AIRNITE

ZERO DAY

ISSUE 01/2026 · IT SECURITY

Freezers at 50 degrees: how attackers take over supermarket refrigeration

In October 2026, attackers took over the refrigeration controllers of around 700 sites in France, and France names an Iranian unit as the culprit. What happened, how it works and what operators should do now.

Published: 20 November 2026 Updated: 21 November 2026 Reading time: 8 min
Author: Airnite editorial team

SOFTWARE. SECURITY. CODE.

// THE SITUATION IN NUMBERS

≈ 700
sites attacked in France
mainly food retail (C4 report of 9 Nov 2026)

≥ 15
fires
caused by the manipulated defrost parameters (C4)

≤ 5.3.2
affected Danfoss AK-SM800A firmware
no CVE numbers yet (BSI, version 1.1 of 17 Nov 2026)

three-digit
devices in Germany openly online
“a low three-digit number” according to the BSI

On the night of 11 to 12 October 2026, freezers warm up in hundreds of French supermarkets. Attackers have remotely taken over the refrigeration controllers and set the defrost parameters to high temperatures. In the morning, the stores have to throw away fresh and frozen food. Three weeks later, stores in Sweden, Belgium and Luxembourg are hit. On 9 November 2026, France officially names a culprit: a cyber unit of Iran's Revolutionary Guards.

// What happened?

On 9 November 2026, France's cyber crisis coordination centre C4, in which ANSSI, the armed forces' cyber command, the defence procurement agency DGA and the intelligence services DGSE and DGSI work together, published a report on the attack. According to it, the refrigeration controllers of **around 700 food retail sites** were compromised on the night of 11 to 12 October, mainly at the Casino, Leclerc, Coopérative U, Metro, Carrefour and Intermarché groups. Small butchers, an abattoir and cooperative food plants were also hit. The consequences: heavy losses of stock and, in **at least 15 cases, fires**.

The C4 attributes the attack to the **Shahid Kaveh** unit, part of the electronic and cyber centre of Iran's Islamic Revolutionary Guard Corps. The authorities cite a body of evidence: the same infrastructure was used at the same time to scan Schneider Electric controllers, the attackers used the FOFA scanning tool, the attack was promoted from 13 October on the propaganda channel CyberbanNews, and traces of Farsi were found in the attack infrastructure. No ransom demand is known; in the C4's assessment the aim was sabotage and destabilisation.

Figures for individual chains come from earlier media reports: according to AFP and BFMTV, as summarised by IT-Connect, between 150 and 200 Intermarché stores and fewer than a hundred Coopérative U stores were affected. According to Malwarebytes, the Les Mousquetaires group (Intermarché, Netto) estimates the damage at several million euros. France's cyber security agency ANSSI had already issued an alert through its CERT-FR on 12 October, naming remote controllers from the **Danfoss AK-SM and AK-SC** series, **Copeland xweb** and **Dixell xweb**. Danfoss told AFP that most of the affected devices were legacy products without software or security updates.

On the night of 1 to 2 November 2026, incidents followed in Sweden (ICA and Coop stores) as well as in Belgium and Luxembourg; in Belgium, heise reports around 40 affected Delhaize stores. Whether the same perpetrators and method were involved there has not been confirmed; the C4 report covers France. From Bavaria, the local paper Kreisbote reported on 18 November that branches of Edeka and Rewe and a butcher's shop were affected.

// How does the attack work?

A supermarket's refrigeration is not a circuit with a thermostat but a small computer network. A central system manager controls cabinets, cold rooms and rack systems. So that the refrigeration or maintenance contractor does not have to travel for every setting, the device has a web interface that can be reached remotely. That very convenience is the way in.

