuite la durée du dégivrage :** selon Le Monde, cité par Malwarebytes, les cycles de dégivrage ont été prolongés d'une à huit heures. Pendant le dégivrage, l'installation chauffe volontairement et les alarmes de température sont retardées. **Enfin la température réellement mesurée** dans les meubles : aucune mesure publique fiable n'est disponible. Seul le résultat est certain : des produits perdus et, dans au moins 15 cas, un départ de feu.

Les autorités n'ont pas publié en détail comment les attaquants sont entrés. On sait que, dès août 2026, l'équipe Team82 de Claroty a présenté des failles dans l'interface web du Danfoss AK-SM 800A et trouvé des milliers d'interfaces d'administration accessibles sur Internet. D'autres découvertes ont suivi les attaques. Le 11 novembre, Midnight Blue a signalé six failles jusque-là inconnues dans le firmware 5.3.2, permettant d'exécuter du code sans authentification, y compris dans le mode Strict, pourtant renforcé. Le 13 novembre, un chercheur a publié 14 failles dans Copeland XWEB EVO. **Rien ne prouve que ces nouvelles failles aient été utilisées lors des attaques d'octobre.** Elles montrent toutefois la vulnérabilité de ces appareils. Le BSI avertit que des attaquants capables d'exécuter du code pourraient installer un firmware malveillant ; les appareils seraient alors inutilisables et devraient être restaurés manuellement ou remplacés.

## // Qui est concerné ?

L'Office fédéral allemand de la sécurité de l'information (BSI) a publié un avis de sécurité le 13 novembre et l'a mis à jour le 17 novembre. Sont concernés les superviseurs Danfoss **AK-SM800A avec un firmware jusqu'à au moins la version 5.3.2** (aucun numéro CVE attribué à ce stade) ainsi que tous les appareils de la famille **Copeland XWEB EVO jusqu'au firmware 5.8.8**. Copeland a arrêté le support logiciel de XWEB EVO en mars 2026 : les failles restantes ne seront donc jamais corrigées. Selon le BSI, des capteurs ont enregistré des tentatives d'exploitation actives de deux failles Copeland peu après leur publication. Et : **selon le BSI, un nombre à trois chiffres peu élevé de ces appareils reste directement accessible depuis Internet en Allemagne.**

La grande distribution n'est donc pas seule en cause. En France, des boucheries, un abattoir et des usines agroalimentaires ont été touchés, en Bavière une boucherie. Des contrôleurs de froid et de bâtiment connectés fonctionnent aussi dans les entrepôts frigorifiques, la restauration et les bâtiments tertiaires. Au même moment, le C4 a observé des attaques contre des équipements de petites installations hydroélectriques. Selon heise, la présidente du BSI, Claudia Plattner, a souligné qu'une telle attaque pouvait toucher n'importe quel pays et trouver des imitateurs à tout moment. Ce qui compte, c'est moins la taille de l'entreprise que la question de savoir si son contrôleur est accessible de l'extérieur et qui en assure la maintenance. Si un prestataire de maintenance est compromis, un seul accès peut, dans le pire des cas, mener un attaquant vers de nombreux sites.

## // Que faire maintenant ?

Les recommandations du BSI, du CERT-FR et de Midnight Blue convergent : les contrôleurs industriels n'ont rien à faire directement sur Internet. Si une connexion permanente avec un site est nécessaire, elle doit passer par un VPN sécurisé. Celui qui ignore si son installation est accessible doit le vérifier aujourd'hui, et non après le prochain incident. Le CERT-FR avertit expressément que des campagnes d'attaques sont probablement toujours en cours.

