It's Probably Nothing
by Sierra Echo Charlie

EDITION 01 / 13 OCTOBER 2026

Hacked supermarket fridges hit 50°C in France

Plus Ahold Delhaize pulls systems offline, and Albert Heijn's app and deliveries go dark

2 stories / Listen online - 3:25

THE TAKEAWAY

Both of today's stories come from the grocery aisle. As far as anyone has said publicly, they aren't connected. One of them has attackers turning supermarket freezers into something closer to ovens, which wasn't on my bingo card for this week.

01 / THE BRIEF

Attackers push French supermarket fridges into forced defrost, reportedly up to 50°C

Overnight on 11-12 October, French time, someone got into the refrigeration controls at a lot of French supermarkets and triggered forced defrost cycles. Reporting that cites BFMTV says set-points went as high as 50 degrees Celsius, which is less a defrost and more a slow cook. Fresh and frozen stock had to be destroyed.

This one is properly confirmed. Dominique Schelcher, chief executive of Coopérative U, said on X that a cyberattack had affected refrigeration production systems at several Coopérative U stores since the previous night. He added that an investigation would be needed to establish what happened. AFP reports that Intermarché and Coopérative U told it the attack made their fridges defrost. AFP also reports that Paris prosecutors confirmed the attack.

The store count depends on who you read. BFMTV said about 150 Intermarché stores. AFP has 150-200 Intermarché stores and almost 100 Coopérative U outlets. The French trade outlet Points de Vente puts it at about 300 Intermarché stores and fewer than 100 Coopérative U stores, plus E.Leclerc stores. Citing another outlet, it says Monoprix and Carrefour Market stores were reportedly involved too. Points de Vente also reports that fires broke out at some sites.

This is the rare OT incident with straightforward physical damage. Nobody can argue it was just IT spillover when the stock is in the skip.

The Danfoss angle is where everyone will head next. Points de Vente reports that the attackers took control of a Danfoss refrigeration regulation system, which the chains use as a common supplier. Points de Vente also relays a Danfoss response through BFMTV reporter Raphaël Grably: the targeted models were obsolete or had not been updated. Nobody has publicly confirmed how the attackers got in, who they are or whether a known vulnerability was used, so it's too early to pin it on any particular Danfoss CVE. My own speculation: when competing chains are hit through the same supplier's kit on the same night, it smells more like a remote-management or vendor-access problem than a store-by-store compromise. That's a hunch, not a finding.

WORTH ASKING

If you look after remotely managed refrigeration controllers in grocery, cold chain or anywhere else, this is a good week to work out exactly what can reach them and whether anyone would notice a set-point jumping to 50 degrees Celsius at 3am.

QUALIFICATIONS

Store counts vary between outlets. The fires come from Points de Vente reporting. The intrusion route, the attacker and any specific vulnerability involved remain unconfirmed.

SOURCES

Cyberattack Manipulates Refrigeration at French Supermarkets, Destroying Fresh Stock (Mallory) - Reporting / context

Cyberattaque sur les systèmes frigorifiques de plusieurs enseignes - Points de Vente - Reporting / context

French supermarket chains say cyberattack forced refrigerator shutdown (AFP via malware.news) - Reporting / context

Attackers Reportedly Hack Supermarket Fridges and Raise Temperatures to 50°C - Reporting / context

02 / THE BRIEF

Ahold Delhaize takes systems offline; Albert Heijn's app, website and deliveries go down

Separately, Ahold Delhaize put out a release on 12 October, tagged as a regulatory press release. It says the company is experiencing a security issue within its network and is taking some systems offline to protect them. Stores are open and serving customers.

In the Netherlands, DutchNews reports that Albert Heijn's website, app and home delivery service became unavailable. Etos and Gall & Gall were affected as well, and customer service and logistics systems were offline. Tills kept working, but personal discounts and app-linked savings were paused. Electronic shelf labels might still be showing last week's offer prices. That small detail says a lot about how much of a modern supermarket lives in the back end. Across the Atlantic, Grocery Dive reports that the websites of all five of the company's US banners were down on Monday morning.

The disclosure doesn't name an attacker or an entry point, and it doesn't say whether ransomware or data theft is involved. Taking systems offline as a precaution across two continents at once usually isn't a minor thing, but that's me reading tea leaves. We'll know more when they say more.

QUALIFICATIONS

The cause, the attacker and any data impact are all unconfirmed. The statement is dated but not timed.

SOURCES

Ahold Delhaize Takes Systems Offline After Cybersecurity Incident, Disrupting Digital Services (Mallory) - Reporting / context

Ahold Delhaize takes precautionary measures following cybersecurity incident - Primary source

Albert Heijn app and deliveries down after "IT incident" - Reporting / context

Ahold Delhaize experiencing cybersecurity issue - Reporting / context

Ahold Delhaize Takes Systems Offline Following Cybersecurity Incident - Reporting / context

---

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

All our threat intelligence comes from Mallory.ai.

Want intelligence your team can act on? Reach out for a chat.