Koniag TECH

THREAT ADVISORY · OCTOBER 2026

Freezer attacks: what they mean for you, and how we can help

Attackers are hijacking internet-connected refrigeration controllers and heating stored food overnight. The same weakness reaches HVAC, plant equipment and smart home devices. Here is what to do now, and where Koniag fits.

THE THREAT

What happened

Overnight on October 11–12, 2026, attackers took over refrigeration controllers at hundreds of French supermarkets, including Intermarché, Carrefour Market and Leclerc, and forced them into continuous defrost. Food spoiled and some units caught fire. On October 29, Reuters reported that the Pentagon is treating similar August freezer failures at US military commissaries as a suspected cyberattack. A link has not been confirmed.

EQUIPMENT	Danfoss AK-SM and AK-SC system managers; Copeland and Dixell XWEB monitoring units
ATTACK METHOD	Exposed controllers forced into defrost overnight, heating cases to as high as 50°C (122°F)
KNOWN WEAKNESSES	Outdated firmware, default passwords, CVE-2025-41450 and CVE-2025-41451
SCALE	An estimated 250–350+ French supermarkets (Oct 11–12); at least six US military commissaries (Aug 26–27, suspected)
STATUS	**Campaign likely ongoing; Pentagon investigating US incidents as a suspected hack**

Why it matters to you

- **The same equipment is here:** Danfoss, Copeland and Dixell controllers are common in US grocery stores, distribution centers, and food and pharmaceutical plants.
- **No data theft needed:** a changed setpoint destroys inventory, closes departments or stops lines, and can create food-safety and fire hazards.
- **Your vendors may be the way in:** one French chain linked the attack to the provider that manages its refrigeration remotely.
- **Insurance may not pay:** spoilage from a cyber event often falls between cyber and property policies.

DO THIS NOW · GROCERY, FOOD AND MANUFACTURING

Five steps to take this week

1. **Find it:** list every refrigeration, HVAC and building controller, including ones contractors manage.
2. **Check exposure:** confirm none can be reached from the internet. Any that can is urgent.
3. **Lock down access:** remove direct internet access, allow remote access only through a VPN with multifactor authentication, and change default passwords.
4. **Patch or replace:** update firmware; replace end-of-life models such as Danfoss AK-SM800 and AK-SC355.
5. **Watch for tampering:** review defrost schedules, setpoints and alarms, add temperature alerts independent of the controller, and tell overnight staff who to call.

Before cutting a monitoring link, check with your broker: some insurance policies require continuous temperature monitoring.

THE BIGGER PICTURE

It's not just freezers

Refrigeration is one example of a wider problem: equipment built for on-site servicing is now online, often without office-IT protections. Free search tools find these devices in minutes, and similar attacks hit supermarkets in Russia and Israel (2022) and a US meatpacking plant (2024).

WHERE IT SHOWS UP	CONNECTED DEVICES AT RISK
Stores and distribution centers	Refrigeration, HVAC, building management, energy systems, cameras and door access
Plants and processing	PLCs, HMIs and line controllers, cold rooms, blast freezers, cleanroom HVAC
Homes and consumers	Smart fridges, thermostats, cameras and doorbells with default passwords and short update lifespans, often on the same network as work laptops.

If you sell or build connected products

Ship devices with no default passwords, a published update period and labeling such as the FCC's U.S. Cyber Trust Mark. Tell customers and staff to change default passwords, enable automatic updates, keep smart devices on separate Wi-Fi and retire unsupported devices.

HOW KONIAG CAN HELP

Find it, fix it, watch it, prove it

Each service covers one part of the response; use one to fill a gap or combine them for end-to-end coverage.

01
Find
VULNERABILITY MGMT

We scan your networks for exposed refrigeration, HVAC and other controllers, then rank fixes and set deadlines.

02
Fix
PATCH MGMT

We work with your contractors to patch firmware on an agreed schedule, add interim protections and rescan.

03
Watch & Respond
SOC MDR

Our 24/7 SOC watches remote access and unusual connections to these devices, overnight included, and contains attacks fast.

04
Prove
PEN TESTING

An autonomous pen test tries to reach your controllers the way an attacker would, to confirm the gap is closed.

Where to start

IF THIS SOUNDS LIKE YOU…	A GOOD PLACE TO START
"We don't know what's connected at our stores or plants."	**Vulnerability Management**
"We know what's exposed, but our contractors manage it and we can't fix it fast enough."	**Patch Management, with Vulnerability Management**
"Were our controllers already tampered with?"	**SOC MDR**
"Nobody watches our alerts overnight, when these attacks happen."	**SOC MDR**
"We need proof for leadership, our insurer or an auditor that we're protected."	**One-time Penetration Test**

Why act now

The tools are free, the method works, and France's national cyber agency warns the campaign is likely still running. Removing internet exposure this week cuts risk far more than waiting for the next maintenance visit.

NEXT STEP

Request a cold-chain and IoT exposure review

Contact your Koniag account team. We'll confirm what's exposed, what to fix first and which services, if any, would close the gap.

Sources: Reuters (via Military Times), Insurance Business, BleepingComputer and Military Times coverage of the French supermarket and US commissary incidents, August–October 2026; CERT-FR alert as reported; CISA, FBI, EPA and DOE, "Primary Mitigations to Reduce Cyber Threats to Operational Technology," May 2025.