Mises à jour et paramètres de sécurité aident, mais ne suffisent pas. Le BSI écrit que de nouveaux correctifs ne garantissent pas que d'autres failles ne seront pas bientôt connues dans un produit concerné. Le CERT-FR recommande d'activer le mode Strict ; Midnight Blue a cependant montré que ce mode est lui aussi vulnérable. Pour les appareils en fin de vie sans mises à jour, le CERT-FR précise qu'une réinitialisation d'usine ne suffit pas non plus. La protection décisive reste la suppression de l'accès direct depuis Internet. La check-list ci-dessous résume les étapes.

## // Comment Airnite vous aide-t-il ?

Dans le cadre d'un **test d'intrusion**, Airnite vérifie précisément ce que votre entreprise expose sur Internet : contrôleurs, interfaces web, accès de télémaintenance et routeurs oubliés. Pour les installations industrielles, nous commençons par une analyse d'exposition passive ; les tests actifs n'ont lieu qu'avec votre accord et selon une procédure convenue. Vous recevez une liste priorisée de constats et de mesures, sans alarmisme. En **conseil**, nous définissons avec vous et votre prestataire de maintenance des accès à distance propres : VPN, authentification à deux facteurs, journalisation et responsabilités claires dans le contrat. En **formation**, la direction du magasin et les services techniques apprennent à reconnaître tôt les signaux d'alerte et à réagir correctement en cas d'incident.

> Remarque : les chiffres sur les magasins touchés et les températures diffèrent selon les sources (pour la Belgique, certains rapports évoquent 70 °C). Nous indiquons chaque chiffre avec son origine. État de la recherche : 21 novembre 2026.

## Check-list : ce qu'il faut faire maintenant

[+] Vérifier si les contrôleurs de froid et de bâtiment (superviseurs, interfaces web, routeurs, modems cellulaires du prestataire) sont accessibles directement depuis Internet – et supprimer immédiatement cette exposition.

[+] N'autoriser la télémaintenance que via un VPN sécurisé ou un réseau protégé ; un filtrage IP dans le pare-feu n'est qu'une mesure d'urgence.

[+] Contrôler l'ensemble de la configuration, en particulier les consignes, les durées et températures de dégivrage et les seuils d'alarme.

[+] Installer les mises à jour de firmware disponibles, changer les mots de passe par défaut et activer le niveau de sécurité le plus élevé (Strict) – sans s'y fier : selon Midnight Blue, le mode Strict est lui aussi vulnérable.

[+] Identifier les appareils en fin de vie sans mises à jour de sécurité (par exemple Copeland XWEB EVO, support arrêté en mars 2026) et planifier leur remplacement – une réinitialisation seule ne suffit pas.

[+] Mettre en place une surveillance indépendante des températures, avec ses propres sondes et une alerte séparée, afin de détecter une manipulation même si le contrôleur de froid est compromis.

[+] Convenir avec le frigoriste ou le prestataire de maintenance qui accède à quels sites et comment, et protéger ces accès par une authentification à deux facteurs.

[+] Définir une procédure d'urgence : qui détecte un écart de température, qui décide du sort des marchandises, qui signale l'incident (police, CERT-FR, CNIL le cas échéant).

## Comment Airnite vous aide

- Tests d'intrusion et sécurité – Attaques contrôlées avec rapport clair et plan d'action.
- Conseil – Un regard extérieur sur vos projets.
- Formations – Votre équipe apprend nos outils et méthodes.

### Vos systèmes sont-ils accessibles depuis Internet ?

Airnite vous accompagne dans une évaluation autorisée de la sécurité et de l'exposition de vos accès à distance. Pour les contrôleurs industriels, nous commençons de manière passive : nous déterminons ce qui est visible de l'extérieur sans intervenir sur l'installation. Les tests actifs sur des installations en production n'ont lieu qu'avec votre accord, une procédure de test convenue et des précautions de sécurité adaptées.

**Demander un premier échange · Écrire un e-mail · Par WhatsApp**

### Contact

Des questions sur cet article ? Écrivez-nous sur WhatsApp : +49 174 6834842

Lire en ligne: https://airnite.de/fr/magazine/frigos-supermarches-pirates-50-degres/

## Sources

Chaque fait de cet article repose sur les sources ci-dessous. Les sources primaires sont signalées.