If the interface is reachable directly from the internet, software vulnerabilities or weak credentials are enough to take over the controller. The attacker does not have to encrypt anything or steal data; they only change values. Three things should be kept apart here. **First, the setpoint:** media reports citing BFMTV said a setpoint of 50 °C was set; the C4 refers more generally to defrost parameters fixed at high temperatures. **Second, the defrost time:** according to Le Monde, quoted by Malwarebytes, defrost cycles were extended from one to eight hours. During defrost the system deliberately heats, and temperature alarms are delayed. **Third, the temperature actually measured** in the cabinets: no reliable public measurements are available. What is certain is the result: spoiled food and, in at least 15 cases, fire.

The authorities have not published in detail exactly how the attackers got in. What is known: as early as August 2026, Claroty's research team Team82 presented flaws in the web interface of the Danfoss AK-SM 800A and found thousands of management interfaces openly reachable on the internet. After the attacks, more findings followed. On 11 November, Midnight Blue reported six previously unknown flaws in firmware 5.3.2 that allow code execution without logging in, explicitly including the specially hardened Strict mode. On 13 November, a researcher published 14 flaws in Copeland XWEB EVO. **There is no evidence that these new flaws were used in the October attacks.** But they show how vulnerable such devices are. The BSI warns that attackers with code execution could install malicious firmware; the devices would then be unusable and would have to be restored by hand or replaced.

// Who is affected?

Germany's Federal Office for Information Security (BSI) published an IT security notice on 13 November and updated it on 17 November. According to it, Danfoss system managers **AK-SM800A with firmware up to at least 5.3.2** are affected (no CVE numbers have been assigned yet), as are all devices of the **Copeland XWEB EVO family up to firmware 5.8.8**. Copeland ended software support for XWEB EVO in March 2026, so the remaining flaws will stay open for good. According to the BSI, sensors registered active exploitation attempts against two of the Copeland flaws shortly after publication. And: **according to the BSI, a low three-digit number of such devices in Germany can still be reached directly from the internet.**

This is not only a problem for large food retailers. In France, butchers, an abattoir and food plants were hit, and in Bavaria a butcher's shop. Networked refrigeration and building controllers also run in cold stores, restaurants and commercial buildings. At the same time, the C4 observed attacks on controllers of small hydroelectric plants. According to heise, BSI President Claudia Plattner stressed that such an attack could hit any country and find imitators at any time. What matters is less the size of the business than whether its controller can be reached from outside and who maintains it. If a maintenance contractor is compromised, in the worst case one access can lead an attacker to many sites.

// What should you do now?

The recommendations of the BSI, CERT-FR and Midnight Blue come down to the same core: industrial controllers do not belong directly on the internet. If a permanent connection to a site is needed, it should go through a secured VPN. Anyone who does not know whether their system is reachable should find out today, not after the next incident. CERT-FR explicitly warns that the attack campaigns are probably still ongoing.

Updates and security settings help but are not enough. The BSI writes that new patches are no guarantee that further vulnerabilities will not soon become known in an affected product. CERT-FR recommends enabling Strict mode; however, Midnight Blue has shown that this mode is also vulnerable. For legacy devices without updates, CERT-FR says even a factory reset is not enough. The decisive protection remains removing direct reachability from the internet. The checklist below sums up the steps.

// How does Airnite help?

In a **penetration test**, Airnite checks precisely what of your company is visible from the internet: controllers, web interfaces, remote maintenance access and forgotten routers. For industrial installations we start with a passive exposure analysis; active testing only takes place with your approval and an agreed procedure. You get a prioritised list of findings and actions, not scaremongering. In **consulting**, we work with you and your maintenance contractor to set up remote access properly: VPN, two-factor authentication, logging and clear responsibilities in the contract. In **training**, store management and facility staff learn to spot warning signs early and to react correctly in an emergency.

> Note: figures on affected stores and temperatures differ between sources (for Belgium, some reports mention 70 °C). We give each figure with its origin. Research status: 21 November 2026.

Checklist: what to do now

[+] Check whether refrigeration and building controllers (system managers, web interfaces, routers, the maintenance contractor's mobile modems) can be reached directly from the internet – and remove that exposure immediately.

[+] Allow remote maintenance only through a secured VPN or protected network; an IP allow-list in the firewall is an emergency measure only.

[+] Review the complete configuration, especially setpoints, defrost times, defrost temperatures and alarm limits.

[+] Install available firmware updates, change default passwords and enable the highest security level (Strict) – but do not rely on it: according to Midnight Blue, Strict mode is also vulnerable.

[+] Identify legacy devices without security updates (such as Copeland XWEB EVO, support ended in March 2026) and plan their replacement – a reset alone is not enough there.

[+] Set up independent temperature monitoring with its own sensors and separate alerting, so that manipulation is noticed even if the refrigeration controller itself is compromised.

[+] Agree with your refrigeration or maintenance contractor who accesses which sites and how, and protect those accounts with two-factor authentication.

[+] Define an emergency procedure: who notices a temperature deviation, who decides about stock, who reports the incident (police, national CERT, data protection if needed).

How Airnite helps

- Penetration Testing & Security – Controlled attacks with a clear report and action plan.
- Consulting – An outside view of your plans and projects.
- Training – Your team learns our tools and processes.

Can your systems be reached from the internet?

Airnite supports you with an authorised security and exposure assessment of your remote access. For industrial controllers we start passively: we determine what is visible from outside without touching the installation. We only run active tests on production systems with your approval, an agreed test procedure and appropriate safety precautions.

Request an initial call · Send an email · Via WhatsApp

Contact

Questions about this article? Message us on WhatsApp: +49 174 6834842

Read online: https://airnite.de/en/magazine/supermarket-refrigeration-hacked-50-degrees/

Sources

Every fact in this article is based on the sources below. Primary sources are marked.

1. **C4 (ANSSI, COMCYBER, DGA, DGSE, DGSI) · CERTFR-2026-CTI-009: Activités cyber offensives menées par des acteurs iraniens liés au CGRI** · 9 Nov 2026 · PRIMARY SOURCE
   French authority report: attribution to the Shahid Kaveh unit, around 700 sites, at least 15 fires, evidence
   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 Oct 2026, updated 16 Oct 2026 · PRIMARY SOURCE
   French authority alert: affected product ranges (Copeland xweb, Danfoss AK-SC and AK-SM, Dixell xweb), recommendations, ongoing campaigns
   https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/

3. **BSI · IT security notice 2026-306525-11e2: Danfoss AK-SM800A & Copeland XWEB EVO – zero-day vulnerabilities in refrigeration controllers** · version 1.0 of 13 Nov 2026, version 1.1 of 17 Nov 2026 · PRIMARY SOURCE
   German authority notice: affected versions, reachable devices in Germany, assessment and measures
   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 Nov 2026 (date according to the BSI) · PRIMARY SOURCE
   Security research: six pre-authentication flaws up to firmware 5.3.2, including Strict mode, recommendations
   https://www.midnightblue.nl/blog/multiple-rce-danfoss-aksm800a

5. **heise online · Hackers breach refrigerators at grocery stores in more countries** · 2 Nov 2026
   Trade press: incidents in Sweden, Belgium and Luxembourg, statement by the BSI president
   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 Nov 2026
   Trade press: BSI notice, Midnight Blue findings, Belgian CCB warning
   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 Oct 2026
   Security research: sequence of events in France, defrost cycles according to Le Monde, Danfoss statement to AFP, damage estimate
   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 Oct 2026
   French trade press: 50 °C setpoint and store numbers (AFP/BFMTV), Claroty Team82 research
   https://www.it-connect.fr/cyberattaque-supermarches-froid-danfoss/

9. **Kreisbote · Hackerangriff auf Kühlsystem: Biomarkt im Landkreis findet zwei Sicherheitslücken** · 18 Nov 2026
   Local press: cases in Bavaria
   https://www.kreisbote.de/lokales/weilheim-schongau/sicherheitsluecken-hackerangriff-auf-kuehlsystem-biomarkt-im-landkreis-fand-zwei-94593420.html

General editorial information, not legal advice and not an assessment of your individual systems. Status: date of publication.

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