1. **C4 (ANSSI, COMCYBER, DGA, DGSE, DGSI) · CERTFR-2026-CTI-009 : Activités cyber offensives menées par des acteurs iraniens liés au CGRI** · 09/11/2026 · SOURCE PRIMAIRE
   Rapport des autorités françaises : imputation à l'unité Shahid Kaveh, environ 700 sites, au moins 15 départs de feu, éléments d'imputation
   https://cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-009.pdf

2. **CERT-FR · CERTFR-2026-ALE-012 : Incident de sécurité ciblant les contrôleurs à distance des installations de réfrigération** · 12/10/2026, mise à jour 16/10/2026 · SOURCE PRIMAIRE
   Alerte des autorités françaises : gammes concernées (Copeland xweb, Danfoss AK-SC et AK-SM, Dixell xweb), recommandations, campagnes en cours
   https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/

3. **BSI · Avis de sécurité 2026-306525-11e2 : Danfoss AK-SM800A & Copeland XWEB EVO – vulnérabilités zero-day dans des contrôleurs de froid** · version 1.0 du 13/11/2026, version 1.1 du 17/11/2026 · SOURCE PRIMAIRE
   Avis de l'autorité allemande : versions concernées, appareils accessibles en Allemagne, évaluation et mesures
   https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-306525-1032.pdf?__blob=publicationFile&v=2

4. **Midnight Blue · Multiple remote code execution vulnerabilities in Danfoss AK-SM800A** · 11/11/2026 (date selon le BSI) · SOURCE PRIMAIRE
   Recherche en sécurité : six failles sans authentification jusqu'au firmware 5.3.2, y compris en mode Strict, recommandations
   https://www.midnightblue.nl/blog/multiple-rce-danfoss-aksm800a

5. **heise online · Hackers breach refrigerators at grocery stores in more countries** · 02/11/2026
   Presse spécialisée : incidents en Suède, en Belgique et au Luxembourg, déclaration de la présidente du BSI
   https://www.heise.de/en/news/Hackers-breach-refrigerators-at-grocery-stores-in-more-countries-11508080.html

6. **heise online · Supermarkt-Angriffe: Danfoss-Kühlsteuerungen blieben trotz Updates angreifbar** · 13/11/2026
   Presse spécialisée : avis du BSI, résultats de Midnight Blue, alerte du CCB belge
   https://www.heise.de/news/Supermarkt-Angriffe-Danfoss-Kuehlsteuerungen-blieben-trotz-Updates-angreifbar-11524376.html

7. **Malwarebytes · Hackers heat up supermarket fridges, spoiling food across France** · 13/10/2026
   Recherche en sécurité : déroulé en France, cycles de dégivrage selon Le Monde, déclaration de Danfoss à l'AFP, estimation des pertes
   https://www.malwarebytes.com/blog/news/2026/10/hackers-heat-up-supermarket-fridges-spoiling-food-across-france

8. **IT-Connect · Super U, Intermarché : des pirates font chauffer les congélateurs à 50 °C** · 12/10/2026
   Presse spécialisée française : consigne de 50 °C et nombre de magasins (AFP/BFMTV), recherche de Claroty Team82
   https://www.it-connect.fr/cyberattaque-supermarches-froid-danfoss/

9. **Kreisbote · Hackerangriff auf Kühlsystem: Biomarkt im Landkreis findet zwei Sicherheitslücken** · 18/11/2026
   Presse locale : cas en Bavière
   https://www.kreisbote.de/lokales/weilheim-schongau/sicherheitsluecken-hackerangriff-auf-kuehlsystem-biomarkt-im-landkreis-fand-zwei-94593420.html

*Information éditoriale générale, sans conseil juridique ni examen individuel de vos systèmes. État : date de publication.*

---

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de